# Foglight Net Monitor 6.3.0
# User and Reference Guide

owners.

**Legend**

■ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

❗ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

# Monitoring network devices

Foglight Net Monitor provides device availability and packet loss monitoring between monitoring locations and network devices. Use it to:

- Monitor the network against service level agreements.

- Check for the presence of devices that are critical to your operating environment.

When you deploy Foglight Net Monitor, a set of predefined dashboards enables you to view the performance of the monitored network devices. This allows you to ensure consistent network device performance by re the collected statistics. Better management of your network devices can be achieved when you are alerted to potential problems before end users are affected.

Foglight Net Monitor relies on the Net Monitor Agent to collect data. The agent collects transaction information from monitored devices and visualizes the collected data in Foglight. You need to configure one agent instance on each monitored location.

Start by installing Foglight Net Monitor on the Management Server, deploying the Net Monitor Agent package, and creating agent instances on one or more hosts. For installation instructions, see the *Foglight Net Monitor  Release Notes*.

Foglight Net Monitor uses the ICMP (Internet Control Message Protocol) service to monitor network devices. You need to configure this service to enable communication with network devices. For more information, see Configuring the ICMP service for monitoring.

As a next step, you can specify the devices that you want to monitor using the Devices Management dashboard. In addition to managing the collection of monitored network devices, this dashboard allows you to edit the data collection settings. For more information, see Managing monitored network devices.

Next, navigate to the Performance Browser. This dashboard displays the state of your system performance, providing a visual representation of the status of the monitored network devices and locations. Using this dashboard on a daily basis you can obtain an in-depth understanding of the state of your monitored network devices. Monitoring the same collection of network devices from different agent locations allows you to rule out any issues that may be related to host connectivity rather than device responsiveness. For more information, see Investigating the performance of network devices.

The Net Monitor Agent is equipped with a set of properties that affect its running state. You can make changes to them, as required. For more information about the Net Monitor Agent properties, see Configuring the agent properties.

For additional information, see the following topics:

- Generating reports

- View reference

# Configuring the ICMP service for monitoring

Foglight Net Monitor uses the ICMP (Internet Control Message Protocol) service to communicate with network devices. There are two versions of this service that are available for use:

- *Foglight Agent Manager ICMP service* uses the *udp2icmp* application, that is installed with the Agent Manager, and can be used to issue ICMP messages to target devices.

- *OS-specific ICMP services* use the following OS-level commands to issue ICMP messages to target devices:

    - `ping`

    - `tracert` (Microsoft Windows only) or `traceroute` (Linux only)

Both types of ICMP services are started through an executable application and require proper permissions to execute. For more information, see Configuring the Agent Manager ICMP service and Configuring OS-Level ICMP services.

By default, Foglight Net Monitor uses the Agent Manager ICMP service for monitoring. OS-level ICMP services can be configured, if needed, using the following option
`-Dnetmonitor.icmpprovider=OS`

There are two ways to specify this option:

- On the command line, when you start up the Agent Manager. For example:
  `fglam -s -Dnetmonitor.icmpprovider=OS`

- As a JVM system property, in the *<fglam_home>/state/default/config/baseline.jvmargs.config* file. For example:
  `-Dnetmonitor.icmpprovider=OS`

Other options are available. For more information, see ICMP service command-line options.

## ICMP service command-line options

The following table describes the Foglight Net Monitor parameters that can be used to configure the ICMP service. You can specify these options on the command line, or in an Agent Manager configuration file. For more information, see Configuring the Agent Manager ICMP service.

**Table 1. Foglight Net Monitor parameters used to configure the ICMP service**

| Option | Description |
| --- | --- |
| **netmonitor.icmpprovider** | All agent instances managed by this Agent Manager uses the OS-level ICMP service. This type of ICMP service uses `ping` and `traceroute`/`tracert` commands. The login user must have proper permissions to execute these commands, without providing a password. |
| **netmonitor.ping.path** | **Unix/Linux only.** If the login user does not have the permissions to execute the `ping` command, use this option to specify the command path. |
| **netmonitor.traceroute.path** | **Unix/Linux only**. If the login user does not have the permissions to execute the `traceroute` command, use this option to specify the command path. |
| **netmonitor.threadpool.size** | **Unix/Linux only**. Sets the thread pool size. You should specify at least 10. |

# Configuring the Agent Manager ICMP service

## Windows configuration

- The user account launching the Agent Manager application must be an Administrator.

- To prevent time-outs in the trace route responses for all hops except the first and the last when the firewall is on, configure the firewall to enable inbound ICMP network traffic. For more information, visit http://technet.microsoft.com/en-us/library/cc972926%28v=ws.10%29.aspx.

    Specifically, for IPv4, you need to use the following configuration:

```
ICMP Echo Request (Type 8, Code 8)

ICMP Echo Reply (Type 0, Code 0)

ICMP TTL Expired (Type 11, Code 0)

ICMP Port Unreachable (Type 3, Code 3)
```

## UNIX/Linux configuration

- If the user account launching the Agent Manager application is not the root user, they must be granted permissions to execute the *<fglam_home>/client/<build id>/bin/udp2icmp* application without providing a password.

- If the Agent Manager secure-launcher is configured with a sudo path, `requiretty` must **not** be set.

# Configuring OS-Level ICMP services

## Windows configuration

- Ensure that the `ping` and `tracert` commands are available.

- The user account launching the Agent Manager application must have permissions to execute both `ping` and `tracert` commands.

## UNIX/Linux configuration

- Ensure that the `ping` and `traceroute` commands are available.

- The user account launching the Agent Manager application must have permissions to execute both `ping` and `traceroute` commands.

- For Suse Linux with the `apparmor` module, enable `traceroute` to execute with the `-I` option. For example:

```
# Execute blow commands to enable traceroute -I option

complain /usr/sbin/traceroute

/etc/init.d/boot.apparmpr restart
```

# Managing monitored network devices

The Devices Management dashboard displays a list of the monitored network devices. It allows you to add or remove network devices from the collection, and to edit their data collection parameters.

**NOTE:** Before adding new network devices for the first time using this dashboard, you must ensure that the following steps are completed:

- Deploy the Net Monitor Agent package to one or more desired monitoring locations (hosts).
- Create one or more Net Monitor Agent instances.
- Set the running mode for the newly agent created instances (Quick Check more or Normal mode).
- Configure data collection intervals for the newly created agent instances.
- Activate the newly created agent instances, and start their data collection. If you need to monitor the same collection of sub-network devices, you can specify private network properties, as required.

You can add one or more network devices using the Devices Management dashboard, and select desired agents (monitoring locations). Use this dashboard to gain an understanding of the complexity of your monitored environment and to review any alarms associated with the monitored devices.



For complete details about the views appearing on this dashboard, see Net Monitor Devices Management views.

***To explore the collection of monitored network devices:***

1 Log in to the Foglight browser interface.

2 On the navigation panel, under **Dashboards**, click **Infrastructure > NetMonitor > Devices Management**.

The Devices Management dashboard appears in the display area.

For more information, see the following topics:

- Expanding your collection of monitored network devices
- Removing network devices from the existing collection
- Viewing and editing individual network device details

# Expanding your collection of monitored network devices

The Devices Management dashboard allows you to expand your collection of monitored network devices by adding new devices to the list. Adding a new network device prompts the Net Monitor Agent to start collecting information about it in the next collection period.

This assumes that you already have the agent package deployed to the Foglight Agent Manager host, and one or more active Net Monitor Agent instances are in place. For complete information on how to deploy an agent package, and how to create and activate agent instances, see the *Administration and Configuration Help*.

***To start monitoring a network device:***

1   On the Devices Management dashboard, click **Add**.

    The **Add Device(s)** dialog box appears.

2    In the **Add Device(s)** dialog box, provide information about the network device that you want to monitor.

- **Device(s) Name**: Type the names of one or more network devices that you want to monitor. This can be a host name or a host IP address. If a host name is specified, Foglight Net Monitor resolves it using DNS.

- **Above devices belong to a private network of**: If the hosts on which these devices are installed belong to a private network, select this check box and type the network name.

    **i** | **NOTE:** Devices belonging to a private network should be monitored from one monitoring location (agent) only. You should specify only one location per monitored device in that case.

- **Expected Response Time**. Specify the expected amount of round-trip response time in milliseconds between the monitored location and the network device.

- **Trace Route (Enable)**: Select this check box if you want to trace the route from the monitoring station to the device. If you do not select this option, you can execute a trace route in real time on the Trace Route page. For more information, see Tracing data packets between monitoring locations and network devices.

- **Monitor by**: Specify one or more rules for collecting information about the monitored devices.

    **Location**: Select the host from which you want to collect information about the monitored devices.

    **i** | **TIP:** The list of all running Net Monitor Agent instances is available for selection in the Location box.

    To add a new monitoring host, you must first create a Net Monitor Agent instance on that host, activate it, and start its data collection. To do that, click **Create new agent**. For more information about creating and activating agent instances and starting their data collection, see the *Administration and Configuration Help*.

    **Interval**: Specify the collection interval for this device. The values in the list reflect the data collection intervals that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with collection intervals of 10 and 15 minutes, these intervals appear in the list.

    **Mode**: Specify the collection mode that you want to use for this device. The values in the list reflect the collection modes that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with one running in *Quick Check* mode, and another in *Normal* mode, both collection modes appear in the list.

**i** | **TIP:** Quick Check mode verifies whether a device is alive; it does not instruct the agent to collect data unless it fails to detect the devices you have told it to monitor. Use Quick Check mode when you want to frequently verify that devices are up and running.

Normal Check mode collects data from the device during the specified collection intervals. This mode allows the agent to send the specified packet size and number of packets to collect and can use trace route to collect paths from one location to the monitored device, when the trace route option is enabled. Quick Check mode just sends packets with specific packet size and does not use trace route. When an agent is run in Quick Check mode, the agent can monitor more devices than in Normal Check mode. If you just want to monitor the device availability and are not interested in the device performance statistics, use Quick Check mode instead of Normal mode.

Click ⊕ Add to add the selected monitoring location to the table. If you want to collect information about the specified devices from a different location, or using a different mode or interval, you can specify additional monitoring locations.

To look for a specific location, you can filter the list using the **Search** box.

| Monitor Location | Monitor Interval | Monitor Mode | |
|---|---|---|---|
| Host1 | 10 minutes | Normal Check | ⊖ |
| Host2 | 10 minutes | Normal Check | ⊖ |

- **Advanced Settings**: To specify advanced settings such as the device name override, the number of packets to ping, the packet size when pinging, ping timeout, or trace route timeout, click **Advanced Settings** and override the default values, as required.

| Advanced Setting | | | × |
|---|---|---|---|
| Device Name Override(Optional): | | | |
| Ping Number of Packets: | 3 | | |
| Ping Packet Size: | 512 | Byte | |
| Ping Timeout: | 30000 | ms | |
| Trace Route Timeout: | 180 | Second | |
| | | Save | Cancel |

**Device Name Override (Optional)**: Type the device name override, as required. Device name override can be used if you monitor two network devices that share an IP address. You can override the name of one of those devices to identify it. If specified, the device override name appears as that device's name in the browser interface. Another reason why you might need to override a device name is when a device is a host object in the Management Server. In that case, if you do not override the device name, its status reflects the host object status, instead of the device status.

**Ping Number of Packets**: Type the number of ICMP (Internet Control Message Protocol) or UDP (Universal Datagram Protocol) packets to send to the device.

**Ping Packet Size**: Type the size of the data portion of the packet in bytes.

**Trace Route Timeout**: Type the amount of time in seconds after which a route trace times out.

When done, click **Save** in the **Advanced Settings** dialog box.

3  In the **Add Device(s)** dialog box, click **Save**.

The **Add Device(s)** dialog box closes, and the Devices Management dashboard refreshes, showing the newly added device in the list.

# Removing network devices from the existing collection

The Devices Management dashboard allows you to remove network devices from the existing collection of monitored devices. Removing a device from the list causes the Net Monitor Agent to stop collecting information about that device. The data previously collected from a removed device is kept in the Foglight database in accordance with the existing persistence settings. For more information about persistence policies, refer to the *Administration and Configuration Help*.

***To stop monitoring a network device:***

1   On the Devices Management dashboard, select the network device that you no longer want to monitor, and click **Delete**.

   The **Confirm** message box appears.
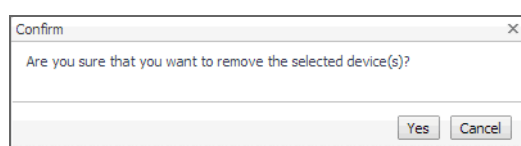
   

2   Click **Yes** to confirm the removal and close the message box.

   A message box appears, indicating that the operation is complete.

3   Click **OK** to close it.

4   In the Devices Management dashboard, review the list of monitored devices.

   The newly removed network device no longer appears in the list.


# Viewing and editing individual network device details

You can view and edit the monitoring settings associated with individual network devices, when required. For example, you can start monitoring a network device using a different host, or change the data collection periods for specific locations.

***To view and edit network device details:***

1   On the Devices Management dashboard, in the row containing the network device whose settings you want to review, in the Edit column, click Edit ✐.

   The **Edit Device** dialog box appears.

2    In the **Edit Device** dialog box, review the device settings, and make any changes, as required.

- **Device Name**: Type the names of one or more network devices that you want to monitor. This can be a host name or a host IP address. If a host name is specified, Foglight Net Monitor resolves it using DNS.

- **Above devices belong to a private network of**: If the hosts on which these devices are installed belong to a private network, select this check box and type the network name.

  > ℹ | **NOTE:** Devices belonging to a private network should be monitored from one monitoring
  >     location (agent) only. You should specify only one location per monitored device in that case.

- **Expected Response Time**. Specify the expected amount of round-trip response time in milliseconds between the monitored location and the network device.

- **Trace Route (Enable)**: Select this check box if you want to trace the route from the monitor station to the device. If you do not select this option, you can execute a trace route in real time on the Trace Route page. For more information, see Tracing data packets between monitoring locations and network devices.

- **Monitor by**: Specify one or more rules for collecting information about the monitored devices.

  **Location**: Select the host from which you want to collect information about the monitored devices.

  > ℹ | **TIP:** The list of all running Net Monitor Agent instances is available for selection in the
  >     **Location** box.

  To add a new monitoring host, you must first create a Net Monitor Agent instance on that host, activate it, and start its data collection. To do that, click **Create new agent**. For more information about creating and activating agent instances and starting their data collection, see the *Administration and Configuration Help*.

  **Interval**: Specify the collection interval for this device. The values in the list reflect the data collection intervals that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with the collection intervals of 10 and 15 minutes, these intervals appear in the list.
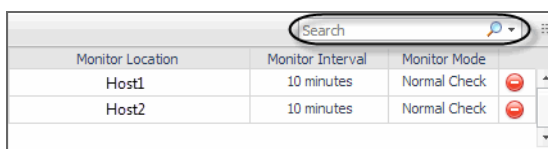
  **Mode**: Specify the collection mode that you want to use for this device. The values in the list reflect the collection modes that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with one running in *Quick Check* mode, and another in *Normal* mode, both collection modes appear in the list.

**i** | **TIP:** Quick Check mode verifies whether a device is alive; it does not instruct the agent to collect data unless it fails to detect the devices you have told it to monitor. Use Quick Check mode when you want to frequently verify that devices are up and running.

Normal Check mode collects data from the device during the specified collection intervals. This mode allows the agent to send the specified packet size and number of packets to collect and can use trace route to collect paths from one location to the monitored device, when the trace route option is enabled. Quick Check mode just sends a fixed number of small-size packets and does not use trace route. When an agent is run in Quick Check mode, the agent can monitor more devices than in Normal Check mode. If you just want to monitor the device availability and are not interested in the device performance statistics, use Quick Check mode instead of Normal mode.

Click ⊕ Add to add the selected monitoring location to the table. If you want to collect information about the specified devices from a different location, or using a different mode or interval, you can specify additional monitoring locations.

To look for a specific location, you can filter the list using the **Search** box.

| Monitor Location | Monitor Interval | Monitor Mode | |
|---|---|---|---|
| Host1 | 10 minutes | Normal Check | ⊖ |
| Host2 | 10 minutes | Normal Check | ⊖ |

- **Advanced Settings**: To specify advanced settings such as the device name override, the number of packets to ping, the packet size when pinging, ping timeout, or trace route timeout, click **Advanced Settings** and override the default values, as required.

Advanced Setting ×

| | |
|---|---|
| Device Name Override(Optional): | |
| Ping Number of Packets: | 3 |
| Ping Packet Size: | 512 Byte |
| Ping Timeout: | 30000 ms |
| Trace Route Timeout: | 180 Second |

Save  Cancel

**Device Name Override (Optional)**: Type the device name override, as required. Device name override can be used if you monitor two network devices that share an IP address. You can override the name of one of those devices to identify it. If specified, the device override name appears as that device's name in the browser interface. Another reason why you might need to override a device name is when a device is a host object in the Management Server. In that case, if you do not override the device name, its status reflects the host object status, instead of the device status.

**Ping Number of Packets**: Type the number of ICMP (Internet Control Message Protocol) or UDP (Universal Datagram Protocol) packets to send to the device.

**Ping Packet Size**: Type the size of the data portion of the packet in bytes.

**Trace Route Timeout**: Type the amount of time in seconds after which a route trace times out.

When done, click **Save** in the **Advanced Settings** dialog box.

3   In the **Edit Device** dialog box, click **Save**.

# Investigating the performance of network devices

A typical monitored environment includes a set of monitored network devices and Net Monitor Agents that collect data about these devices. These components are displayed on the Performance Browser dashboard. Use this dashboard to see the state of individual network devices when monitored from one or multiple locations.
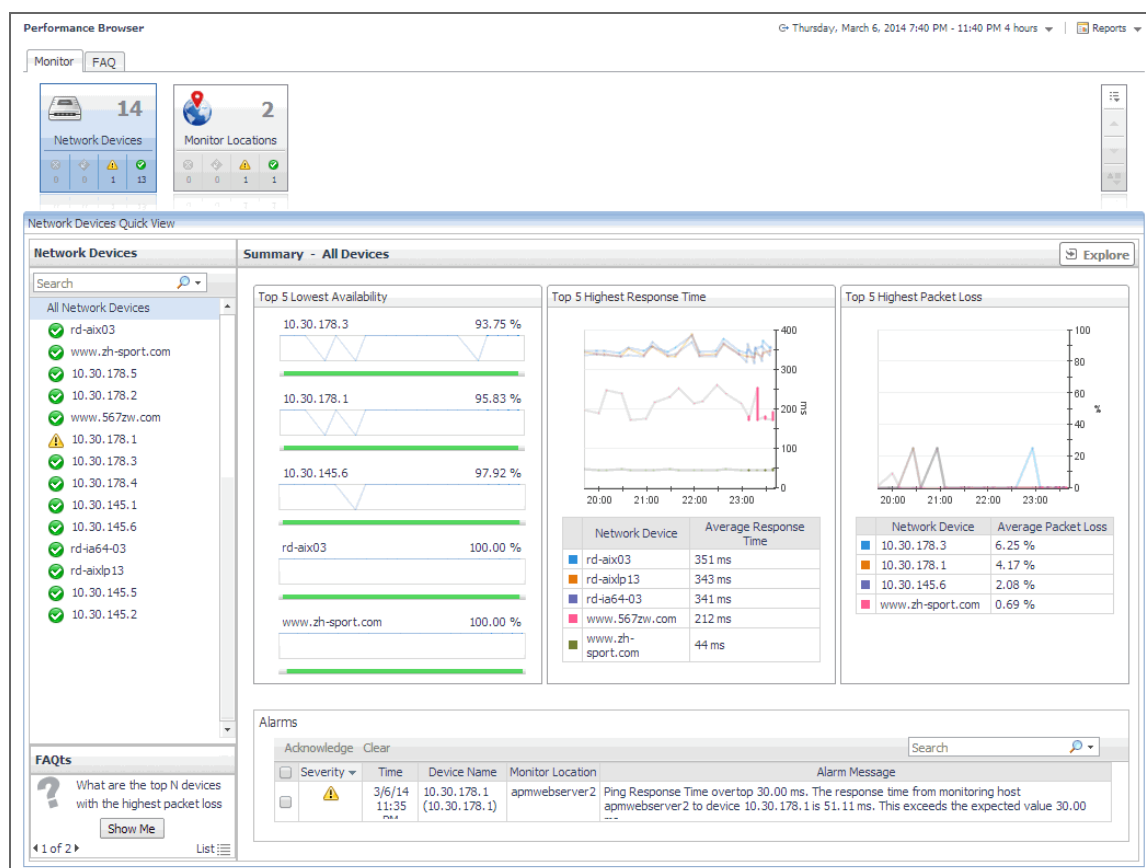


You can access this dashboard from the navigation panel. Under **Dashboards**, click **Infrastructure > NetMonitor > Performance Browser**.

When you navigate to the Performance Browser for the first time, the **Monitoring** tab appears open. This tab provides an overall summary of your monitored network devices.

> **i** | **TIP:** In addition to the Monitoring tab, the Performance Browser also offers the FAQ tab. For more information, see Exploring the FAQ tab.

Start by indicating the type of objects that you want to investigate. To do that, select the appropriate tile at the top of the **Monitoring** tab: **Network Devices** or **Monitor Locations**. This causes the Quick View to display information about the selected objects. Next, select an object or group of objects in the Quick View, such as **All Network Devices** or **All Monitor Locations**, to display additional information about that selection.
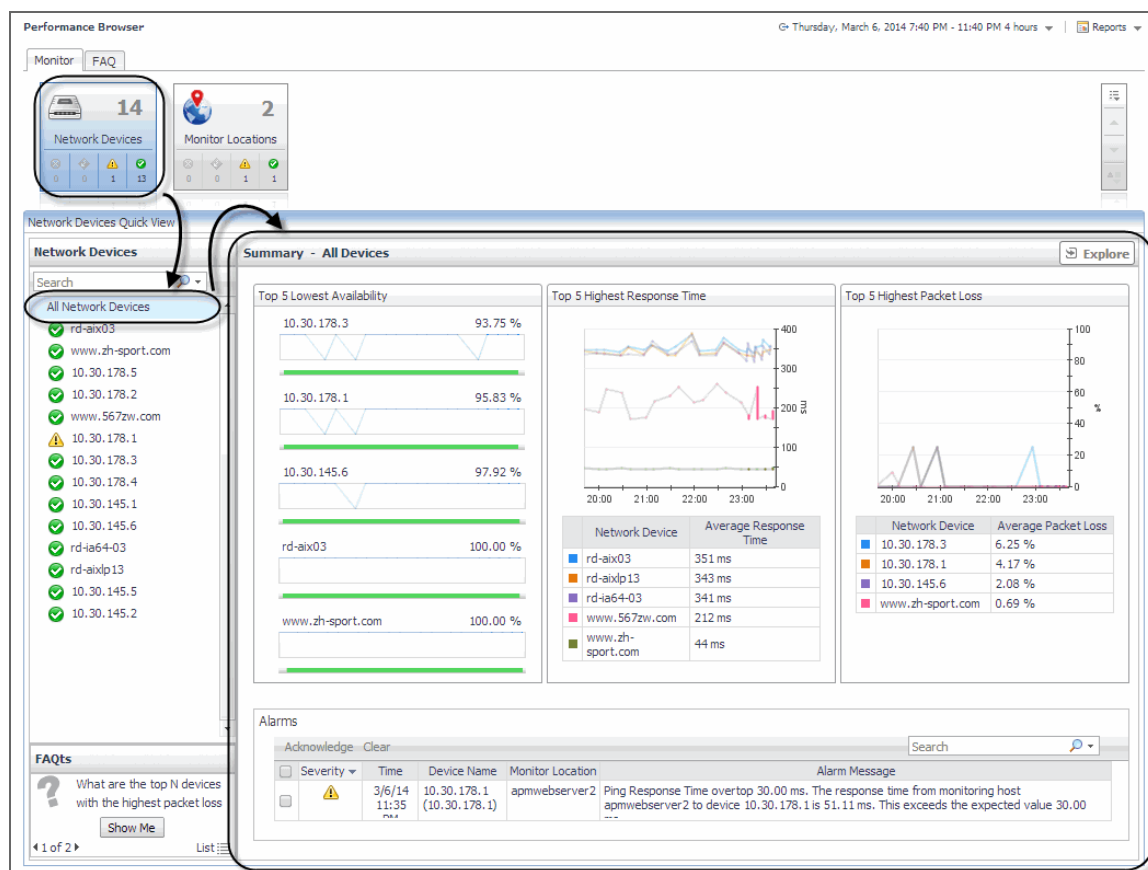
For complete details about the views appearing on this dashboard, see Net Monitor Performance Browser views.

For more information, see the following topics:

- Exploring individual network devices
- Tracing data packets between monitoring locations and network devices
- Exploring the FAQ tab

# Exploring individual network devices

When you select a network device in the **Summary - All Devices** view, you can see additional information, such as response times and packet loss values, in the **Device Detail** view. High levels of these indicators typically point to network congestion, and may require additional investigation.
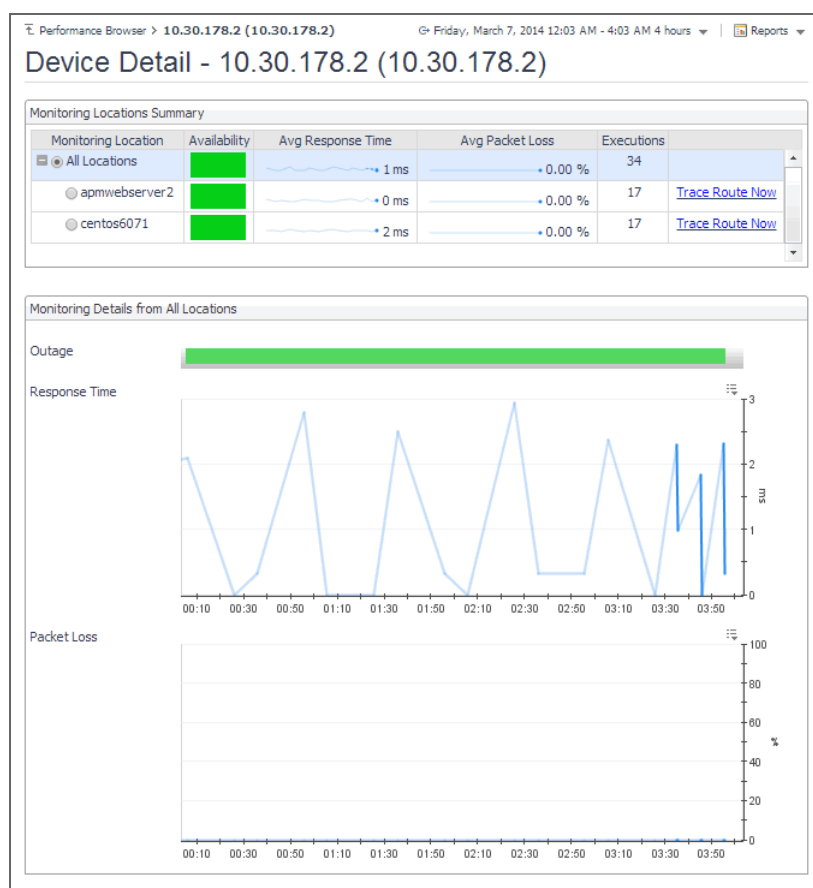
For complete details about the data appearing on this view, see Device Detail view.

***To drill down on a network device:***

1  On the Performance Browser dashboard, select the **Network Devices** tile.

2  In the **Network Devices Quick View**, in the **Network Devices** panel on the left, select a network device.

3  In the **Summary - Single Device Summary** on the right, click **Explore**.

The **Device Detail** view appears in the display area.

# Tracing data packets between monitoring locations and network devices

When you monitor a network device from a monitoring location, the monitoring agent sends a configured number of data packets to the device. The complete path of each data packet, from the monitoring location to the network device, represents a route. On the way to its destination, a data packet often runs through a number of other devices, so the route consists of one or more *hops*, where each device it passes through is counted as one hop.

The **Trace Result** view allows you to trace a route between a monitoring location and a network device, and review the time a data packet spends at each individual hop. This can help you investigate signs of performance degradation. For example, if your system reports higher than usual response times and frequent time-outs, you can trace the route of data packets to determine what is causing the bottlenecks.

Another example is when a device ping times out, this may be related to a possible wrong network route which can be seen on this page. For instance, if the expected trace route consists of ten hops, but the trace route in the chart appears to consist of five hops, you can identify the IP address associated with the broken hop in the chart. This can help you to quickly identify the root cause of a broken network.
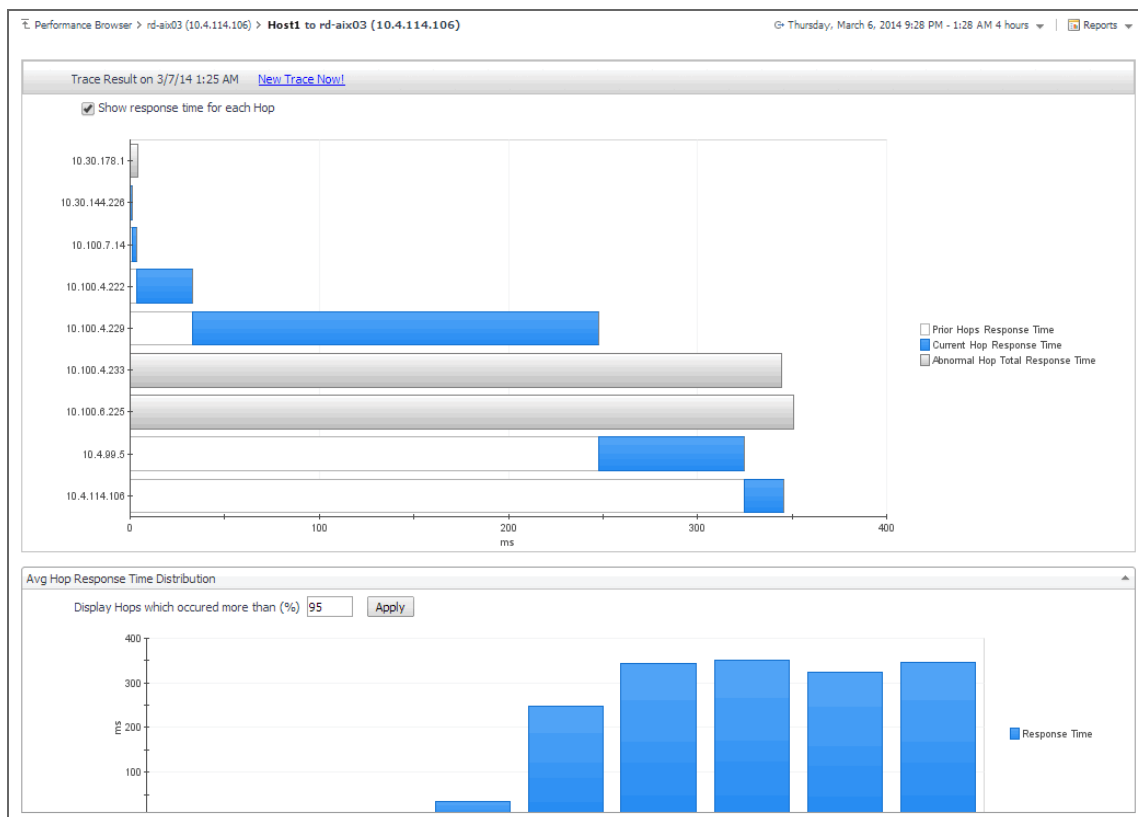
For complete details about the data appearing on this view, see Trace Result view.

***To trace a data packet route:***

1 On the Performance Browser dashboard, select the **Network Devices** tile.

2 In the **Network Devices Quick View**, in the **Network Devices** panel on the left, select a network device.

3 In the **Summary - Single Device Summary** on the right, click **Explore**.

4 On the Device Detail dashboard, in the **Monitoring Locations Summary** view, in the row containing the monitoring host from which data packets are sent to the device, click **Trace Route Now**.

The **Trace Result** view appears in the display area.

The trace route request runs in the background and takes several minutes to complete. Instead of waiting for it to complete, you can navigate to other dashboards, and then return to this page to review the trace route.

> **i** | **IMPORTANT:** If the trace route option is disabled in the device settings (see Viewing and editing individual network device details), this page is not populated with data. You can quickly execute a trace route in real time on this page by clicking Trace Route Now.

# Exploring the FAQ tab

The **FAQ** tab available on the Performance Browser allows you to look at frequently asked questions about your monitored devices and review the answers. The **Categories** view shows several question categories. Selecting a category shows the questions belonging to that category in the **Questions** pane. From there, clicking a question shows the answer on the right.
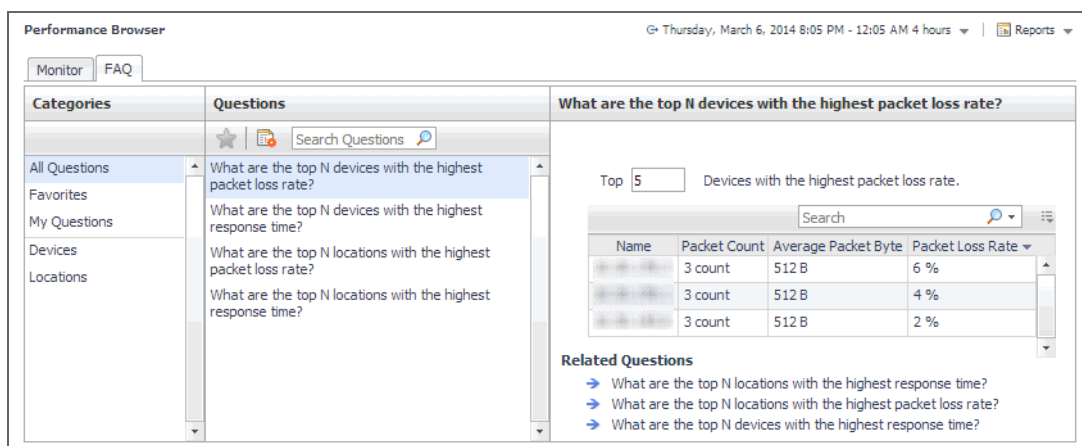
# Generating reports

Foglight Net Monitor supports the report generation ability. This allows you to create reports using a set of predefined templates to report on the various aspects of your monitored environment. Foglight Net Monitor includes a collection of predefined report templates.

You can generate, copy, and edit reports using the Reports dashboard included with the Foglight Management Server. For more information about this dashboard, see the *Foglight User Help*.

## Report templates

**Table 2. Predefined report templates**

| Report Template | Description |
|---|---|
| **All Device Daily Outage Report** | Shows network device availability over the specified time range, per monitoring location. |
| **All Device Summary Report** | Shows network device performance statistics over the specified time range, per monitoring location. The statistics include the device availability, average response time, average packet loss, hop count, and the number of executions. |
| **Single Device Report** | Shows the performance details for a selected network device during the specified time range, per monitoring location. The statistics include the monitoring host availability, average response time, average packet loss, hop count, and the number of executions. It also provides trace route summary details for each host. |

# Configuring the agent properties

The Net Monitor Agent collects data about monitored network devices and sends it to the Management Server. Monitoring agents keep track of resource utilization metrics and alert you when certain pre-defined thresholds are reached.

When an agent connects to Foglight, it is provided with sets of properties that it uses to configure its correct running state. Each agent is provided with a combination of two types of properties: agent properties and shareable properties.

Default versions of these properties are installed with Foglight for Net Monitor. However, you can edit the default shareable and agent properties, configure agent properties that apply only to a specific agent instance, and create edited clones of shareable properties that are used by a subset of agents of a certain type.

For complete information about working with agent properties, see the *Administration and Configuration Help.*

***To configure agent properties:***

1   Log in to the Foglight browser interface.

2   Ensure that the navigation panel is open.

    To open the navigation panel, click the right-facing arrow on the left.

3   Open the Agent Status dashboard and navigate to the agent properties.

    a   On the navigation panel, under **Dashboards**, choose **Administration > Agents > Agent Status**.

    > **i** | **IMPORTANT:** Another way of editing agent properties is through the Agent Properties dashboard. The properties you specify on this dashboard apply to all instances of the selected agent type, excluding any of the existing agents. To be certain that you are editing the properties of a particular agent instance and to prevent overwriting of properties of another agent instance, use the Agent Status dashboard instead of the Agent Properties dashboard.

    b   On the Agent Status dashboard, select the instance of the Net Monitor Agent whose properties you want to modify and click **Edit Properties**.

    c   Indicate that you want to edit the properties of the selected agent instance.

        A list of agent properties appears in the display area.

# Configuring Net Monitor agent properties

When you first install Foglight Net Monitor, you must deploy the Net Monitor Agent package on one or more hosts (monitoring locations). Then, create new agent instances, and set the running mode on those instances (Quick Check mode or Normal mode), and data collection intervals using the Net Monitor Agent properties.

Next, activate the agent instances, and start the data collection. If you monitor the same collection of sub-network devices, you can specify private network properties, as required. The Net Monitor Agent includes the following groups of agent properties that control its behavior:

• NetMonitor Devices Settings

• Data Collection Scheduler

When you finish configuring the Net Monitor Agent instances and their agent properties, you can specify the network devices that you want to monitor, and associate them with appropriate monitoring agents, as required. This can be done using the Devices Management dashboard. For more information about this dashboard, see Managing Monitored Network Devices.

## NetMonitor Devices Settings

The **Settings** properties specify the collection mode, any private networks to which the monitored network devices belong, and identify the monitored network devices.

- **Run Quick Check Mode**: Quick Check is a utility included with the Net Monitor Agent. It verifies whether a device is alive. It instructs the agent to collect data only if it fails to detect the devices that the agent is configured to monitor. Use Quick Check mode when you want to verify that devices are up and running.

  If Quick Check detects the devices in the currently monitored list, Foglight continues to collect data according to the sample frequency. However, if it fails to detect the devices, it immediately initiates a data collection cycle and triggers the *Network Device Not Found* rule which sends an email to the system administrator.

  To have the agent run in Quick Check mode, select **True**.

- **Private Network Config Item**: A list identifying private networks to which the monitored network devices belong, if applicable. Each entry in the list includes the following columns:

  - **Private network ID**: The ID of the private network.

  - **Private Ip Pattern**: An expression representing the pattern of the private network IP. This property is used in combination with the network ID. Any IP addresses that match the specified pattern are in same network. For example, if the network ID is `private network 1` and the IP pattern is `10.30.178.1-10.30.178.254`, the agent monitors all devices in `private network 1` that are in the `10.30.178.1-10.30.178.254` range.

    Examples of private IP pattern ranges include:

    ```
    192.168.0.1-192.168.0.254
    192.168.0.1-192.168.0.254, 192.168.1.1-192.168.1.254
    ```

- **Device Item**: A list identifying the devices monitored by the agent instance. Each entry in the list includes the following columns:

  > **i** | **IMPORTANT:** Do not use this list to specify monitored devices. Instead, use the Devices Management dashboard. For more information about this dashboard, see Managing monitored network devices.

  - **Device name**: The name of the monitored network device.

  - **Device's network ID**: The ID of the network associated with the network device. Configure this property if you want the agent to monitor more than one device with the same IP address but with different network IDs.

  - **Device Type**: The type of the network device: **Host** (if the device is used by a host system), or **Other** (if the device is used by a different machine type, such as a printer).

  - **Device name override**: The device name override, if applicable.

  - **Ping Timeout (Milliseconds)**: The amount of time in milliseconds after which a ping request times out.

  - **Trace Route?**: Select if you want to trace routes to this network device.

  - **Trace Route Timeout (Seconds)**: Type the amount of time in seconds after which a route trace times out.

  - **Number of Packets**: The number of ICMP (Internet Control Message Protocol) or UDP (Universal Datagram Protocol) packets to send to monitored network devices.

  - **Data Size (Bytes)**: The size of the data portion of the packet in bytes.

  - **Expected Response Time (Milliseconds)**: The expected amount of round-trip response time in milliseconds between the monitoring location and monitored network devices.

# Data Collection Scheduler

The **Data Collection Scheduler** agent properties specify the data frequency settings that the Net Monitor Agent uses to collect metrics from the monitored websites.

- **Collector Config**: A list containing the data collectors the agent uses. Each entry in the list includes the following columns:

    - **Collector Name**: The name of the collector the uses to gather data.

    - **Default Collection Interval**: The number of milliseconds, seconds, minutes, hours, or days during which the Net Monitor Agent collects data.

    - **Time Unit**: The time unit associated with the **Default Collection Interval**: **milliseconds**, **seconds**, **minutes**, **hours**, or **days**.

    - **Fast-Mode Collection Interval**: The number of milliseconds, seconds, minutes, hours, or days during which the Net Monitor Agent collects data when working in the fast collection mode.

    - **Fast-Mode Time Unit**: The time unit associated with the **Fast-Mode Collection Interval**: **milliseconds**, **seconds**, **minutes**, **hours**, or **days**.

    - **Fast-Mode Max Count**: The maximum number of the times the Net Monitor Agent can stay in fast collection mode.

# View reference

Foglight displays monitoring data in views that group, format, and display data. The main types are described below.

Dashboards are top-level views that contain lower-level views. The dashboards supplied with Foglight, as well as those created by users, are accessible from the navigation panel.

Lower-level views in Foglight can be added to dashboards or can be accessed by drilling down from a dashboard. They receive and display data directly from the Management Server or from other views. Some views filter or select data that appears in other views in the same dashboard. Some are tree views with expandable nodes for selecting servers, applications, or data.

Foglight Net Monitor ships with several dashboards that allow you to monitor and configure your monitored environment. Each of these dashboards contains a number of views. This section describes these views in more detail. For more information about the available dashboards, see Managing monitored network devices and Investigating the performance of network devices.

This cartridge includes the following groups of views:

- Net Monitor Devices Management views

- Net Monitor Performance Browser views

# Net Monitor Devices Management views

The Devices Management dashboard contains the following views:

- Agent Alarms view

- Devices Management table

## Agent Alarms view

### Purpose

The **Agent Alarms** view displays the alarms generated against the existing agents.

## How to get here

On the Devices Management dashboard, this view appears just below the Devices Management table.

## Description of the View

**Table 3. Agent Alarms view**

| | |
|---|---|
| **Description** | Lists the alarms generated against the monitored locations.<br><br>**NOTE:** To acknowledge or clear one or more alarms appearing in this table, select them and click **Acknowledge** or **Clear**, as required. For more information about alarms in Foglight, see the *Foglight User Guide*. |
| **Data displayed** | • **Ack'ed**. Indicates if the alarm is acknowledged: `true` or `false`.<br>• **Device Name**. The name of the device against which the alarm is generated, as configured on the Devices Management dashboard. For more information, see Managing monitored network devices.<br>• **Severity**. Indicates the alarm severity: Warning ⚠, Critical ◈, or Fatal ⊗.<br>• **Time**. The date and time when the alarm is generated.<br>• **Alarm Message**. The alarm message. |
| **Where to go next** | Drill down on:<br>• **Any row**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms in Foglight, see the *Foglight User Help*.<br><br> |

## Devices Management table

## Purpose

The **Devices Management** view displays the monitored network devices.

## How to get here

On the Devices Management dashboard, this view appears just above the Agent Alarms view.

## Description of the View

**Table 4. Devices Management view**

| | |
|---|---|
| **Data displayed** | • **Device Name Override**. The device name override, if one is specified.<br>• **Device Name**. The name of the monitored device.<br>• **Device Status**. The state of the highest severity alarm raised against the network device: Warning ⚠, Critical ◆, or Fatal ⊗.<br>• **Expected Response Time**. The expected round-trip response time between the host on which the Net Monitor Agent is installed and the network device.<br>• **Monitor Location**. A color-coded indicator of the data collection state for each location from which this network device is monitored. Green indicates Normal, yellow Warning, orange Critical, and red the Fatal state.<br>• **NetworkID**. The ID of the private network to which the network device belongs, if applicable.<br>• **Trace Route?**. Indicates if the route from the monitoring agent to the network device is traced. |

# Net Monitor Performance Browser views

The Performance Browser contains the following views:

- Alarms view
- Device Detail view
- FAQ tab
- FAQts view
- Net Monitor Environment view
- Network Devices view
- Monitor tab
- Monitor Locations view
- Quick View
- Single Location Summary view

# Alarms view

## Purpose

The **Alarms** view lists the alarms generated against the selected object or group of objects in the Quick View.

> **i** | **TIP:** To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear, as required. For more information about alarms in Foglight, see the Foglight User Guide.

| Alarms | | | | |
|---|---|---|---|---|
| Acknowledge Clear | | | | Search |
| ☐ Severity ▼ | Time | Device Name | Monitor Location | Alarm Message |
| ☐ ⚠ | 3/10/14 10:40 PM | 10.30.178.3 (10.30.178.3) | Host1 | Device is unavailable. Network device 10.30.178.3 is not reachable from Host1 |
| ☐ ⚠ | 3/10/14 10:40 PM | 10.30.178.1 (10.30.178.1) | Host1 | Device is unavailable. Network device 10.30.178.1 is not reachable from Host1 |
| ☐ ⚠ | 3/10/14 10:40 PM | 10.30.178.5 (10.30.178.5) | Host1 | Device is unavailable. Network device 10.30.178.5 is not reachable from Host1 |

## How to get here

1. Navigate to the Performance Browser.

2. On the Monitor tab, in the Net Monitor Environment view, select the **Network Devices** or **Locations** tile.

3. In the Quick View, in the panel on the left, select **All Network Devices**, a network device, or a monitoring location.

   The **Alarms** view appears at the bottom of the panel on the right.

## Description of the view

**Table 5. Alarms view**

| | |
|---|---|
| | • **Alarm Message**. The alarm message, explaining the reason for this alarm. |
| | • **Device Name**. The name of the monitored device against which the alarm is generated. |
| **Data displayed** | • **Monitor Location**. The name of the host running the instance of the Net Monitor Agent that monitors this device. |
| | • **Severity**. Indicates the alarm severity: Warning ⚠, Critical ◆, or Fatal ⊗. |
| | • **Time**. The time at which the alarm is generated. |

# Device Detail view

## Purpose

The **Device Detail** view provides details about the selected network device. Use it to find out the average response times of this device from different monitoring locations, and to review its overall health.
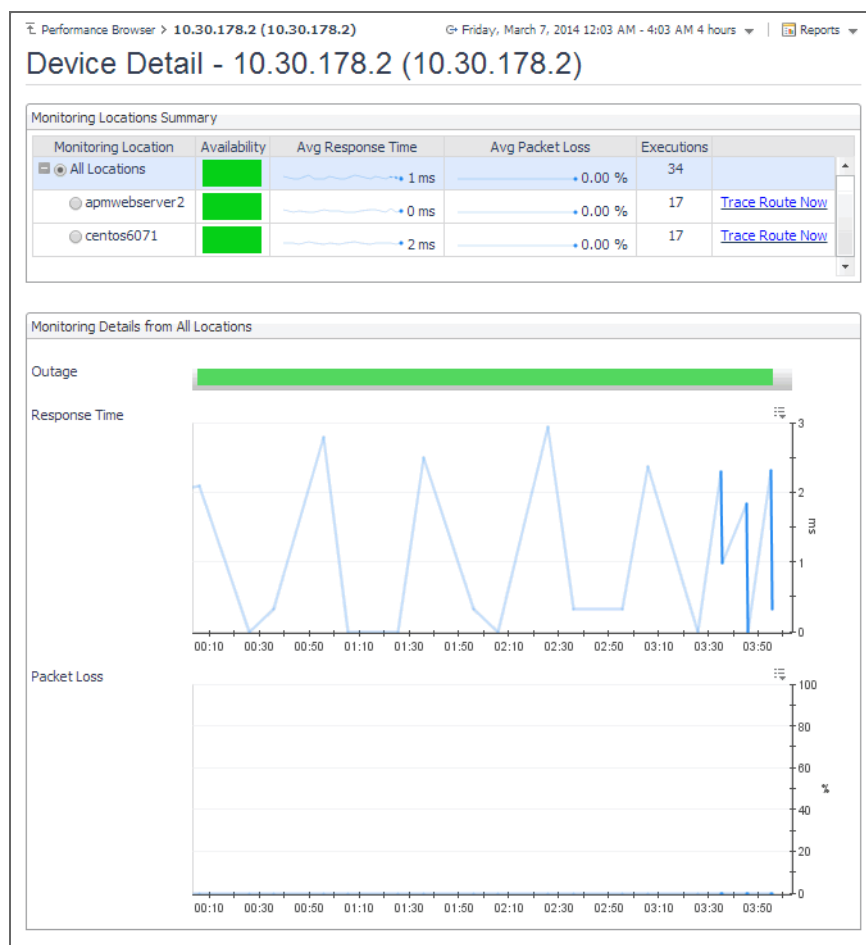
## How to get here

1. Navigate to the Performance Browser.

2. On the Monitor tab, in the Net Monitor Environment view, select the **Network Devices** tile.

3. In the Quick View, in the Network Devices view, select a network device.

4. In the Summary - Single Device Summary view, click **Explore**.

   The **Device Detail** view appears in the display area.

## Description of embedded views

This view is made up of the following embedded views:

- Monitoring Locations Summary
- Monitoring Details from All Locations

## Monitoring Locations Summary

**Table 6. Monitoring Locations Summary view**

| Description | Lists the hosts from which the selected network device is monitored. |
| --- | --- |
| **Data displayed** | • **Availability**. A color-coded bar, representing the availability of the device over the selected time range. The color of the bar changes depending on the alarm state. Red indicates the Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.<br>• **Avg Packet Loss**. The average percentage of time the data packets sent to the monitored device are not echoed back. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.<br>• **Avg Response Time**. The average round-trip response time between the monitoring agent and the network device.<br>• **Executions**. The number of times the Net Monitor Agent sends data packets to the selected network device.<br>• **Monitoring Location**. The name of the host from which the selected network device is monitored. |
| **Where to go next** | Drill down on:<br>**Trace Route Now**. For more information, see Trace Result view. |

## Monitoring Details from All Locations

**Table 7. Monitoring Details from All Locations view**

| Description | Shows how well the selected network device is responding to the data collection requests from all of the monitoring locations. |
| --- | --- |
| **Data displayed** | • **Outage**. A color-coded bar, representing the availability of the monitored network device over the selected time range. The color of the bar reflects the percentage of time the device is unresponsive.<br>• **Packet Loss**. The percentage of time the data packets sent to the monitored device are not echoed back, over the selected time range. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.<br>• **Response Time**. The round-trip response time between the monitoring agent and the network device, over the selected time range. |

# FAQ tab

## Purpose

The **FAQ** tab shows answers to common questions related to your network devices or monitoring locations.
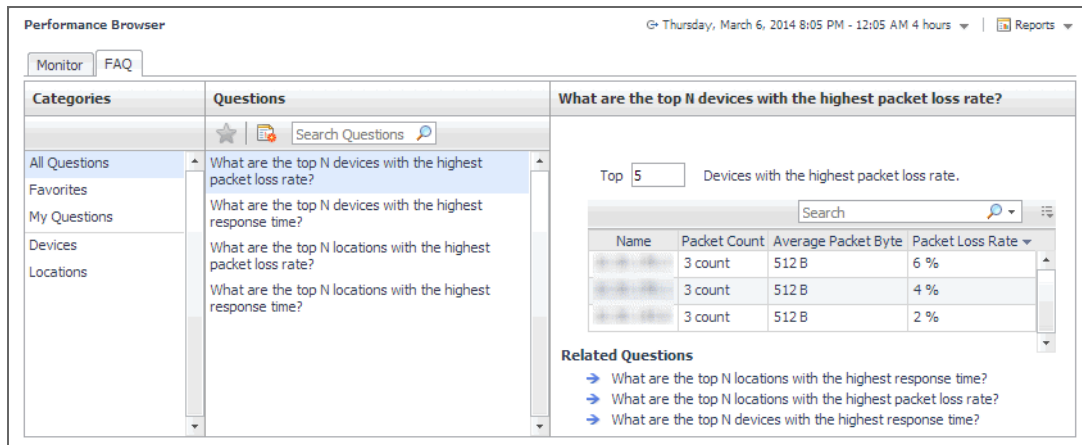
## How to get here

Navigate to the Performance Browser, and open the **FAQts** tab.

## Description of embedded views

This view is made up of the following embedded views:

- Answer
- Categories
- Questions

## Answer

This view provides an answer to the question selected in the Questions view. The answer appears in the following form:

**Top** *x* *<objects of category>...*

Where *x* is the number of objects of the category you provided in the Categories view.

Specify *x* by entering a number.

## Categories

This view lists the categories for which questions can be answered for you by Foglight.

Click a category in the list to select it.

## Questions

This view lists the questions, for the category selected in the Categories, that can be answered for you by Foglight.

Click a question in the list to select it.

If the list of questions is long and you want to narrow it down, search for a particular text string using the **Search Questions** box.

# FAQts view

## Purpose

The **FAQts** view shows answers to common questions related to your transactions or locations. The collection of available questions depends on the tile selected in the Net Monitor Environment view. If you select the **Network**

**Devices** tile, this view displays the questions related to the monitored network devices. Selecting the **Monitor Locations** tile causes the view to display the questions related to your monitoring locations.
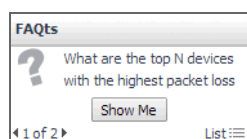


### How to get here

In the Performance Browser, in the Quick View, the **FAQts** view appears in the bottom-left corner.

# Net Monitor Environment view

### Purpose

The Net Monitor Environment view displays a high-level overview of your monitored environment. The view has two tiles, each representing the monitored objects of interest: **Network Devices** and **Monitor Locations**.
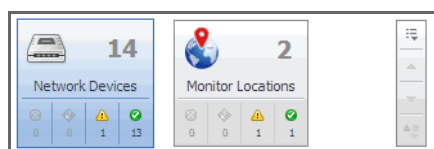


Each tile shows how many of the corresponding object instances there are in your monitored infrastructure, as well as the count of objects of that type in each of the alarm states Normal ✓, Warning ⚠, Critical ◆, or Fatal ✕). For example, the following image shows 14 network devices: none in the Fatal or Critical states, one in Warning, and 13 in the Normal state.

You can move the tiles by dragging and dropping until you achieve the desired layout. To hide one or more tiles, on the tool bar on the right, click ☷, and in the popup that appears, click a tile that you want to hide.
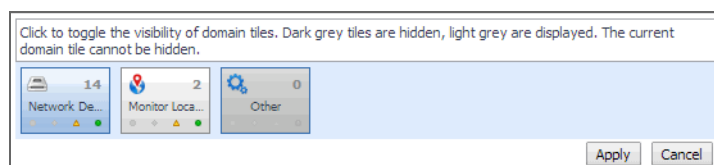


Clicking the object type icon, the object type name, or the object count, shows summary information for that object type in the Quick View. Clicking an alarm state (for example, Warning) on a tile displays summary information in the Quick View for the objects of that type that are in the selected alarm state. If an alarm state has a count of zero, then you can not drill down on the alarm state.

### How to get here

This view appears in the upper part of the Performance Browser, just above the Quick View.

### Description of embedded views

This view is made up of the following embedded views:

- Monitor Locations
- Network Devices

### Monitor Locations

**Table 8. Monitor Locations view**

| Description | Shows the number of locations in your environment from which websites are monitored, and total alarm counts associated with those locations. |
| --- | --- |
| Data displayed | • **Alarm counts**. The total counts of alarms generated against the existing monitoring locations, broken down by alarm types (Normal, Warning, Critical, Fatal).<br>• **Location count**. The number of locations in your environment. |
| Where to go next | Drill down on:<br>• **Alarm counts**. Lists the locations associated with the alarms in the Monitor Locations view, appearing in the Quick View.<br>• **Location count**. Displays a combination of location views in the Quick View. |

## Network Devices

**Table 9. Network Devices view**

| Description | Shows the number of monitored network devices in your environment and total alarm counts associated with them. |
| --- | --- |
| Data displayed | • **Alarm counts**. The total counts of alarms associated with the monitored network devices, broken down by alarm types (Normal, Warning, Critical, Fatal).<br>• **Device count**. The number of monitored network devices in your environment. |
| Where to go next | Drill down on:<br>• **Alarm counts**. Lists the network devices associated with the alarms in the Network Devices view, appearing in the Quick View.<br>• **Device count**. Displays a combination of device views in the Quick View. |

# Network Devices view

The **Network Devices** view lists the monitored network devices and shows their alarm states.

If a device name override is specified, this name appears in the list. If a device belongs to a private network, the private network ID is appended to the device.

Selecting **All Network Devices** shows the overall response and availability information for the monitored devices in the Summary - All Devices view on the right. Similarly, selecting a device in the list shows device-specific metrics in the **Summary - Single Device Summary view** view on the right.

## How to get here

• In the Performance Browser, in the Net Monitor Environment view, select the **Network Devices** tile.

   The Network Devices view appears in the Quick View on the left.

## Description of the view

**Table 10. Network Devices view**

| | |
|---|---|
| **Data displayed** | • **Alarm severity**. The state of the most recent alarm raised against the associated network device: Warning ⚠, Critical ◆, or Fatal ⊗.<br><br>• **All Network Devices**. A parent node for the network device object instances that appear in this view.<br><br>• **Network Device**. The network device name. |
| **Where to go next** | Drill down on:<br><br>• **All Network Devices**. Shows the Summary - All Devices view in the Quick View.<br><br>• **Network Device**. Shows the Summary - Single Device Summary view in the Quick View. |

# Monitor tab

## Purpose

The **Monitor** tab is a container view. This tab displays a combination of location- or device-related information, depending on your selection in the Net Monitor Environment view and the Quick View. Use it to gain an understanding of how well your monitored network devices are performing, and to investigate any potential issues.
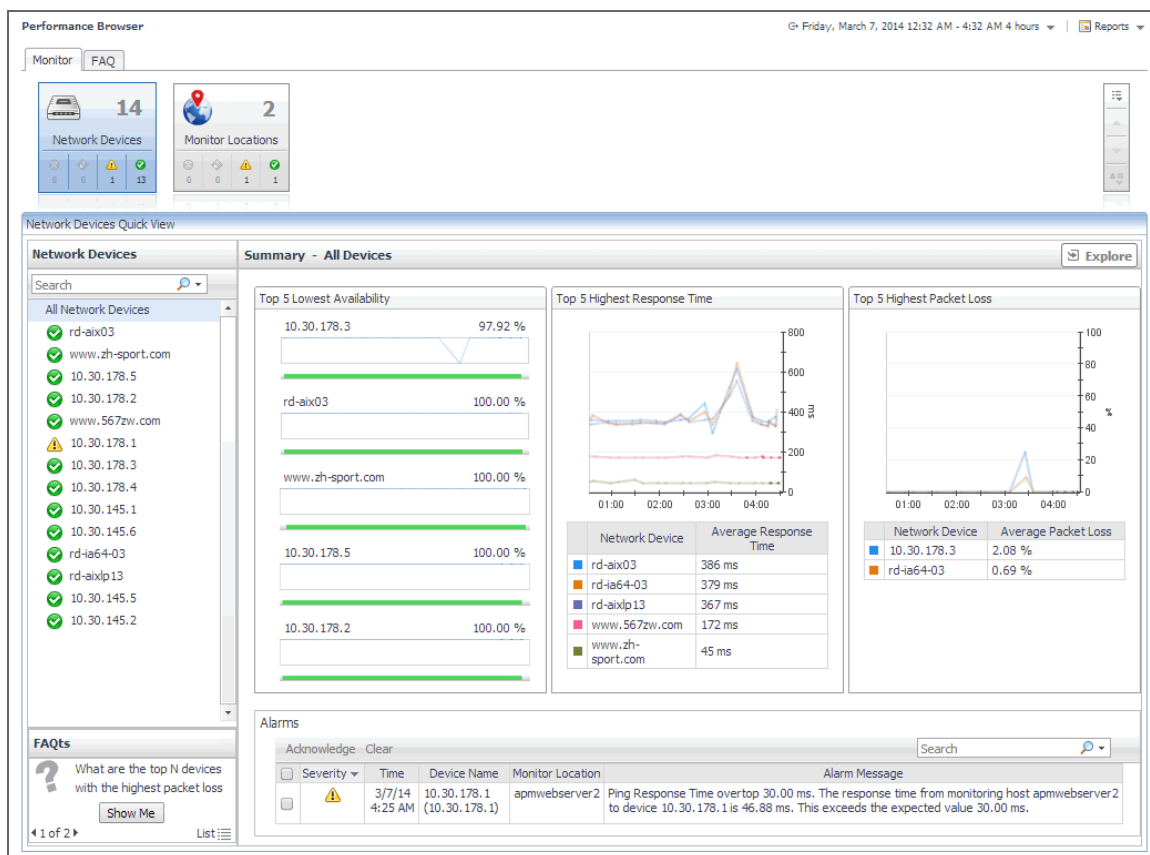


## How to get here

• Navigate to the Performance Browser.

  The **Monitor** tab appears open.

## Embedded views

This view is made up of the following views:

- Net Monitor Environment view
- Quick View

# Monitor Locations view

The **Monitor Locations** view lists the hosts that are running instances of the Net Monitor Agent, and shows their states.
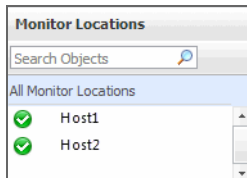


Selecting **All Monitor Locations** shows a list of all host names in the Summary - All Monitor Locations view on the right. Similarly, selecting a location in the list shows location-specific metrics in the **Single Location Summary view** view on the right.

## How to get here

- In the Performance Browser, in the Net Monitor Environment view, select the Monitor **Locations** tile.

  The Monitor Locations view appears in the Quick View on the left.

## Description of the View

**Table 11. Monitor Locations view**

| | |
|---|---|
| **Data displayed** | • **Alarm severity**. The state of the most recent alarm raised against the associated location: Warning ⚠, Critical ◈, or Fatal ⊗. <br> • **All Monitor Locations**. A parent node for the location object instances that appear in this view. <br> • **Location**. The name of the host on which the Net Monitor Agent is running. |
| **Where to go next** | Drill down on: <br> • **All Monitor Locations**. Shows the Summary - All Monitor Locations view in the Quick View. <br> • **Location**. Shows the Single Location Summary view in the Quick View. |

# Quick View

## Purpose

The **Quick View** is a container view. It contains a combination of location or transaction views, depending on your selection in the Net Monitor Environment view and the panel on the left. Use it to understand the performance of the monitored network devices, and to investigate any issues that they may be experiencing.
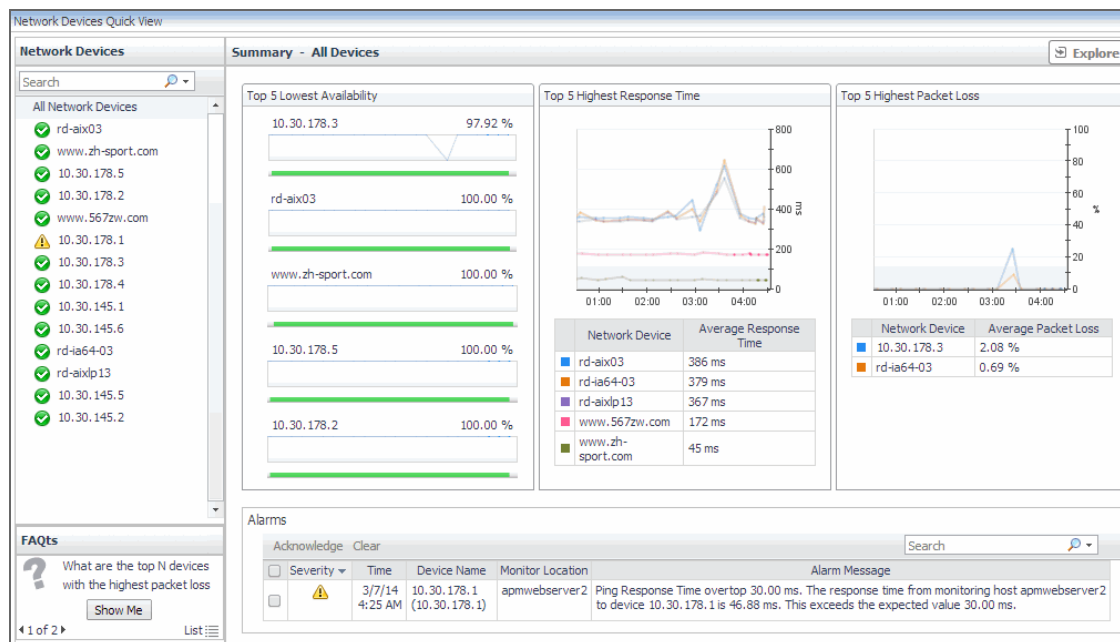
## How to get here

This view appears in the Performance Browser, just below the Net Monitor Environment view.

## Embedded views

This view contains a combination of some of the following views, depending on your previous selections:

- Alarms view

- FAQts view

- Monitor Locations view

- Network Devices view

- Single Location Summary view

- Summary - All Devices view

- Summary - All Monitor Locations view

- Summary - Single Device Summary view

# Single Location Summary view

## Purpose

The **Single Location Summary** view displays overall response and availability information for the network devices monitored from the selected location. It identifies the network devices with the lowest availability, highest response time, and highest data packet loss, showing the top five transactions in each of these categories. Use this view to identify the network devices with performance disruptions, and to investigate them further.
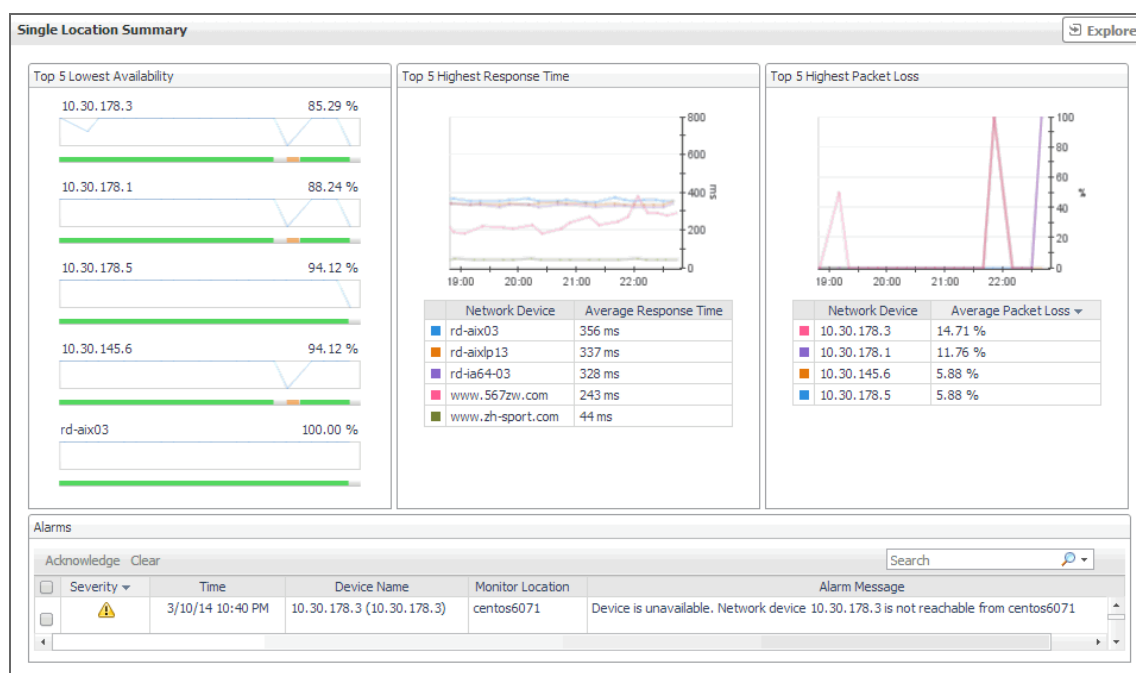
## How to get here

1   Navigate to the Performance Browser.

2   On the Monitor tab, in the Net Monitor Environment view, select the **Monitor Locations** tile.

3   In the Quick View, in the Monitor Locations view, select a monitoring location.

    The **Single Location Summary** view appears on the right.

## Description of embedded views

This view is made up of the following embedded views:

- Alarms
- Top 5 Highest Packet Loss
- Top 5 Highest Response Time
- Top 5 Lowest Availability

## Alarms

For more information, see Alarms view.

## Top 5 Highest Packet Loss

**Table 12. Top 5 Highest Packet Loss view**

| Description | Identifies the top five network devices that are monitored from the selected location and have the highest data packet loss. |
|---|---|
| Data displayed | • **Average Packet Loss**. The average percentage of time that the data packets sent to the monitored device from the selected location are not echoed back. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.<br>• **Network Device**. The IP address of the monitored network device. |

## Top 5 Highest Response Time

**Table 13. Top 5 Highest Response Time view**

| Description | Identifies the top five network devices with the highest response time that are monitored from the selected location. |
| --- | --- |
| Data displayed | • **Avg Response Time**. The average round-trip response time between the selected monitoring location and the network device.<br>• **Network Device**. The IP address of the monitored network device. |

## Top 5 Lowest Availability

**Table 14. Top 5 Lowest Availability view**

| Description | Identifies the top five network devices that are monitored from the selected location and have the lowest availability. |
| --- | --- |
| Data displayed | • **Availability**. A sparkline and a color-coded bar, indicating the levels of availability of the network device over the selected time range.<br>• **Network Device**. The IP address of the monitored network device, followed by the percentage of its average availability. |

# Summary - All Devices view

## Purpose

The **Summary - All Devices** view displays overall response and availability information for all monitored network devices. It identifies the network devices with the lowest availability, highest response time, and highest data packet loss, showing the top five network devices in each of these categories. Use this view to identify the devices with performance degradation, and to investigate them further.
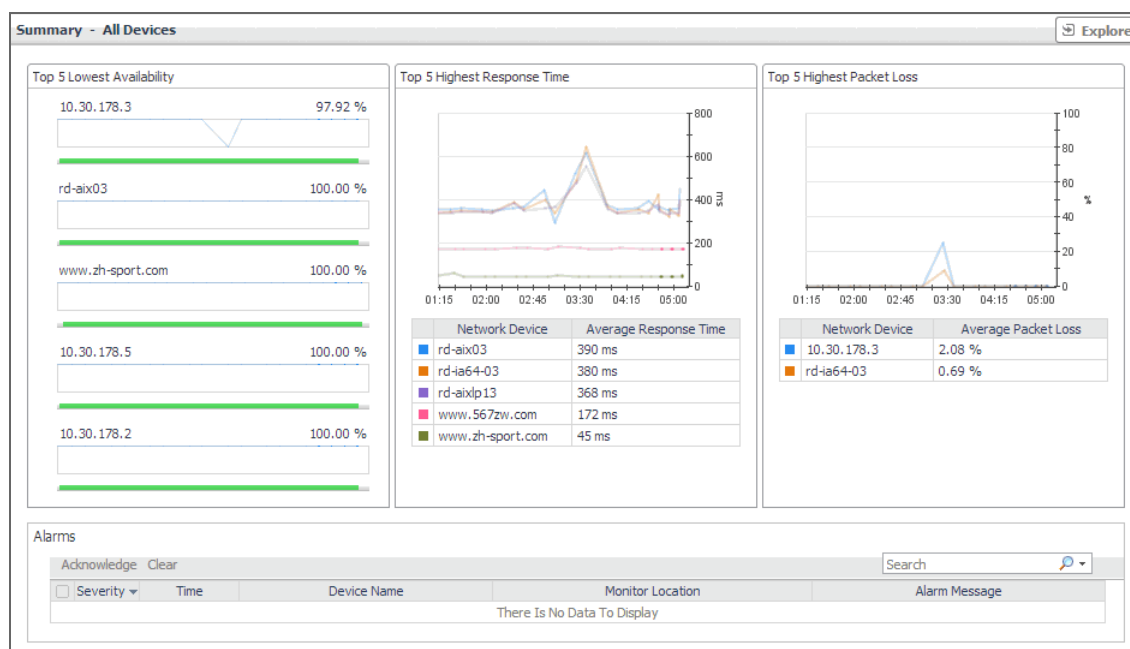


## How to get here

1  Navigate to the Performance Browser.

2  On the Monitor tab, in the Net Monitor Environment view, select the **Network Devices** tile.

3    In the Quick View, in the Network Devices view, select **All Network Devices**.

The **Summary - All Devices** view appears on the right.

## Description of embedded views

This view is made up of the following embedded views:

- Alarms
- Top 5 Highest Packet Loss
- Top 5 Highest Response Time
- Top 5 Lowest Availability

### Alarms

For more information, see Alarms view.

### Top 5 Highest Packet Loss

**Table 15. Top 5 Highest Packet Loss view**

| Description | Identifies the top five network devices with the highest data packet loss. |
| --- | --- |
| Data displayed | • **Average Packet Loss**. The average percentage of time that the data packets sent to the monitored device are not echoed back. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.<br>• **Network Device**. The IP address of the monitored network device. |

### Top 5 Highest Response Time

**Table 16. Top 5 Highest Response Time view**

| Description | Identifies the top five network devices with the highest response time. |
| --- | --- |
| Data displayed | • **Avg Response Time**. The average round-trip response time between the network device and its monitoring locations.<br>• **Network Device**. The IP address of the monitored network device. |

### Top 5 Lowest Availability

**Table 17. Top 5 Lowest Availability view**

| Description | Identifies the top five network devices with the lowest availability. |
| --- | --- |
| Data displayed | • **Availability**. A sparkline and a color-coded bar, indicating the levels of availability of the network device over the selected time range.<br>• **Network Device**. The IP address of the monitored network device, followed by the percentage of its average availability. |

# Summary - All Monitor Locations view

## Purpose

The **Summary - All Monitor Locations** view displays a list of existing monitoring locations, identifies the periods of time that each device was unavailable, and shows the counts of alarms generated for each location, if applicable.
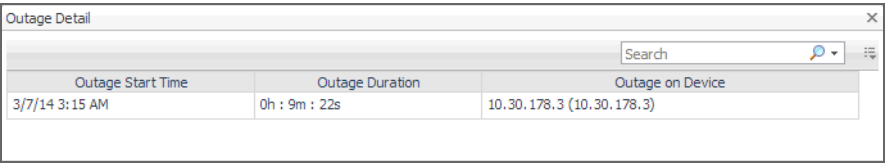
## How to get here

1  Navigate to the Performance Browser.

2  On the Monitor tab, in the Net Monitor Environment view, select the **Monitor Locations** tile.

3  In the Quick View, in the Monitor Locations view, select **All Monitor Locations**.

   The **Summary - All Monitor Locations** view appears on the right.

## Description of the view

**Table 18. Summary - All Monitor Locations view**

| Data displayed | • **Location**. The name of the host from which network devices are monitored.<br>• **Outage**. The number of times any network devices was unresponsive to data collection requests, followed by the total outage duration.<br>• **Device Alarms**. The counts of alarms generated against the monitoring device in each alarm state: Normal ✅, Warning ⚠, Critical 🔶, or Fatal ❌. |
| --- | --- |
| Where to go next | Drill down on:<br>• **Outage**. Displays the **Outage Detail** dialog box.<br><br> |

# Summary - Single Device Summary view

## Purpose

The **Summary - Single Device Summary** view provides an overview of the selected network device. Use it to find out the latest data collection statistics from each monitoring location, and to review its overall health.
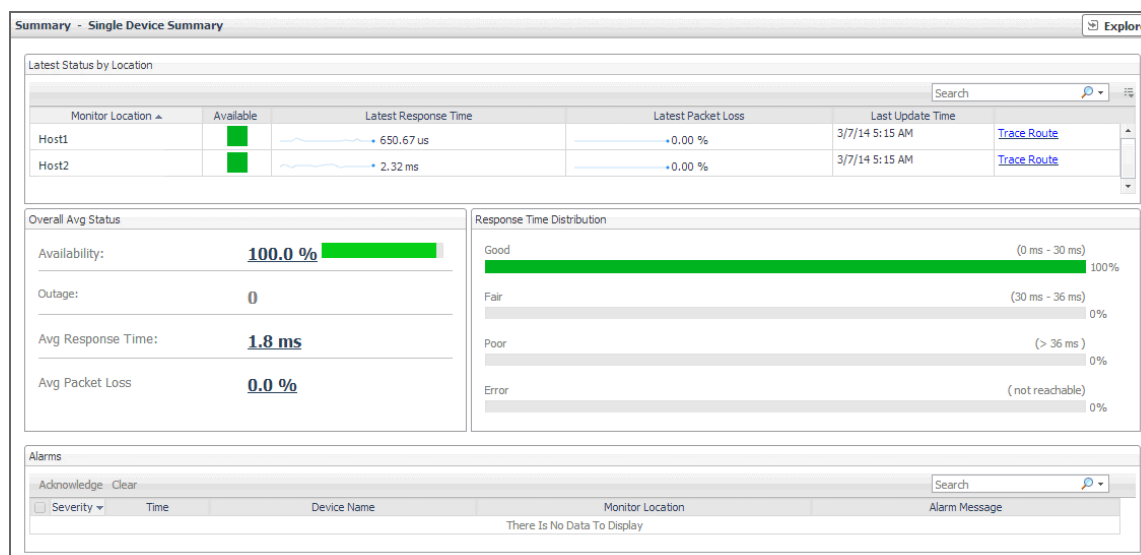
## How to get here

1. Navigate to the Performance Browser.

2. On the Monitor tab, in the Net Monitor Environment view, select the **Network Devices** tile.

3. In the Quick View, in the Network Devices view, select a network device.

   The **Summary - Single Device Summary** view appears on the right.

## Description of embedded views

This view is made up of the following embedded views:

- Alarms
- Latest Status by Locations
- Overall Avg Status
- Response Time Distribution

## Alarms

For more information, see Alarms view.

## Latest Status by Locations

**Table 19. Latest Status by Location view**

| Description | Lists the hosts from which the selected network device is monitored. |
| --- | --- |
| **Data displayed** | <ul><li>**Available**. A color-coded bar, representing the availability of the device over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.</li><li>**Latest Packet Loss**. The percentage of data packets sent to the monitored device that are not echoed back in the most recent collection period. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.</li><li>**Latest Response Time**. The round-trip response time between the monitoring agent and the network device in the most recent collection period.</li><li>**Monitoring Location**. The name of the host from which the selected network device is monitored.</li></ul> |
| **Where to go next** | Drill down on:<br><ul><li>**Trace Route Now**. For more information, see Trace Result view.</li></ul> |

## Overall Avg Status

**Table 20. Overall Avg Status view**

| Description | Shows how well the selected network device is responding to the data collection requests from all of its monitoring locations. |
| --- | --- |
| **Data displayed** | <ul><li>**Availability**. The percentage of time the selected network device was available for monitoring, followed by a color-coded bar, representing the availability of the device over the selected time range. The color of the bar changes depending on the device availability. Orange indicates a device outage, green means a normal state, white means that no monitoring occurred.</li><li>**Avg Packet Loss**. The percentage of time that the data packets sent to the monitored device are not echoed back, over the selected time range. By default, the monitoring agent sends three data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.</li><li>**Avg Response Time**. The round-trip response time between the monitoring agent and the network device, over the selected time range.</li><li>**Outage**. The number of times the selected network device was unresponsive to data collection requests, followed by the total outage duration.</li></ul> |
| **Where to go next** | Drill down on:<br>**Availability**, **Avg Packet Loss**, or **Outage**. For more information, see Device Detail view. |

## Response Time Distribution

**Table 21. Response Time Distribution view**

| Description | The distribution of the device response times in each of the available categories: **Good**, **Fair**, **Poor**, and **Error**. |
| --- | --- |
| Data displayed | • **Error**. The percentage of times the network device was unresponsive.<br>• **Good**: The percentage of times the network device takes between zero and the expected response time configured for the device.<br>• **Fair**: The percentage of times the network device takes between the expected response time configured for the device and the expected response time, times the rate to respond to data collection requests.<br>• **Poor**: The percentage of times the network device takes between higher than expected response time configured for the device, times the rate to respond to data collection requests. |

# Trace Result view

## Purpose

The **Trace Result** view displays the length of the hops on a packet's route to its destination, and the distribution of average response times for each hop. Use this information to investigate a device with longer than expected response times and to identify the points in the route that may be the cause of the data packet delay.
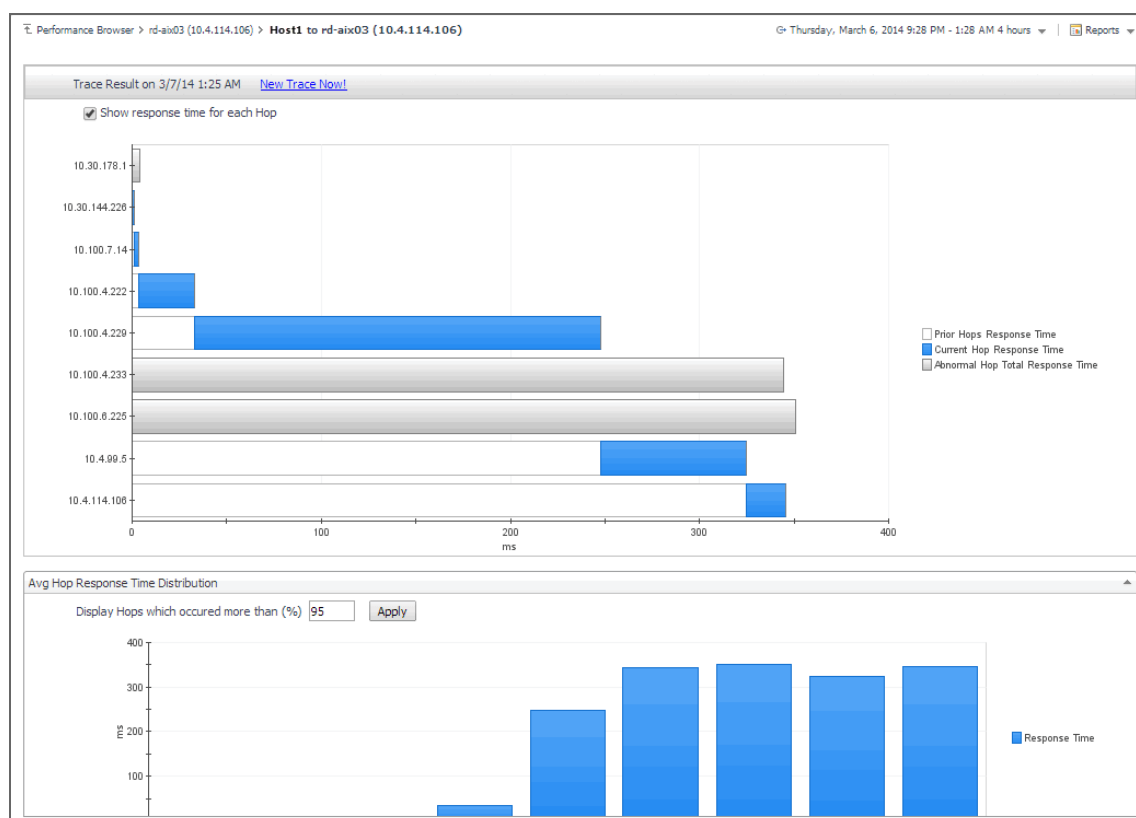


## How to get here

1   Navigate to the Performance Browser.

2   On the Monitor tab, in the Net Monitor Environment view, select the **Network Devices** tile.

3  In the Quick View, in the Network Devices view, select a network device.

4  In the Summary - Single Device Summary view, in the embedded Latest Status by Locations view, in the row containing a monitored location whose route to the selected network device you want to trace, click **Trace Route**.

The **Trace Result** view appears in the display area.

The trace route request runs in the background and takes several minutes to complete. Instead of waiting for it to complete, you can navigate to other dashboards, and then return to this page to review the trace route.

> ℹ | **IMPORTANT:** If the trace route option is disabled in the device settings (see Viewing and editing individual network device details), this page is not populated with data. You can quickly execute a trace route in real time on this page by clicking Trace Route Now.

## Description of embedded views

This view is made up of the following embedded views:

- Avg Hop Response Time Distribution
- Trace Result

## Avg Hop Response Time Distribution

**Table 22. Avg Hop Response Time Distribution view**

| Description | Displays a chart showing the hop response times for the selected route. Each route consists of one or more hops. A hop is the route between one network device and the next on a packet's way to its destination. A hop destination is a device through which the packet passes on the route. |
| --- | --- |
| Data displayed | • **Prior Hops Response Time**. When **Show response time for each Hop** is selected, this area in the chart represents the length of time the data packets take to travel from the monitoring location to this device. <br><br> • **Current Hops Response Time**. When **Show response time for each Hop** is selected, this area in the chart represents the length of time the data packets take to travel from the previous device to this device, on the way to its destination. <br><br> • **Abnormal Hops Response Time**. When **Show response time for each Hop** is selected, this area in the chart represents the length of time the data packets take to travel from the monitoring location to this device, that result in an error. <br><br> • **Response Time**. When **Show response time for each Hop** is cleared, this area in the chart represents the length of time the data packets take to travel from the monitoring location to this device, on the way to its destination. |

## Trace Result

**Table 23. Trace Result view**

| Description | The distribution of the device response times for each hop that occurred more than a selected percentage of times. <br><br> **NOTE:** Use the **Display Hops which occurred more than (%)** box to specify a desired percentage. |
| --- | --- |
| Data displayed | • **Response Time**. These areas in the chart represent the length of time the network device takes to send the data packet from the monitoring location to this device, on the way to its destination. |

# About Us

## We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

## Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

## Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

## Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.