

Chapter 8



Real-time Status Monitoring

8.1 Introduction

Helix offers two types of reporting: real-time status reports and historic trend reports. Immediately upon logging into the Helix web interface, the default view is a real-time status of your monitored devices on the Device Summary page. You are able to see any current failures instantly. In a single click Helix provides you with test details on any monitored device, a 24 hour graphical snapshot of performance and event history, and test results for the last 30 days.

8.1.1 Helix Terms

Helix monitors the availability and performance of your network and application systems, and their underlying components. These systems and components may be routers, switches, servers, databases, networks, or applications.

A **test** is the measure of device functioning. Tests are used to monitor your devices. Helix reports the status of each test. Test status (shown on the `Status | Tests` page) is the current status category (ok, warning, critical, unknown, unreachable, suspended, or not configured) for a test. Device status (shown on the `Status | Device` page) is the worst current test status for a device.

Helix uses boundaries called **thresholds** to determine a test's status. An **event** occurs whenever a test result crosses a threshold.

An **action** is an activity that is automatically triggered by an event. Actions can be designed to take place immediately when a single event occurs or after the same event occurs repeatedly. For instance, an E-mail notification can be sent whenever a test crosses the warning threshold, or it can be sent after a test has crossed the warning threshold five consecutive times.

8.2 Helix Status View

8.2 displays the Helix icons used to display device and test status.

Status	Description
OK	The test was within configured thresholds.
WARNING	The test violated the Warning threshold
CRITICAL	The test violated the Critical threshold, or alternately it FAILED to perform for some reason (see description below for failed tests).
TRANSIENT	Test status is TRANSIENT if the test's status has changed, but the flap prevention threshold has not been crossed (set in dge.xml). For example, if you configure a test so that no action is taken until the result has been CRITICAL for three test cycles, test status changes to TRANSIENT after the first CRITICAL result is returned. It remains TRANSIENT until either the problem is resolved, in which case test status changes to a lower severity, or the third CRITICAL result is returned, after which test status is CRITICAL and appropriate action is taken.
UNKNOWN	Test status can be UNKNOWN for one of several reasons, see description below. This can be monitor dependent.

Status	Description
UNREACHABLE	<p>A test is in this state if all the 'parent' devices are down and the downstream device is unreachable based on the topology. Additionally, if a DGE is unreachable by the WebApp, it displays the UNREACHABLE state for all the tests and devices on that DGE.</p> <p>This state is useful to prevent alarm floods when a parent device goes down in a network.</p>
NOTCONFIGURED	<p>If there are no tests configured for a device in that category</p>

Test status can be UNKNOWN for one of several reasons:

- When a new test is added to a device, the provisioning database notifies the relevant DGE. When the DGE gets this notification, it retrieves the test details from the provisioning database and schedules the test for monitoring. A scheduled test is added to a queue at the interval configured for the test. Items from the queues are tested (often in large batches) in sequential order. Depending on how many tests you have configured on a particular DGE/location, a newly added test may remain in the queue for seconds or minutes. While the test is waiting in the queue, the Web Application shows UNKNOWN state for the test, since it does not yet have any polled results to display.
- Some tests do a rate calculation ($[\text{result1} - \text{result2}] / \text{time_elapsed_between_tests}$), which requires two polled results. For example, most network interface tests (Traffic In/Out, Util In/Out) are in this category. Until the second result is polled, these tests show UNKNOWN state. If a test is configured for a five-minute polling interval, it remains in UNKNOWN state for approximately ten minutes, until two results are received and the rate is calculated.

- If a device is not reachable (e.g., it's been turned off, there are network problems, etc.), tests for that device appear in UNKNOWN state, indicating that no polled value could be retrieved.
- In the case of SNMP tests, if the OID is no longer valid (ifIndex has changed), the test appears in UNKNOWN state, indicating that no polled value could be retrieved.

Although not represented by a particular icon, a test can have a status of FAIL, which means that the device was reached but the test failed to be performed. An example is when a POP3 port test is performed and the supplied login/password combination fails. This is monitor dependent.



Figure 8.1 Helix Symbols Used to Report Status

Test Timeouts

If a standard test does not return a result within a certain timeout interval, test status is FAILED. There are three types of timeouts:

- Fixed
The timeout value is always the same (e.g., 10 seconds).
- Dynamic
The timeout value changes depending on some user-configured value (e.g, threshold + 5 seconds).
- Static

The value is specified in a configuration file and does not frequently change.


Monitor Type	Timeout Type	Timeout Interval	Comments
ICMP ping	fixed	10 seconds	
SNMP	fixed	11 seconds	Helix retries 3 times within this period
TCP-based (HTTP, SMTP, POP3, etc.)	dynamic	Largest configured threshold (End-user, Admin, or SLA) + 5 seconds	
UDP-based (DNS, RADIUS, NTP, etc.)	dynamic	Largest configured threshold (End-user, Admin, or SLA) + 3 seconds. (If all thresholds are 0, timeout is 5 seconds.)	
Script-based plugin monitors	fixed	60 seconds	
Script-based plugin actions	static	Value specified in configuration file, or 60 seconds if none specified	Applicable when <code>waitForTerminate</code> property is enabled in the configuration file

8.2.1 Device Status Summary View

❑ To view the Device Summary for your department, do one of the following:

- Log in to Helix. You will be taken to the Device Summary page for your department.
- If you are already logged in, click on the **STATUS** tab and your Device Summary or Container Summary screen will load (depending on your user preferences).

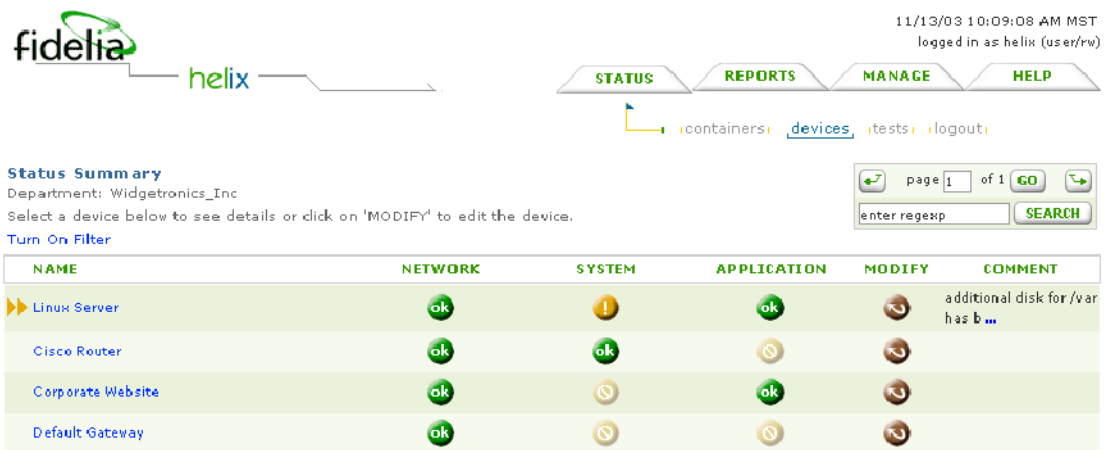
The Device Summary View is the default view after the **STATUS** tab is selected. There is one row for each device in your department that is being monitored. Each row gives the device name and the status for each of three categories of tests: Network, System, and Application.

The  modify icon links you to a page for modifying a device's settings.

If the device status for one group of tests is warning, at least one current test result for that test category is in warning range. Similarly, if the device status for one category of tests is critical, at least one current test result for that group is in critical range. The worst test status of all tests in the category determines the icon displayed. The rule for displaying the icons (from most to least severe) is:

- critical (most severe)
- warning
- transient
- unreachable
- unknown
- ok
- suspended
- not configured (least severe)

A sample Device Summary page is shown below.



11/13/03 10:09:08 AM MST
logged in as helix (user/rw)

STATUS REPORTS MANAGE HELP

containers devices tests logout

page 1 of 1 GO

enter regexp SEARCH










NAME	NETWORK	SYSTEM	APPLICATION	MODIFY	COMMENT
Linux Server	ok	!	ok		additional disk for /var has b...
Cisco Router	ok	ok			
Corporate Website	ok		ok		
Default Gateway	ok				

Figure 8.2 Device Summary Page

❑ To modify the settings for a device:

1. Click on the **STATUS** tab on the main navigation bar to go to the Status Summary page
2. Click on the  modify icon for the desired device and you will be taken to the Update Device page.
3. See the Section 9.1, “Managing Devices” on page 83 for instructions on managing devices.

8.2.2 Test Summary View

The Test Summary page contains one row for each test being conducted. Each row contains test status, test name, current test value, the warning and critical thresholds, the time the last test was conducted, and the time the test has remained in the current state.

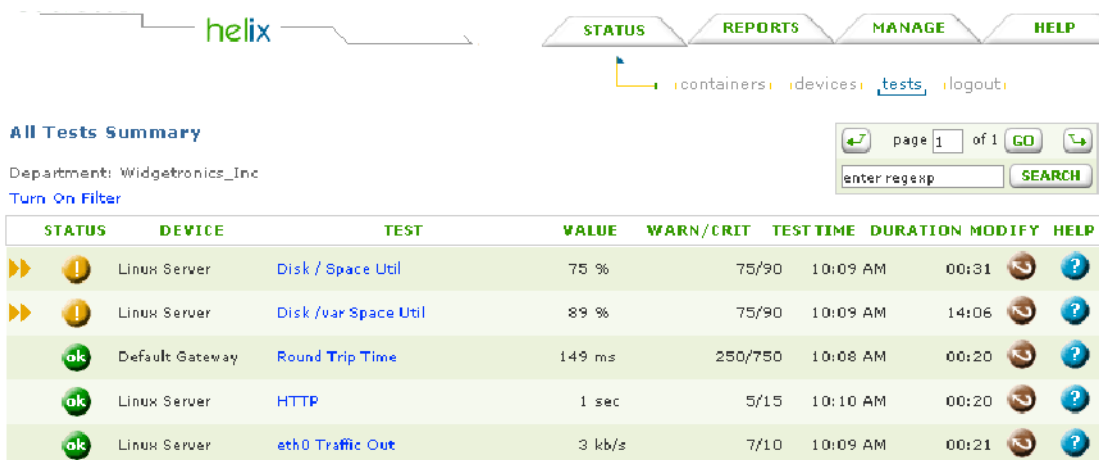


Figure 8.3 Test Summary Page

❑ To view the test summary for a specific device:

Click on the **STATUS** tab on the main navigation bar to go to the Device Summary page. Click on the **device name** link for the device of interest and you will be taken to the Device Status Details page.

8.2.3 Test Details View

The Test Details page graphically displays performance and event history for a single test over the last 6-24 hours. Figure 5 below illustrates the four graphs on the Test Details page:

- a three-dimensional bar graph of test results for the last 6 hours
- a pie chart showing percent of last 24 hours in each of the following statuses:
 - ▶ OK
 - ▶ WARNING
 - ▶ CRITICAL
 - ▶ UNKNOWN
 - ▶ UNREACHABLE
- a line graph of test results for the last 24 hours

- a frequency distribution graph for the last 24 hours

Test Details
Default Gateway - Performance and Event History
Events for the last 24 hours
[View raw data](#)
[View historical graphs](#)
[View trend analysis](#)

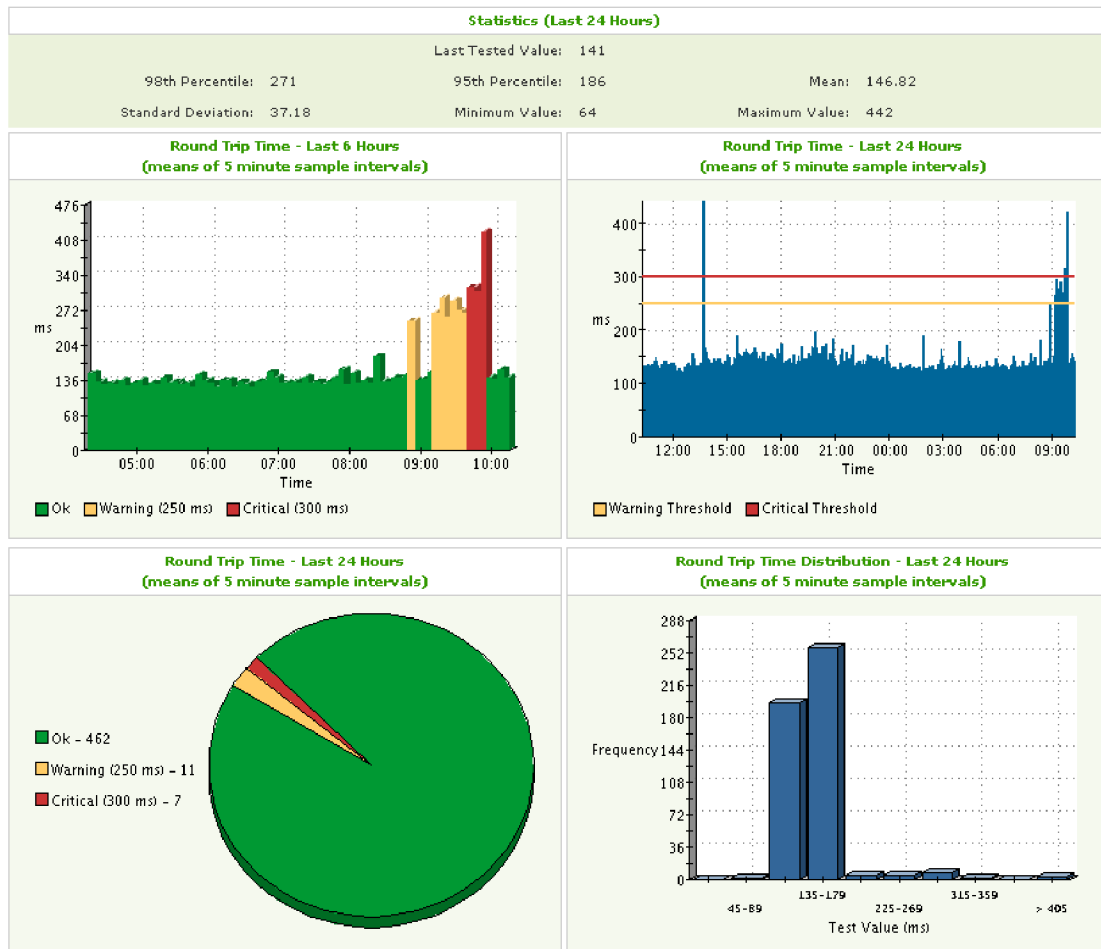


Figure 8.4 Test Details Page

To view the details for one specific test:

1. Click on the **STATUS** tab on the main navigation bar to go to the Device Summary page.

2. Click on the **device name** link for the device of interest and you will be taken to the Test Summary page.
3. Click on the **test name** link for the test of interest and you will be taken to the Test Details page for that test.

From the Test Details page, users also have access to the following information for that test:

- Event log - WARNING & CRITICAL events for the last 24 hours
- Raw event data - ALL test results recorded for the last 24 hours (regardless of severity)
- Historical Graphs - performance graphs for last week, last 30 days, and last year
- Trend analysis

8.2.4 Test Container Summary View

The Test Container Summary View, available via `STATUS | Containers` displays the consolidated view of logical systems or applications by grouping together tests in a virtual device. The status of a container is the 'worst' of any of the its components. Hence, if any device or nested container within a container turns critical, the status will 'bubble up' and turn the top level container to also be critical.

In addition to viewing the real-time status of Service Containers, you can generate reports on containers which tell you the downtime, which element caused a container to be unavailable, etc.

Please see Section 9.5, "Managing Test Containers (Virtual Devices)" on page 105 for more detailed information.

8.2.5 Device Display Filters

Via Helix's device summary views (i.e. Device Summary and Device Groups Summary pages), users can set default filters in order to only view devices in specific states. For example, users

may elect to filter out devices that are in an 'OK' status. Additionally, users can specify how many devices are displayed on a single page. Especially for large deployments, these two features can dramatically cut down on the number of entries a user must scroll through to get a quick snapshot of system health. A toggle switch on the Device Summary & Device Groups Summary pages quickly disables or enables the filter(s).

□ **To set device filter and paging preferences:**

1. Click `MANAGE | prefs`.
2. Select the device states you want to view on the summary pages. Device states that are not selected are filtered out by default.
3. Change the number of devices to view on each page in the **Maximum Summary Screen** field.
4. When you have finished configuring preferences, click **Update User** to save your changes. These changes become part of your user profile and serve as defaults each time you log in to Helix.

8.2.6 Device Comment Field

A user can enter a comment that will display on the Device Summary page. This could be used in any way by the user to communicate device-specific information, such as to identify why a device is being suspended or as general information on the current state of the device.

□ **To create a comment for a specific device:**

1. Click on the **MANAGE** tab on the main navigation bar to go to the Manage Devices page.
2. Click on the **Comments** link for the device of interest and you will be taken to an Update Device page.
3. Add the comments and click the **Update Device** button to save changes. (This can also be accomplished when suspending a device.)

4. Navigate to the **Device Summary** page and confirm that the comment appears for the device you updated.

8.2.7 Context-sensitive Help or Action

Helix's Test Summary view displays a **HELP** link used to provide context-sensitive help to users. Selecting the link displays a pop-up window with information configured by your administrator or operations personnel to address device or test help topics. Although completely customizable, one suggested use of this functionality is to provide online help documentation for a specific device or test in the absence of senior administration personnel (e.g. nighttime operations).

An alternative to providing text based help, is to enable an action (e.g. server re-start) via the **HELP** link. This is a powerful option, as an administrator can configure any number of files to work in this fashion, enabling a large number of background processes via the web app. Please contact your Helix administrator for details of how the functionality is being deployed in your organization.

8.3 Event Logs

An Event Log lists every time a test status has changed state in the past 24 hours. Each entry gives the device name, time the event occurred, test name, type of test, low (warning) and high (critical) thresholds, and the actual test value.

The event logs can be viewed from the **REPORTS** page by specifying the devices and the time period desired.

Event Log

Events Log for 11/1/03 - 11/13/03

Device Name	Time	Test Name	Warning	Critical	Test Value
Network Monitoring	11/10/03 10:41 AM	HTTP	5 sec	15 sec	1 sec
Network Monitoring	11/10/03 10:41 AM	Disk /var Space Util	75 %	90 %	90 %
Network Monitoring	11/10/03 10:41 AM	Swap Space Usage	90 %	100 %	1 %

8 · Real-time Status Monitoring
· **Event Logs**
·

