

Chapter 22



Administrator Web Guide

22.1 NetVigil Administration Basics

This chapter describes the web application relevant to a NetVigil “administrator” (belonging to an administrative group). Note that an ‘administrative’ user can view multiple departments, but a departmental user can only see his own department devices.

NOTE: Most of the menu items in the Administrator Web interface are similar to the Web interface for a departmental user and are described in greater detail in the Chapter “Netvigil Web Interface” in Volume 2.

22.1.1 Logging In

The NetVigil superuser will probably create the Admin-Group structure and assign you to an Admin-Class, which will determine the scope of your ability to see, create, modify and delete entities within the application.

□ To access NetVigil:

1. Type **http://netvigil.your.domain** into your web browser.
2. Enter the Department name, Username and Password given to you by your administrator.
3. Click on the **Login** button to enter the site.

If you are an Administrator, you will see the administration interface as described above. If you are not an administrator, please refer to the *User Guide* for assistance with your NetVigil account.

22.1.2 Department Status Summary View

- ❑ **To view the Status Summary for all your Departments, do one of the following:**
 - Log in to NetVigil. You will be taken to the **Department Status Summary** page.
 - If you are already logged in, click on the **STATUS** tab and the **Department Status Summary** screen will load.

The Department Status Summary View is the administrative default view when the **STATUS** tab is selected. There is one row for each Department with monitored devices. Each row gives the Department name and an icon representing the worst test status for the Department at the far right of the row.

If the Department status for one group of tests is **WARNING**, at least one current test result for that test category on the Department is in **WARNING** range. Similarly, if the Department status for one category of tests is **CRITICAL**, at least one current test result for that category on the Department 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**
- **UNREACHABLE**
- **UNKNOWN**
- **OK**
- **SUSPENDED**
- **UNCONFIGURED** (least severe)

Figure 22.1 shows a sample Department Status Summary page.

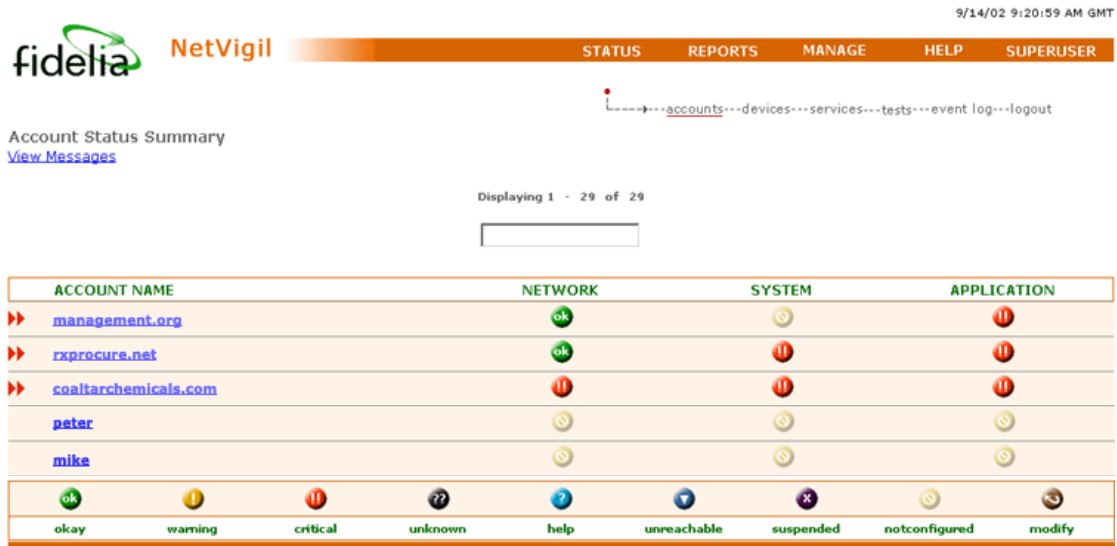


Figure 22.1 Department Status Summary Page

22.1.3 Device Status Summary View

The Device Status Summary View under the main **STATUS** tab displays all the devices on all the Departments that you have been given permission to view/manage. Each row displayed gives the device name and an icon representing the worst test status for the device at the far right of the row.

If the Department status for one group of tests is **WARNING**, at least one current test result for that test category on the Department is in **WARNING** range. Similarly, if the Department status for one category of tests is **CRITICAL**, at least one current test result for that category on the Department is in **CRITICAL** range. The worst test status of all tests in the category determines the icon displayed. To view the device status summary for a specific Department:

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

22.1.4 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. For example, in the sample Device Test Status Summary page in Figure 22.2 below, the ping Packet Loss test has been in OK status for 1 hour & 18 minutes.

❑ To view the test summary for a specific device:

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

3. Click on the **device name** link for the device of interest and you will be taken to the Device Test Status Summary page.

Test Summary
 Account: sales_demo
 Device: www.momentump.com
[Device performance for the last 24 hours](#)

Displaying 1 - 3 of 3

STATUS	TEST	VALUE	WARN/CRIT	TEST TIME	DURATION	HELP
⚠	Packet Loss	60 %	50/80	3:43 AM	00:03	?
ok	HTTP	1 sec	3/7	3:42 AM	00:44	?
ok	Round Trip Time	58 ms	250/1500	3:43 AM	2d 15:18	?

ok ⚠ !! ?? ? ▼ ✖ ⏸ ⚙
 okay warning critical unknown help unreachable suspended notconfigured modify

Figure 22.2 Device Test Status Summary Page

22.1.5 Event Logs

An Event Log lists every time a test status has changed in the past 24 hours. Each line gives the device name, time the event occurred, test name, type of test, low (warning) and high (critical) thresholds, and the test value. The Event Log is typically sorted by device and then by test, but may not show other devices or even a device name, depending on which level of detail you are viewing. The various levels of viewing event logs are explained below.

❑ To view the Event Log for all Departments/devices:

1. Click on the **STATUS** tab on the main navigation bar.
2. Click on the **Event Log** link on the secondary navigation bar.

Please wait for the information to load, as the databases for all the Data Gathering Engines (DGEs) are being queried.

22.2 Administrative Reports

NetVigil provides report templates for analyzing systems usage and performance. The reports are designed to provide a summary view of all the Departments assigned to you as an administrator. The currently available reports detail Department/device health, event history for Departments/devices/tests in a drill down fashion, and audit Department and user activity. The Admin-Class to which you are assigned adheres to the privileges matrix and provides the filter for which User-Classes you will see on your reports. Consequently, if you are managing a single department, you may have full access to the department information, but will not be able to see another department's reports (and vice versa). This restriction can be modified by the enterprise's Superuser to fit your needs.

IMPORTANT NOTE The WARNING or CRITICAL events used to generate Admin reports are based on Admin Thresholds, which are thresholds established by an Administrator for each combination of test type and User-Class. (See Section 9.5.4, “Setting Admin Action Profiles and Thresholds” on page 140 for more details.) End-users who run similar reports see reporting results based on WARNING and CRITICAL thresholds that they have established themselves on a per test basis, either by accepting default test thresholds or by specifying threshold values. Thus, reports based on WARNING or CRITICAL severities may show different results, depending on whether they are generated by an Administrator or an end-user. Because SLA thresholds are the same for both Administrators and end-users, reports based on SLA severities display the same results.

□ To view the following reports:

1. Click on the **REPORTS** tab on the main navigation bar. You will be taken to the Manage Reports page (see Figure 22.3 below.)
2. Depending on report type, select a **Duration** and/or **Severity** via the drop down list, then click **Go**.

3. To view the User Audit Report, simply click **Go**.

The screenshot shows the 'Manage Reports' page in the NetVigil Administrator interface. The page is organized into several sections:

- Header:** Includes the 'fidelia NetVigil' logo, a navigation bar with 'STATUS', 'REPORTS', 'MANAGE', 'HELP', and 'SUPERUSER' tabs, and a timestamp '9/12/02 8:12:54 AM GMT'. There are also links for 'create', 'custom', and 'logout'.
- Section a) Fault Management Reports:** Contains three report rows:
 - Service Instability:** Rows: 10, Severity: User, Duration: September, Go button.
 - Device Instability:** Rows: 10, Device Type: Windows, Severity: User, Duration: September, Go button.
 - Threshold Violations:** For: Bandwidth, Device Type: Windows, Severity: User, Duration: September, Go button.
- Section b) Performance and Capacity Planning Reports:** Contains two report rows:
 - Top 'N' Usage & Trend Report:** Rows: 10, Level: Account, Duration: September, Order: Most, Go button. A dropdown menu is open showing options: Advanced Port Test, Advanced SNMP Test, BGP Peer Status, BGP Route Update Rate, and Block IO Received.
 - 30 Day Upcoming Trends:** For: Bandwidth, Go button.
- Section c) SLA Reports:** Contains two report rows:
 - Unavailability/Downtime:** Duration: September, Go button.
 - Threshold Violations:** For: Bandwidth, Device Type: Windows, Duration: September, Go button.
- Section d) Management Reports:** Contains one report row:
 - User Audits:** Go button.
- Section e) Stored/Scheduled Reports:** Contains one report row:
 - Saved Queries:** (Manage Queries) Query: Select Query, Go button.

Figure 22.3 Manage Reports Page

22.2.1 Management Reports

User Audits

This administrator-level report displays discrete numbers of Departments, users, devices, tests by category, and logins for each User-Class within the domain of the administrator seeking the information. Also displayed for each User-Class, are average numbers per Department for: devices, ICMP tests, SNMP tests, and Port test.

The Superuser is also able to see the currently logged in users by clicking on the link 'Who's logged in now'.

22.3 Creating Read-Only Devices

NetVigil administrators have the option of creating read-only devices for viewing by end-users. This functionality can be extremely useful when a service provider or IT department must provide shared access to a device (i.e. partitioned server, router, switch) for a number of end-users. In this case, it may be desirable to restrict end-user access to a single device.

NOTE *End-users sharing the same department also share the devices, tests and actions in that Department. Therefore, any read-only device created for an end-user will be seen by other end-users of the same Department.*

□ To create a read-only device:

1. Search for the desired end-user for whom you want to create a read-only device and represent them. If necessary, see Section 8.3.7, “Representing Users” on page 129 for instructions.
2. Click on the **Administer** tab.
3. Click on the **Create A Device** link in the information bar.
4. Select the **Read-Only** check box.
5. Select or fill in all the required fields indicated, and add any optional information in the comments field.
6. Select the **Smart Notification** box if desired.
7. Choose the desired test types for discovery, and the SNMP version and community ID (if applicable).
8. Click on the **Create Device** button to confirm changes and begin test discovery process.
9. Once test discovery is complete, select the desired tests for the device and assign any action profiles (if desired by the end-user.)
10. Click the **Provision Tests** button to confirm the test creation.

Note that this is different from exporting a device which is described in Chapter 8, “Users and Departments” on page 122