

Chapter 16

Manage NetVigil

The `Manage` menu in the NetVigil user interface allows creating and configuring of containers, devices, tests, actions, etc. using the web interface.



16.1 Adding Devices For Monitoring

The Manage Devices page displays all the department's devices and links to perform various administrative functions on the devices. Each row contains the device name and address, type of device, whether monitoring is currently active or suspended, a link for suspending or

resuming monitoring, and the physical device location. Additionally, there are links for updating or deleting the device, and for managing the tests for the device.

Manage Devices
[Create A Device](#)
[Test Baseline Management](#)

page 1 of 1 Go
 name or perl5re Search
 sort by name

DEVICE NAME ▲	ADDRESS	DEVICE TYPE	STATUS	LOCATION	<input type="checkbox"/>	MODIFY
Cisco	192.168.1.254	IP Router		New York	<input type="checkbox"/>	Update Tests
mail.fidelia	mail.fidelia.com	Linux/Other Unix		New York	<input type="checkbox"/>	Update Tests
solaris	192.168.1.156	Linux/Other Unix		New York	<input type="checkbox"/>	Update Tests
support	192.168.1.150	Linux/Other Unix		New York	<input type="checkbox"/>	Update Tests
winserv	192.168.1.20	Windows		New York	<input type="checkbox"/>	Update Tests

Apply the following updates to the devices selected above:

Modify devices: Device Type: Smart Notification:

SNMP Version: SNMP Community:

Custom Attribute #1: Custom Attribute #2: Custom Attribute #3:

Custom Attribute #4: Custom Attribute #5:

Display Comment: Auto-Clear Comment:

Comment:

Figure 16.1 Manage Devices Page

❑ To create a new device

1. Click on the **MANAGE** tab. You will be taken to the Manage Devices page.
2. Click on the **Create A Device** link
3. Select the type of device you are configuring via the drop down list (i.e. Linux or any other Unix server, Windows server, managed switch/hub, IP router, Firewall Appliance, Load Balancer, Proxy Server, VPN concentrator, Wireless Access Point or Any Other).
4. Give your device a name in the **Device Name** box.
5. Type in the fully qualified host name or IP address of the device.
6. Optionally, add comments.

7. Use the **Location** dropdown list to assign the device to a DGE Location. (A DGE Location is a collection of DGEs, not necessarily in the same physical location, that are grouped for load-balancing purposes.) If this device will be monitored via WMI, select a DGE Location that contains WMI-enabled DGEs.
8. Leave **Smart Notification** selected to prevent getting alarms on tests when the device is unreachable. See Section 17.3, “Smart Notifications” on page 238 for more information.
9. Check all the boxes that apply for the test types you wish to discover on the device. Please note that not all tests are available on all devices. If you are not sure what tests are available on the device, please contact your administrator.
10. Optionally, for SNMP only: Select the SNMP version running on the device. If you are not sure what SNMP version is running on the device, please contact your administrator.
11. Optionally, for SNMP only: Enter the SNMP Community ID. If you are not sure of the SNMP Community ID on the device, please contact your administrator. For SNMP version 3, specify the community ID in the following syntax:

```
user : authentication_password : encryption_password
```

12. Click the **Create Device** button to begin the test discovery process.

NOTE Test discovery may take up to 1 minute, depending on the number of test types you chose. Please follow the on-screen instructions as the device is queried.



Create Device

Select or complete the required fields below. Click 'Create Device' to confirm.

* - indicates a required field

* Type of Device:	<input type="text" value="Select Device Type"/>
* Device Name:	<input type="text"/>
* Fully Qualified Host Name/IP Address:	<input type="text"/>
Comments/Description (optional):	<input type="text"/>
Custom Attribute #1:	<input type="text"/>
Custom Attribute #2:	<input type="text"/>
Custom Attribute #3:	<input type="text"/>
Custom Attribute #4:	<input type="text"/>
Custom Attribute #5:	<input type="text"/>
Automatically Clear Comment When In OK State:	<input type="checkbox"/>
Display Comment In Summary Screen:	<input type="checkbox"/>
* Create In Location:	<input type="text" value="Select Location"/>
SNMP Version Supported:	1 <input checked="" type="radio"/> 2c <input type="radio"/>
SNMP Community String:	<input type="text" value="public"/>
SNMP (Agent) Port:	<input type="text" value="161"/>
Enable Smart Notification:	<input type="checkbox"/> ?
Create New Tests After Creating This Device:	<input checked="" type="checkbox"/>
Create Device Dependency After Creating This Device:	<input type="checkbox"/>
<input type="button" value="Create Device"/> <input type="button" value="Reset"/>	

Figure 16.2 Create Device Page

□ To update a device:

1. Click on the **MANAGE** tab and you will be taken to the Manage Devices page.
2. Click on the **Update** link in the row for the device you wish to update and you will be taken to the Update Device page for that device. (This link will be visible only if you have read-write privileges and the device is not a read-only device)
3. Enter the desired changes. For example, if a device's IP address has changed, enter the new address. The properties that can be modified are: type of device (unix server, router, etc.), device name, device IP address (or fully qualified domain name), SNMP version, and community ID.

4. Click on the **Update Device** button at the bottom of the page.

The suspend/resume feature allows you to temporarily turn off all the tests for a device and turn them on again. This feature is useful if you are performing maintenance task on a device and do not want to receive alerts while the device is offline. Once a device is suspended, the polling and data collection for all the tests on the device is suspended and thus any associated actions to the tests will not generate notifications. The suspend/resume feature is available at both the device and the individual test level. Furthermore, when a device is suspended (e.g. for maintenance), this time is not included in the total downtime reports since it is considered a planned outage.

□ To suspend or resume a device:

1. Click `MANAGE | devices`.
2. On the Manage Devices page, find the device that you want to suspend or resume, and then click **Update**.
3. On the Update Device page, select **Suspend/Resume This Device**. (If the device is suspended, the option is **Resume**. Otherwise, the option is **Suspend**.)
4. Click **Submit**.

□ To delete a device:

WARNING: Deleting a device will remove all information about that device from the database, including all historical records. Deletions are not reversible. Suspending a device may be preferable because there is no loss of data.

1. Click `MANAGE | devices`.
2. On the Manage Devices page, find the device that you want to delete, and then click **Update**.
3. On the Update Device page, select **Delete This Device (and associated tests)**.
4. Click **Submit**.
5. If you are sure that you want to delete the device, click **Delete** on the Delete Device confirmation page.

Auto-Update for Device Capacity Change

NetVigil provides a mechanism for refreshing maximum values or SNMP object identifiers (SNMP OID) when an SNMP test has changed. For example, when memory or disk capacity has changed, tests that return percentage-based values would be incorrect unless the max value (for determining 100%) is refreshed. Additionally, in some cases even replacing a device with similar hardware can cause the SNMP OIDs to change, thus creating a mismatch between the current SNMP OIDs and the ones which NetVigil discovered during initial provisioning.

If one of the previous situations occurs, the user need only repeat the test provisioning process in the web application for a changed device. NetVigil will discover whether any material changes on the device have occurred and highlight those changes on the **Configure Tests** page, giving the user the option to also change thresholds and/or actions that apply to the test.

If you see a non-OK test, you can click on the non-OK icon itself (at the test level, not device level) to see the returned error message. However, if the OID is marked as “invalid” and the tests do not exist (e.g. a port module or disk partition no longer exists), then these tests should be deleted manually since NetVigil will not automatically delete these tests.

16.2 Managing Standard Tests

16.2.1 Before You Provision Tests

Your User Group privileges determine whether or not you can create your own actions. Assigning actions to tests can be done in several ways, but all require that an action has already been created either by you or by your User Group administrator. Options include:

- Assign your custom action to one or more tests during the test provisioning process.
- Assign an admin-created default action to one or more tests during the test provisioning process. This option will appear as an action option in the drop down list on the Configure Tests page.
- Update individual tests using a custom or default action after tests have been provisioned.
- Mass update all tests on a device a custom or default action after tests have been provisioned.

16.2.2 Test Autodiscovery

For some monitors (test types), NetVigil can automatically discover which tests are supported by a given device. For example, if you add a new router to your network, NetVigil can discover which SNMP tests the router supports. You can then select which of the supported tests you want to run. Alternately, if you know exactly which tests you want, you can skip the auto-discovery process and provision those tests manually.

16.2.3 Grouping Tests by Subtype

One test configuration option, **Group all SNMP tests with same type and sub-type together**, only appears when you choose to auto-discover SNMP tests. The option gives the following advantages:

- Compact, organized display of discovered tests (especially useful for large devices)
- Mass configuration of thresholds and action profiles for similar tests

If the grouping option is not selected, every discovered SNMP test is listed individually, as shown in Figure 16.3. You can set a separate test interval, warning threshold, critical threshold, and action profile for each test.

test-server-01 - Vendor: Linux Version: 2.4.18-3

snmp Tests							
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Test Name:	Interval:	Thresholds (warn/critical):		Units:	Action Profile:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	System Load Avg	5 min	6	8		None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Block IO Sent	5 min	200	400	b/s	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Block IO Rcvd	5 min	200	400	b/s	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	System Interrupts	5 min	200	400	i/s	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Swap in from Disk	5 min	1000	2000	kb/s	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Swap out to Disk	5 min	1000	2000	kb/s	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	User CPU Time	5 min	85	95	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	System CPU Time	5 min	85	95	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Logged In Users	5 min	50	100	users	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Application/Process Count	5 min	150	500	apps	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	PhyMemUsed	5 min	40	90	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	VirtMemUsed	5 min	90	100	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disk /	5 min	75	90	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disk /boot	5 min	75	90	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disk /var	5 min	75	90	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	eth0 Status	5 min	2	2		None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	eth0 Util In	5 min	70	85	%	None
<input checked="" type="checkbox"/>	<input type="checkbox"/>	eth0 Util Out	5 min	70	85	%	None

Figure 16.3 Discovered SNMP tests, listed individually

If the grouping option is selected, discovered tests with the same subtype are grouped together. Figure 16.4 shows the results of auto-discovery of SNMP tests for the same device as the one shown in Figure

16.3. However, in this image, discovered tests are grouped by subtype. For example, the **eth0 Util In** and **eth0 Util Out** tests are grouped under the **snmp/bandwidth (Interface Utilization)** test subtype.

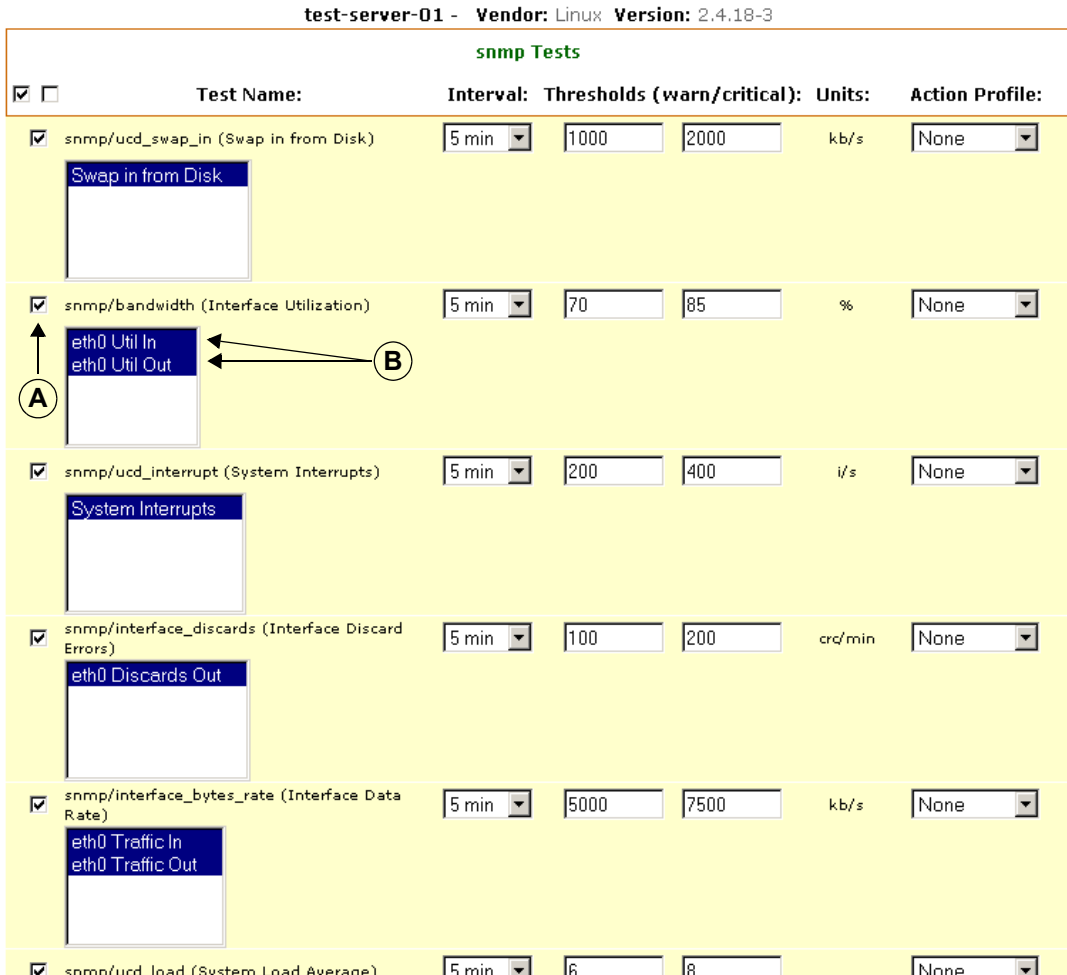


Figure 16.4 Discovered SNMP tests, grouped by subtype

You can select/clear the checkbox near a subtype name (item A in Figure 16.4) to provision/not provision all tests within that subtype. To provision some, but not all, tests within a subtype, make sure that the

subtype checkbox is selected. Then, from the list of tests within the subtype (item B in Figure 16.4), select only those that you want to provision.

The configuration parameters that you set (Interval, Thresholds, Action Profile) for a subtype are applied to all selected tests within the subtype. You can change the configuration for an individual test after it is provisioned.

This grouping feature is useful when you have many tests of the same subtype for a single device. For example, assume that you have a large switch with 100 ports, each of which supports Util In and Util Out interface utilization tests. If the grouping option is not selected, the list of discovered tests has 200 entries for these tests. If the grouping option is selected, the list of discovered tests is more compact, and instead of configuring and provisioning 200 tests, you can configure and provision a single subtype, **snmp/bandwidth (Interface Utilization)**. The Interval, Thresholds, and Action Profile selected for the subtype are applied to all tests in the group. (You can change the configuration for individual tests after the tests are provisioned.)

NOTE: Internal settings in the TestType.xml file may sometimes override the **Group all SNMP tests...** option because of which some test subtypes may always be grouped, even if you do not select the grouping option.

❑ To create standard tests:

1. Click `MANAGE | devices`.
2. In the Manage Devices window, find the device for which you want to provision tests.
 - ▶ If the device already has tests provisioned, click **Tests** and continue with Step 3.
 - ▶ If no tests are provisioned for the device, click **Create Tests** and continue with Step 4.
3. In the Manage Tests window click **Create New Standard Tests**.

4. In the Add Standard Tests window, from the **Available test types** list, select those categories that include tests that you want to provision for this device. Optionally, select **Perform auto-discovery of supported (*) test types**. NetVigil can perform auto-discovery for any test type marked with an asterisk (*).
5. Click **Add Tests**.
6. If one or more of the selected test types include multiple subtypes, you must refine your search by choosing the subtypes that you want to provision. (If you did not select any test type that contains multiple subtypes, continue with Step 9.) In the Create New Tests - Step 2 window, select the subtypes that you want to provision. For example, if you chose to provision ping tests, you can now choose to provision either or both of the subtypes: Packet Loss and Round Trip Time.
7. Optionally, select one or more of the following:
 - ▶ **If one or more already provisioned tests are discovered, show a duplicate instance instead of ignoring them**

If this option is cleared and NetVigil discovers a provisioned test of this subtype for this device (e.g., a Packet Loss test is already configured for this device), the test subtype does not appear in the list of tests that you can choose to provision.

If this option is selected and NetVigil discovers a provisioned test of this subtype for this device, the test subtype is listed and you can provision another test of the same subtype for the device.

If this option is not selected, but some of the configured parameters for the test do not match the re-discovered parameters (such as max, oid, etc.), then the test is displayed so that you have the option to update the values.
 - ▶ **Group all SNMP tests with same type and sub-type together**

This is only available if you have chosen to autodiscover SNMP tests. See “Grouping Tests by Subtype” on page 205 for a detailed explanation of this option.
8. Click **Continue**.
9. If you have chosen to autodiscover tests, please wait for the discovery process to complete. This may take a short time.

10. In the Create New Tests: Step 3 window, select those tests that you want to provision. (If you've chosen to group SNMP tests by subtype, select subtypes and, optionally, individual tests within subtypes.) For each test, enter the following:

Field	Used For
Test Name	A unique identifier for this test.
Interval	The frequency, in minutes, at which the test will run.
Thresholds/Units	If the test result passes the number of units specified by the Warning or Critical threshold, the test goes into Warning or Critical state, respectively.
Action Profile	The action (or series of actions) to be taken when the test enters specific states.

If you've chosen to group SNMP tests by subtype, these parameters are applied at the subtype level -- that is, to all selected tests within the subtype.

11. Click **Provision Tests**. The newly provisioned test(s) appear in the Manage Tests window.

☐ To update an existing test:

1. Go to the Manage Tests page for the device being tested (see Figure 16.5).
2. Click on the **Update** link for the test you want to modify and you will be taken to the Update Test page.
3. Make the desired changes.

4. Click on the **Update** button to complete the changes.

The screenshot shows the NetVigil web interface. At the top right, the date and time are 8/29/02 9:11:45 PM GMT. The navigation bar includes links for STATUS, REPORTS, MANAGE, and HELP. Below the navigation bar, there are breadcrumb links: [devices](#) --- [services](#) --- [actions](#) --- [user](#) --- [password](#) --- [logout](#) --- [-----](#) |. The main heading is "Manage Devices" with a sub-link "[Create A Device](#)". Below this, it says "Displaying 1 - 15 of 15" and shows a search input field. The main content is a table with columns: DEVICE NAME, DEVICE ADDRESS, TYPE, STATUS, and LOCATION. The table lists 10 devices. Two devices, "aisoft-tech.com" and "pugmarks.net", have a red 'X' icon in the STATUS column. Below the table, there is a summary bar with a red 'X' icon and the text "suspended".

DEVICE NAME	DEVICE ADDRESS	TYPE	STATUS	LOCATION	
studyukguide.com	203.129.220.106	Windows NT/2K/XP		Denver	Update Suspend Tests
aisoft-tech.com	192.168.123.100	Linux/Other Unix		Denver	Update Resume Tests
djrummy.net	204.0.23.217	Linux/Other Unix		Englewood	Update Suspend Tests
dhrugroup.com	10.10.124.11	Linux/Other Unix		Denver	Update Suspend Create Tests Create Custom Tests
trisyscom.com	11.11.125.12	IP Router		Denver	Update Suspend Tests
baseinformation.com	192.168.123.25	Linux/Other Unix		Denver	Update Suspend Create Tests Create Custom Tests
maxateev.com	192.168.123.254	IP Router		Denver	Update Suspend Tests
server1.fidelia.com	192.168.123.1	Linux/Other Unix		Denver	Update Suspend Tests
support.fidelia.com	10.10.123.1	Linux/Other Unix		Englewood	Update Suspend Tests
pugmarks.net	112.117.123.11	Windows NT/2K/XP		Denver	Update Resume Tests
pugmarks.com	10.10.124.11	Windows NT/2K/XP		Denver	Update Suspend Tests

suspended

Figure 16.5 Manage Tests Page

□ To suspend or resume a test:

NOTE: When you resume a suspended test, the test is rescheduled to run on the monitor. If you visit the Test Summary page for the device that the test is on, you may see an unknown (question mark) icon in the status column. This indicates that the test has been rescheduled, but that its status is not yet known because it hasn't yet run. After the test runs, the unknown icon is replaced with the appropriate status icon.

1. Click `MANAGE | devices`.
2. On the Manage Devices page, find the device whose test(s) you want to suspend or resume, and then click **Tests**.
3. On the Manage Tests page, select the test(s) you want to suspend or resume in the **Select** column.
4. In the **Apply the following updates to the tests selected above:** area, select **Suspend** or **Resume**, as appropriate, from the **Modify Test:** list.
5. Click **Submit** to suspend or resume the test(s).

□ To delete a test:

1. Click `MANAGE | devices`.
2. On the Manage Devices page, find the device whose test(s) you want to delete, and then click **Tests**.
3. On the Manage Tests page, select the test(s) you want to delete in the **Select** column.
4. In the **Apply the following updates to the tests selected above:** area, select **Delete** from the **Modify Test:** list.
5. Click **Submit** to delete the test(s).

16.3 Managing Advanced Tests

16.3.1 Monitoring Databases Using SQL Query

You can issue a SQL query against supported databases in Netvigil. On the test provisioning page, select the driver from the drop down list and a properly formatted SQL query in the text box.

As an example:

```
Port : 7663
Driver Class : MySQL
Database : aggregateddatadb
Query : select id from Validation Table
Username : emerald
Password : xxxxx
```

In order to monitor a MySQL database:

1. click on manage -> devices -> tests
2. click on "create new standard tests"
3. select "sql_query" monitor, click on "add tests"
4. use following parameters for resulting test

```
test name = MySQL : Database: Status
driver class = MySQL
query = show tables;
database = mysql
username = user allowed to log into database (e.g. "root")
password/again = password for above user
port = tcp port for MySQL (e.g. 3306)
```

5. make sure the checkbox next to test name is selected, submit form

If the database is not running, the test will return FAIL status. Otherwise, the test will show time taken to perform the "show table;" query. As a caution, the username that is used for this test must be allowed to access the database specified remotely. See following documents regarding access control requirements:

```
http://dev.mysql.com/doc/mysql/en/Remote_connection.html
http://dev.mysql.com/doc/mysql/en/Connection_access.html
http://dev.mysql.com/doc/mysql/en/Access_denied.html
```

16.3.2 URL Transaction Tests

You can create a URL transaction test in NetVigil which can connect to a web site, fill in a form, click on various hyperlinks, etc. so as to simulate a real user. This is a very powerful feature in NetVigil which allows testing the response time and errors in most web enabled applications.

The system is fairly intuitive with context sensitive help and has a mini-browser that displays the various stages of the URL transaction. You can then save and even export/import this transaction for other sites.

The steps to create a transaction script are:

1. Click on the modify icon for any device, and click on “create new custom tests”
2. Scroll down to “web transaction test” and click on “manage web transaction test scripts”
3. Click on “create web transaction script”
4. Select “no” if you are not behind a proxy (typically the case)
5. Enter the URL you wish to monitor. This would be the same URL you would use when accessing the site in question using a browser. For tomcat monitoring, this would be `http://your_web_app_host/logon.jsp`. If you wish to use the same script for multiple web servers, select the “replace this url hostname...” option. Click “next”
6. The URL you have entered will be loaded and presented on a small window. This window is meant to show your progress on the web transaction...do not click on any links on this window
7. Various elements found on the page will be displayed to you on subsequent pages. You would select the element (e.g. form, link) and an item from the selected element. e.g. for NetVigil webapp, if you wanted to login you would select the “form” element “logonForm” and click “next”
8. Depending on what element/item you choose, you will be presented with corresponding options and as you progress through the transaction, the small web window would show which page you are in. You can always consult this small window to determine which element/item you would want to pick from the transaction monitor
9. When you have completed the session, it is time to close out the transaction script, so click on “finished”. The small window will be closed automatically
10. Provide a unique name for the script and if you wanted to search for a specific text message during the session, you can enter it also
11. Go back to device summary and click on modify icon for a device which has a web server running and is serving the content for which the script was created

12. Click on “create new custom tests” and scroll down to “web transaction test”
13. Check the “provision?” box, provide a test name (e.g. NetVigil WebApp) and select the newly created script from drop-down list of “test script”
14. Click “provision tests”

16.3.3 Advanced SNMP Tests

NetVigil automatically detects standard MIBs and their tests. To run a test that is part of a vendor-specific MIB, you can create an Advanced SNMP Test containing the OID of the vendor-specific test.

□ To create an Advanced SNMP test:

1. Click `MANAGE | Devices`.
2. On the Manage Devices page, find the device for which you want to create a test and click **Tests**.
3. On the Manage Tests page, click **Create New Advanced Tests**.
4. On the Create Advanced Tests page, select the **Advanced SNMP Test** option. Fill in the test name, test **Interval**, warning and critical **Thresholds**, and, if desired, an **Action Profile**. Then fill in the following:

Table 16.1 Advanced SNMP Test Fields

Field	Purpose
SNMP Object ID	The OID of the vendor-specific test that you want NetVigil to poll.
Result Multiplier	A number by which each test result is multiplied. If a test returns a number of bytes, for example, you can use a Result Multiplier of 8 to convert the result to bits.
Maximum Value	Maximum possible return value for this test. You can generally ignore this unless you are using the test result to calculate a percentage of a whole. In that case, enter the value of the whole in this field. For example, if a test returns the number of MB available on a disk and you want to calculate the percentage of the disk’s storage space that is available, enter the disk’s total storage space in this field.

Table 16.1 Advanced SNMP Test Fields

Field	Purpose
Post Processing Directive	<p>The computation applied to the test result after it has been multiplied by the Result Multiplier. Options include:</p> <ul style="list-style-type: none"> • <code>Delta</code> = current polled value - last polled value (e.g., 3 MB of disk space used since last poll) • <code>Rate</code> = <code>Delta</code> / time between polls (e.g., rate of disk usage is 3 MB in 5 minutes) • <code>Delta Percent</code> = (current polled value - last polled value) / Maximum Value (e.g., the difference between the current value and the last value represents 2% of total disk space) • <code>Reverse Percent</code> = the difference between 100% and the percentage represented by the last polled value (e.g., last polled value for a disk usage test represents 20% of total disk space, so the reverse percent is 80%, which is the amount of free space) • <code>Rate Percent</code> = percentage change since the last poll (e.g., rate of change measured as a percentage of the whole is 2% of total disk space in 5 minutes) • <code>Percent</code> = current polled value / Maximum Value (e.g., current polled value represents 20% of total disk space) • <code>None</code> = polled value is not processed in any way

Table 16.1 Advanced SNMP Test Fields

Field	Purpose
Test Units	The units in which test results are displayed.
As test value rises, severity:	<p>Specify the relationship between test value and severity. Options include:</p> <ul style="list-style-type: none"> • Ascends: As the value of the test result rises, severity rises. • Descends: As the value of the test result rises, severity falls. • Auto: If you select this option, NetVigil sets this option based on the Warning and Critical thresholds for this test. If the Critical threshold is higher, as test value rises, severity ascends. If the Warning threshold is higher, as test value rises, severity descends. • Discrete: You can set fixed integers or ranges of numbers using the syntax: 1,3,5,11-20

5. Click **Provision Tests**.

16.3.4 Advanced Port Tests

Advanced Port Tests allow you to send a text string to a TCP port, then check the response against an expected string (the return string does not have to be a perfect match, only a substring match).

□ To create an Advanced Port test:

1. Click **MANAGE | Devices**.
2. On the Manage Devices page, find the device for which you want to create a test and click **Tests**.
3. On the Manage Tests page, click **Create New Advanced Tests**.

4. On the Create Advanced Tests page, select the **Advanced Port Test** option. Fill in the test name, test **Interval**, warning and critical **Thresholds**, and, if desired, an **Action Profile**. Then fill in the following:

Table 16.2 Advanced Port Test Fields

Field	Purpose
Send String	The string to be sent to the remote TCP port.
Expect String	The string against which the remote port's response is checked. The Action Profile is activated when the response is a substring match for the Expect String .
Port	The TCP port on this device to which the DGE will send the Send String .

5. Click **Provision Tests**.

The DGE connects to the target port specified, transmits the “send” string if one is specified and then performs a case-insensitive sub-string match for the “expect” string if one is specified. As an example, to monitor if the sshd TCP port is alive and responding:

```
test Name: sshd service
send string: (blank)
expect string: SSH
port: 22
```

If you just want to test connectivity to a TCP port, leave the “expect” string blank.

To note that it is also possible to send a multi-line string when setting up the above test by separating each line with `\r\n` (carriage return + line feed).

□ How to test if TCP port is alive

This can be accomplished by creating an advanced port test and not specifying any send/expect strings. For example, if you wish to monitor port 7000 on device “my_device”, click on manage -> devices -> tests (next to my_device) -> create new advanced tests) and provide the following parameters:

test name: (as you see fit)

send string: (blank)

expect string: (blank)

port: 7000

Now the DGE will test to make sure that my_device is accepting incoming connections on port 7000 at the specified interval.

16.3.5 External Tests

An External Test is one that is run outside of NetVigil (by a standalone script, for example). The test result is inserted into NetVigil via the External Data Feed (EDF) and aggregated as though NetVigil had collected it. Although the test itself is not run by NetVigil, by creating an External Test, you determine how test results will be processed after they are received via EDF.

□ To create an External test:

1. Click **MANAGE** | **Devices**.
2. On the Manage Devices page, find the device for which you want to create a test and click **Tests**.
3. On the Manage Tests page, click **Create New Advanced Tests**.
4. On the Create Advanced Tests page, select the **External Test** option. Fill in the test name, test **Interval**, warning and critical **Thresholds**, and, if desired, an **Action Profile**. Then fill in the following:

Table 16.3 External Test Fields

Field	Purpose
Test Units	The units in which test results are displayed.
Maximum Value	Maximum possible return value for this test. You can generally ignore this unless you are using the test result to calculate a percentage of a whole. In that case, enter the value of the whole in this field. For example, if a test returns the number of MB available on a disk and you want to calculate the percentage of the disk's storage space that is available, enter the disk's total storage space in this field.

Table 16.3 External Test Fields

Field	Purpose
Result Multiplier	A number by which the test result is multiplied. If a test returns a number of bytes, for example, you can use a Result Multiplier of 8 to convert the result to bits.

Table 16.3 External Test Fields

Field	Purpose
Post Processing Directive	<p>The computation applied to the test result after it has been multiplied by the Result Multiplier. Options include:</p> <ul style="list-style-type: none"> • <code>Delta</code> = current polled value - last polled value (e.g., 3 MB of disk space used since last poll) • <code>Rate</code> = <code>Delta</code> / time between polls (e.g., rate of disk usage is 3 MB in 5 minutes) • <code>Delta Percent</code> = (current polled value - last polled value) / Maximum Value (e.g., the difference between the current value and the last value represents 2% of total disk space) • <code>Reverse Percent</code> = the difference between 100% and the percentage represented by the last polled value (e.g., last polled value for a disk usage test represents 20% of total disk space, so the reverse percent is 80%, which is the amount of free space) • <code>Rate Percent</code> = percentage change since the last poll (e.g., rate of change measured as a percentage of the whole is 2% of total disk space in 5 minutes) • <code>Percent</code> = current polled value / Maximum Value (e.g., current polled value represents 20% of total disk space) • <code>None</code> = polled value is not processed in any way

Table 16.3 External Test Fields

Field	Purpose
As test value rises, severity:	<p>Specify the relationship between test value and severity. Options include:</p> <ul style="list-style-type: none"> • Ascends: As the value of the test result rises, severity rises. • Descends: As the value of the test result rises, severity falls. • Auto: If you select this option, NetVigil sets this option based on the Warning and Critical thresholds for this test. If the Critical threshold is higher, as test value rises, severity ascends. If the Warning threshold is higher, as test value rises, severity descends. • Discrete: You can set fixed numbers or ranges using the syntax: 1,3,5,11-20

5. Click **Provision Tests**.

16.4 Suppressing Tests

When you suppress a test, it continues to run at the specified interval and trigger events, notifications, etc., but its status does not affect the overall status of any associated device, Service Container, or Department. When the status of the test changes (e.g., from WARNING to CRITICAL or from CRITICAL to OK), the test is automatically unsuppressed and NetVigil again takes the test’s status into account for determining device, Service Container, and Department status.

In the default sort order of the Device Details and All Tests Summary pages, suppressed tests appear at the bottom of the list with a single arrow to the left of the status icon. (For additional information, see “To see which tests are suppressed:” on page 224.)

IMPORTANT: A **suppressed** test continues to run, but its status does not affect the overall status of related objects. A **suspended** test stops running and does not trigger events, notifications, etc. until it is **resumed**.

For example, assume that a device has two network tests configured. When both tests have status OK, the overall status of the device in the **Network** column of the Device Summary Page is OK. If one of these tests goes into WARNING state, the overall status of the device in the **Network** column of the Device Summary Page changes to WARNING. However, if you suppress the test that is in WARNING state, the status of the remaining tests determines device status. In this case, there is only one other test, with status OK, so the overall device Network status is OK.


If the suppressed test returns to status OK, it is no longer suppressed. The next time its status becomes WARNING, overall device status will also become WARNING, unless you suppress the test once again.

□ To suppress a test:

1. Click `MANAGE | devices`.
2. On the Manage Devices page, find the device for which you want to suppress a test, and click **Tests**.
3. On the Manage Tests page, find the test(s) that you want to suppress, and select their checkboxes in the **Select** column.
4. At the bottom of the Manage Tests page, in the **Apply the following updates to the tests selected above** area, select **Suppress** from the **Modify Tests** list, and then click **Submit**.

The suppressed tests at the bottom of the list on the All Tests Summary and Device Test Summary pages, and are marked by a single arrow to the left of the Status icon.

□ To unsuppress a test:

1. Click `STATUS | Tests`. By default, suppressed tests appear at the bottom of the All Tests Summary page, with a single arrow to the left of the **Status** icon.
2. On the All Tests Summary page, select a suppressed test and click the corresponding **Modify**  icon.
3. On the Update Test page, in the **Update Test Parameters** area, clear the **Suppress** checkbox, and then click **Submit**. On the All Tests Summary page, the test returns to its normal position in the list and no longer has a single arrow to the left of the **Status** icon.

□ To see which tests are suppressed:

1. Click `STATUS | Tests`. By default, suppressed tests appear at the bottom of the All Tests Summary page, with a single arrow to the left of the **Status** icon.

16.5 Smart Thresholds Using Baselines

Baselining is a process by which NetVigil can automatically set the Warning and Critical thresholds for each test based on the test's historical data. This allows one to set customized thresholds automatically based on each test's individual behavior.

As an example, the response time for a local device is normally much smaller than the response time for a device in a remote datacenter because of network latency. Rather than setting the response time Warning threshold for all devices to be the same, you can use the baseline feature to calculate the 95th percentile of the response time reported for each device over a three-month period, and then set the Warning threshold to be 10% higher than this 95th percentile value.

The Baseline Data Set

The baseline value is calculated for each test based on its own historical data. You select the devices and tests for which you want to run baselining by specifying a combination of device name, test name and test type.

Each time NetVigil aggregates a test result, it stores three values: The minimum, maximum, and mean values of the tested variable over the course of the aggregation period. For example, if NetVigil is configured to store data for 1 day at 10 minute samples, and a test is set up to run every 10 minutes, in the course of a day it generates 144 test results. Each test result includes the maximum, minimum, and mean values of the tested quantity for the 10 minute period. You can generate a baseline from the maximum, minimum, or mean samples within the specified date range.

Managing Baselines

The table that follows explains the items on the Baseline Management page:

Table 16.4 Baseline Management fields

Field	Purpose
Device Name/RegExp	The name of a device whose tests are to be baselined, or a regular expression containing '*' wildcards to match multiple device names.
TestName/RegExp	The name of an individual test to be baselined, or a regular expression containing the '*' wildcards to match multiple test names.
Test Type/Subtype	The Monitor and Subtype of the test(s) to be baselined. e.g. port/http, snmp/chassis_temp
Start Date, End Date	The start and end date of the test results to be used in calculating the baseline. NOTE: Each selected test must have test results available for the full date range.
Taking values of	The value from each test result (maximum, minimum, or mean) that is used to calculate the baseline. See "The Baseline Data Set" on page 224 for more information.
And using the	The method (average or 95th percentile) used to calculate the baseline from the maximum, minimum, or mean test results. average is the mean of the test results (sum of test results / number of test results).
Warning Threshold	A percentage above or below the calculated baseline. Select above if the test result gets worse as it gets higher. Select below if the test result gets worse as it gets lower. When the test result crosses this threshold, test status is set to Warning .
Critical Threshold	A percentage above or below the calculated baseline. Select above if the test result gets worse as it gets higher. Select below if the test result gets worse as it gets lower. When the test result crosses this threshold, test status is set to Critical .

To create a baseline and set thresholds for one or more tests:

1. Select the **MANAGE** tab.

2. On the Manage Devices page, click **Test Baseline Management**.
3. Specify the Device(s), Test Name(s), and Test Type/Subtype of the tests you want to baseline.
4. Enter the date range of the test results to be used in calculating the baseline.
5. Near **Taking values of:**, specify whether you want the baseline to be calculated from the `maximum`, `minimum`, or `mean` values of the test results (see “The Baseline Data Set” on page 224 for more information).
6. Near **And using the:**, select a method for calculating the baseline from the selected results.
7. Correlate the Warning and Critical Thresholds to the baseline. For each threshold, enter a percentage above or below the baseline, and then click **Submit**.
8. The system calculates the baselines- this step might take some time depending on the amount of data to be processed.
9. Once the baselines are calculated, the Test Baseline Management window is displayed which lists each test that matches your search criteria along with the current thresholds (in the **Old Warn/Crit** column) and the new values that have been calculated from the baseline (in the **New Warn/Crit** column). At this point, thresholds have not yet changed. Select those tests whose thresholds you want to change, and then click **Done**.

NOTE If you access the Test Baseline Management page from either the Manage Tests page or the Update Test page, some of the Baseline Management information is filled in.

16.6 Configuring Test Schedules

You can configure a time schedule (hour and day of week) for running a test, and assign this schedule to a test. By default, the test schedule is 24x7 (all the time). These schedules are stored in your local timezone specified in Manage->Prefs.

Update Schedule
Fill in information for the schedule below. Click Update Schedule to confirm. Example: for 9am-5pm, select the checkboxes from 9a to 4p

* Schedule Name:

Schedule Description:

	12a	1	2	3	4	5	6	7	8	9	10	11	12p	1	2	3	4	5	6	7	8	9	10	11
Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mon	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thu	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fri	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

❑ To create a new test schedule:

1. Select **MANAGE** | **other**.
2. On the Manage Links page, click **Manage Test Schedules**.
3. On the Manage Schedules page, click **Create a schedule**.
4. On the Create Schedule page, enter a **Schedule Name** and, optionally, a **Schedule Description**. Then select the hours of the day on those days of the week on which you want this schedule to run. You can select or clear an entire row or column at a time by clicking the row or column header.
5. Selecting the checkbox for an hour means all minutes in that hour, e.g. 5:00 to 5:59
6. Click **Create Schedule**.

□ **To schedule a test:**

1. Click `MANAGE | devices`.
2. On the `Manage Devices` page, find the device whose test(s) you want to schedule, and then click **Tests**.
3. On the `Manage Tests` page, select the test(s) you want to schedule in the **Select** column.
4. In the **Apply the following updates to the tests selected above:** area, select the schedule that you want to apply from the **Test Schedule** list.
5. Click **Submit** to schedule the test(s).

16.7 Device Dependency

In network environments, switches, routers, etc. are often the physical gateways that provide access to other network devices. If critical “parent devices” are unavailable, monitoring may be impeded for devices that are accessed via the parents. To distinguish between devices that are genuinely in a `CRITICAL` state and those that are `UNREACHABLE` because of a problem with one or more parent devices, you can create device dependencies.

A device dependency is a parent-child relationship between monitored devices. A single parent can have multiple children, and a single child can have multiple parents. Device dependencies are cascading. If A is a child of B, and B is a child of C, it is only necessary to configure A as a child of B and B as a child of C. NetVigil automatically recognizes the dependency between A and C.

If a device is tested and the result is `CRITICAL` (for all thresholds), `UNKNOWN`, or `FAILED`, some additional processing is used to determine if the device is reachable.

1. A current packet loss test is examined for the device. If such a test exists and packet loss is not 100%, the device is considered reachable.
2. If no packet loss test exists, all immediate parent devices are examined. If the device has no parents, it is considered reachable and the result of the test is the measured value. If all parents have a current packet loss test which was measured at 100%, the device is considered unreachable.

3. If no packet loss test exists for the parent, or no recent test result is found for an existing packet loss test, the child device is considered reachable and the result of the test is the measured value.

Dependency Restrictions

Device dependencies must conform to these rules:

1. Circular dependency is not allowed. For example, if you set up the following dependencies:

Device A **depends on** Device B **depends on** Device C

You cannot configure Device C to depend on Device A.

2. Parent and child devices must belong to the same DGE Location.

To configure device dependency:

1. Create the parent device
2. Create the child device
3. Click `MANAGE | devices`.
4. On the Manage Devices page, find the device that will be the *child* device in the dependency and click **Update**.
5. On the Update Device page, click **Update Device Dependency**.
6. On the Update Device Dependency page, select the device or devices on which this child depends from the **Does Not Depend On** list, and then click **Done**. (If you return to the Device Dependency page you will see that the parent device(s) appear in the **Depends On** list).

NOTE: Device dependencies are cascading. If A is a child of B, and B is a child of C, it is only necessary to configure A as a child of B and B as a child of C. NetVigil automatically recognizes the dependency between A and C.

The next time the parent device has a CRITICAL ping/pl test result, the child device will have UNREACHABLE status.

16.8 Managing Account Preferences

To update your personal information, preferences, and/or password:

1. Click on the **MANAGE** tab on the main navigation bar.

2. Click on the **prefs** tab on the secondary navigation bar and you will be taken to the Update User page.
3. Enter any changes desired. Modifiable fields include: **E-mail, day phone, evening phone, mobile phone, pager, timezone,** and **password**. Please contact your administrator if you wish to modify your contact address.
4. In the **Preferences** section, select the checkboxes for all the device states you wish to view on the summary pages, leaving blank all those you wish to filter out by default.
5. Change the number of devices to view on each page in the **Maximum To Display** field.
6. Click the **Update User** button to save your changes.
These changes will become part of your user profile and will serve as defaults each time you log in to NetVigil.