

Chapter 9



Administrator Action Profiles & Thresholds



9.1 Overview

NOTE: This chapter describes Action Profiles and notifications that are configured by Administrators. For information on Action Profiles and notifications configured by end-users, “Managing Action” in the Web User Guide.

When a test result crosses a threshold, NetVigil takes action based on rules called Action Profiles. Some possible actions are:

- E-mail (requires setting up of an outbound mail relay in `netvigil.xml`)
- Pager via E-mail
- Sending SNMP traps
- Opening trouble-tickets in Remedy or RT
- Running an external script (to reboot or restart a process)

An Action Profile specifies one or more actions and the conditions under which each action occurs. For example, an Action Profile can be configured to send an E-mail when a device is first detected down, then page after another test cycle and reboot if the condition persists after five test cycles. You can also suppress alarms, auto-clear suppressed alarms during maintenance, etc. Additionally, Chapter 26, “Plugin Actions” describes how you can build your own custom plug-in actions to extend the notification framework.

9.2 Action Profiles Created by End-Users

End-users can configure their own Action Profiles, which are available to all end-users within the same Department. End-user configured Action Profiles can specify a variety of actions and multiple recipients. For additional information, see “Managing Actions” in the Web User Guide.

9.3 Action Profiles Created by Administrators

Administrators can create two types of Action Profiles: User-Class Action Profiles and Administrator Action Profiles. These are described in detail in the sections that follow.

9.3.1 User-Class Action Profiles

User-Class Action Profiles are used as defaults for tests created by end-users associated with a particular User-Class. These Action Profiles send E-mail to the Department’s default E-mail address when tests cross standard test thresholds. No other action types or recipients can be configured. To generate different types of actions (e.g, alphanumeric paging) or to specify recipients other than the Departmental E-mail account, end-users must create their own Action Profiles.

Default Action Profiles are assigned on a User-Class/test type basis. That is, within a User-Class every test type has its own default Action Profile. When an Administrator configures a default Action Profile for a test type, this becomes the default setting for all Departments associated with the User-Class. A single User-Class Action Profile can be assigned to multiple test types within the User-Class.

For example, assume that an Administrator creates a User-Class Action Profile named PING-DEFAULT for a User-Class named ENGINEERING-RW. This Action Profile specifies that if a test goes into WARNING state, an E-mail message is sent to the Department’s E-mail address. If the test goes into CRITICAL state, another E-mail message is sent. The Administrator sets PING-DEFAULT as the default Action Profile for ICMP RTT and packet loss tests. Subsequently, when an end-user from any of the Departments associated with the ENGINEERING-RW User-Class creates an ICMP RTT test, the Action Profile is PING-DEFAULT, unless the end-user changes it.

For procedures related to User-Class Action Profiles, see Section 9.5.1, “Managing User-Class Action Profiles” on page 137.

NOTE: The mere creation of a User-Class Action Profile does not cause actions to occur. An Action Profile must be assigned to one or more test types in order for actions to take place.

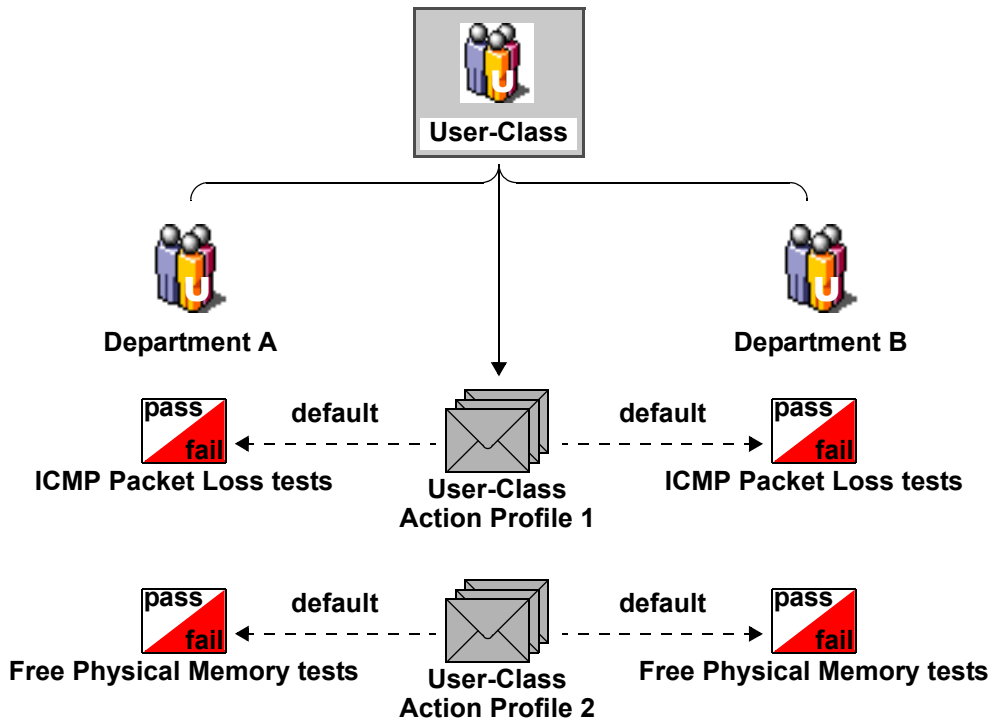


Figure 9.1 Using User-Class Action Profiles as defaults for end-user tests

9.3.2 Administrator Action Profiles

Administrator Action Profiles can perform different kinds of actions and notify multiple recipients when tests cross Admin or SLA thresholds. (For additional information on Admin and SLA thresholds, see Section 9.4.2, “Admin and SLA Thresholds” on page 135.) An Administrator Action Profile is available to all Administrators associated with a given Admin-Class.

For procedures related to Administrator Action Profiles, see Section 9.5.3, “Managing Administrator Action Profiles” on page 139.

NOTE: The mere creation of an Administrator Action Profile does not cause actions to occur. An Action Profile must be assigned to one or more test types in order for actions to take place.

9.3.3 Comparing User-Class and Administrator Action Profiles

The two types of Administrator-created Action Profiles are summarized in the table that follows:

Type of Action Profile	Possible Actions	Who is Notified?	What Thresholds Trigger Notification?	Notes
User-Class Action Profile	E-mail only	Departmental E-mail address	Regular test thresholds	Used as a default Action Profile for tests created by end-users. Applies to all Departments associated with a single User-Class.
Administrator Action Profile	All	Configured E-mail address(es); should be Administrator addresses	SLA and Admin Thresholds	Used in SLA and Admin Action Profiles. Available to all Admin-Groups associated with a single Admin-Class.

9.4 Thresholds Configured by Administrators

9.4.1 User-Class Default Thresholds

User-Class default thresholds, which are configured for each User-Class/test-type, are the default values for tests created by end-users. That is, within a User-Class every test type has its own default WARNING and CRITICAL thresholds. When an Administrator configures a default threshold for a test type, this becomes the default setting for all Departments associated with the User-Class.

For example, assume that an Administrator configures default thresholds for a User-Class named ENGINEERING-RW. He sets the defaults for ICMP Round Trip Time tests to 200 ms for the WARNING threshold and 250 ms for the CRITICAL threshold. Subsequently, when

an end-user from any of the Departments associated with the ENGINEERING-RW User-Class creates a Ping RTT test, the CRITICAL and WARNING thresholds will be 200 and 250 ms, respectively, unless the end-user changes them.

For procedures related to User-Class default thresholds, see Section 9.5.2, “Setting Default Action Profiles and Thresholds for User-Classes” on page 138.

9.4.2 Admin and SLA Thresholds

Admin and SLA thresholds, which are distinct from the thresholds that can be configured by end-users, enable Administrators to get separate reports and alarms without creating additional tests. **Admin thresholds**, which are configured for both WARNING and SEVERITY levels, enable Administrators to get notifications and generate reports based on events that are of interest only to Administrators (these thresholds were earlier referred to as Shadow Thresholds). **SLA thresholds**, which are configured at one level only, allow both Administrators and end-users to see whether Service Level Agreements are being met. A single test result that crosses Admin, end-user, and SLA thresholds can generate three separate events based on each of the three types of thresholds.

NetVigil’s ability to generate different events based on the same test results provides the following benefits:

- Increased efficiency: Using a single test to generate multiple results means less time spent configuring tests and less network traffic.
- Increased accuracy: If separate thresholds are compared with separate test results, data will be inconsistent. For example, assume that two ICMP packet loss tests are configured for the same device. The results of one test are checked against an end-user threshold, while the results of the other test are checked against an Admin threshold. A short-lived outage that is detected by the end-user test may be over before the Administrator test next polls the device. Consequently, end-user reports will reflect the outage, while Administrator reports will not.

Checking the same result against end-user, Admin, and SLA thresholds preserves data consistency.

Both SLA and Admin thresholds are configured by a NetVigil Administrator on a User-Class/test type basis. In other words, an SLA or Admin threshold that is configured for ICMP Packet Loss tests for a given User-Class is applied to all ICMP Packet Loss tests created by end-users associated with that User-Class.

For example, assume that the head of the IT division for an organization has an SLA that guarantees that response time on the network will stay below 50 ms. To check this, she sets the SLA threshold for Round Trip Time to 50 ms. At the same time, an end-user creates a Round Trip Time test for one of his servers. He finds any RTT below 75 ms acceptable, so he sets the Warning and Critical thresholds to 75 and 85 ms, respectively. During one polling interval, the recorded Round Trip Time is 65 ms. Because this falls below the end-user thresholds, it does not trigger a user event, and if the end-user runs a device instability report, the server does not appear. However, the polled result does exceed the SLA threshold, so an SLA violation event is recorded. If the Administrator runs an event report against SLA thresholds, she will see that Departments associated with this User-Class are not getting the performance promised in the SLA.

Alternately, the head of the IT division may not want to be notified of Round Trip Time delays unless they exceed 100 ms. By creating an Admin threshold with a value of 100 ms and an Administrator Action Profile based on that threshold, the Administrator ensures that she is only notified when the situation warrants her attention.

For procedures related to Admin and SLA thresholds, see Section 9.5.4, “Setting Admin Action Profiles and Thresholds” on page 140 and Section 9.5.5, “Setting SLA Action Profiles and Thresholds” on page 141.

IMPORTANT NOTE The WARNING or CRITICAL events used to generate Admin reports are based on Admin Thresholds. 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 established for the benefit of both Administrators and end-users alike, reports based on SLA severities display the same results.

9.5 Managing Action Profiles and Thresholds

9.5.1 Managing User-Class Action Profiles

❑ To create a User-Class Action Profile:

1. Click `MANAGE | user class`.
2. On the Manage User Classes page, find the User Class for which you want to create an Action Profile and click **User Class Actions**.
3. On the Manage User Class Action Profiles page, click **Create User Class Action Profile**.
4. On the Create Action Profile page, enter a unique **Action Profile Name**. Optionally, enter an **Action Profile Description**.
Note that the only notification type available is E-mail. This is sent to the Department mailbox of the end-user who created the test.
5. Configure up to five actions for the action profile. Remember to avoid overlapping logic between the actions. Otherwise, the recipient may receive duplicate notifications for a single test event.
6. Click **Create User Class Action Profile**.
7. To assign a User-Class Action Profile to one or more test types, see Section 9.5.2, “Setting Default Action Profiles and Thresholds for User-Classes” on page 138.

❑ To update a User-Class Action Profile:

1. Click `MANAGE | user class`.
2. On the Manage User Classes page, find the User Class for which you want to update an Action Profile and click **User Class Actions**.
3. On the Manage User Class Action Profiles page, find the Action Profile that you want to update and click **Update**.
4. On the Update User Class Action Profile page, make the desired changes, and then click **Update Action Profile**.

❑ To delete a User-Class Action Profile:

1. Click `MANAGE | user class`.
2. On the Manage User Classes page, find the User Class for which you want to update an Action Profile and click **User Class Actions**.

3. On the Manage User Class Action Profiles page, find the Action Profile that you want to delete and click **Delete**.
4. If you are certain that you want to delete this Action Profile, on the Delete User Class Action Profile page, click **Delete**.

9.5.2 Setting Default Action Profiles and Thresholds for User-Classes

Default thresholds define WARNING and CRITICAL status for end-user tests. Warning thresholds are usually selected to provide early warning of potential problems or to identify trends that approach critical status. Critical thresholds are usually set at levels that warn of impending SLA violations or device failures. Administrators must create default and Admin thresholds for all tests available to each User-Class.

NOTE *In general, default settings are established when a User-Class is created and should not be changed.*

□ To configure default thresholds/Action Profiles for a User-Class:

1. Click `MANAGE | user class`.
2. On the Manage User Classes page, find the User-Class for which you want to set defaults and click **Default Thresholds and Actions**.
3. On the Update User Class Default Thresholds page, set the following for each **Available Test**:

Field	Purpose
Warning Threshold	The test result that causes the test's status to change to WARNING.
Critical Threshold	The test result that causes the test's status to change to CRITICAL.

Field	Purpose
Severity Behavior with Value	<p>Specify the relationship between test value and severity. Options include:</p> <ul style="list-style-type: none"> • <i>Ascends</i>: As the value of the test result rises, severity rises. • <i>Descends</i>: As the value of the test result rises, severity falls. • <i>Auto</i>: 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. • <i>Discrete</i>: You can set fixed integers or ranges of numbers using the syntax: 1,3,5,10-25
User Class Action	<p>The default Action Profile that is applied to tests of this type that are created by end-users from this User Class. These Actions Profiles are for notification of end-users (not Administrators) and always E-mail the recipient specified for the Department of the end-user who creates the test.</p>

4. Click **Update Default Thresholds**.

9.5.3 Managing Administrator Action Profiles

□ To create an Administrator Action Profile:

1. Click `MANAGE | actions`.
2. On the Manage Administrator Action Profiles page, click **Create New Administrator Action Profile**.
3. On the Create Administrator Action Profile page, enter a unique name for the Action Profile. Optionally, enter a description.
4. For each action, choose the type of notification in the **Notify Using** list and the address(es) of one or more recipients. This is usually yourself or someone else who is responsible for monitoring your system's performance. To enter multiple message recipients, separate the addresses with commas (e.g., `jdoe@acme.com, fcheng@acme.com`).

5. Select the check boxes to identify which test states should trigger notifications.
6. If you checked the repeat or wait instructions, select the desired number of test cycles from the drop-down lists of choices.
Remember to avoid overlapping logic between the actions contained in the profile. Otherwise, a recipient may receive duplicate notifications for a single test event.
7. Click **Create Action Profile**.

❑ To update an Administrator Action Profile:

1. Click `MANAGE | actions`.
2. On the Manage Administrator Action Profiles page, find the Action Profile that you want to update and click **Update**.
3. On the Update Administrator Action Profile page, make the desired changes, and then click **Update Action Profile**.

❑ To delete an Administrator Action Profile:

1. Click `MANAGE | actions`.
2. On the Manage Administrator Action Profiles page, find the Action Profile that you want to delete and click **Delete**.
3. If you are certain that you want to delete this Action Profile, on the Delete Administrator Action Profile page, click **Delete**.

9.5.4 Setting Admin Action Profiles and Thresholds

❑ To configure Admin thresholds/Action Profiles for a User-Class:

1. Click `MANAGE | user class`.
2. On the Manage User Classes page, find the User-Class for which you want to set Admin thresholds and Action Profiles and click **Admin Thresholds and Actions**.

3. On the Update User Class Admin Thresholds page, set the following for each available test:

Field	Purpose
Warning Threshold	The test result that causes the test's status to change to WARNING.
Critical Threshold	The test result that causes the test's status to change to CRITICAL.
Admin Action Profile	The default Administrator Action Profile that is applied to tests of this type.

4. Click **Update Admin Thresholds**.

9.5.5 Setting SLA Action Profiles and Thresholds

SLA thresholds are designed for both Administrator and end-user use. Although SLA thresholds are created and modified by Administrators only, every end-user has read-only access to an SLA Report for their Department. By providing this view into the SLA, Administrators give end-users confidence that SLA violations are being tracked at the individual event level.

❑ To configure SLA thresholds/Action Profiles for a User-Class:

1. Click `MANAGE | user class`.
2. On the Manage User Classes page, find the User-Class for which you want to set SLA thresholds and actions and click **SLA Thresholds & Actions**.
3. On the Update User Class SLA Thresholds page, set the following for each available test:

Field	Purpose
SLA Threshold	The test result that causes an SLA event to be generated.
Admin Action Profile	The Administrator Action Profile that is applied to tests of this type. This is for notification of Administrators (not end-users) and always notifies the recipient(s) defined in the Administrator Action Profile.

4. Click **Update SLA Thresholds**.