



Alert Set-Up Using Dotcom-Monitor

Dotcom-Monitor is an active external service that simulates end-user interactions with Internet services such as web applications, mail servers, and video streaming. As Dotcom-Monitor imitates a user's behavior, it simultaneously monitors for problems affecting availability, accessibility, and performance. Alerts are a critical part of the Dotcom-Monitor service and provide real-time notification whenever service-affecting problems are detected.

Dotcom-Monitor offers an extremely flexible framework for problem notification. There are several main concepts that should be understood to maximize the power of this alerting system. These include:

- Notification devices
- Groups
- Templates
- Schedulers
- Filters
- Escalations
- Throttling
- Uptime alerts

Notification Devices

The notification device is the basic building block of Dotcom-Monitor's alerting system. It specifies the alert-delivery mechanism. Dotcom-Monitor supports any combination of the following delivery options:

- E-mail – E-mail alerts contain detailed information about the monitored device¹, the task name, the affected monitoring location(s), the error code and the error description.
- Wireless e-mail (text messaging) – This is a common method of sending alerts to wireless phones and pagers in the U.S. Wireless e-mail messages provide basic error information, such as the device name, monitoring location, error code and a brief error description. Dotcom-Monitor formats wireless e-mails as 180 characters to improve readability on most pagers and phones. Within the U.S. and Canada, the sending address is displayed as a phone number followed by a domain name, such as 6125551212@vtext.net. Outside of these regions, wireless text alerts are available using the SMS option. There is no additional cost for wireless e-mail; however, there is a charge for SMS when this option is used.

¹ A monitored (or monitoring) device is grouping of monitoring tasks.



DOTCOM-MONITOR

- SMS (Short Message Service) – SMS is a delivery option for wireless devices, but unlike wireless e-mail, the service is not based on e-mail. SMS addresses are entered in the same manner as phone numbers (country code + area code + number) and delivered over a mobile telephone network. Dotcom-Monitor assesses a surcharge for each SMS sent.
- Phone – Alerts can be sent to any voice-enabled phone. This option provides a specific message with the details of the problem. Dotcom-Monitor's automated system can detect whether an individual has received the call or if it is forwarded to a voice-mail system and treats the call accordingly. Phone alerts are interactive and provide an option for postponing additional alerts to the number called, which prevents repeated alerts while the issue is being resolved. Dotcom-Monitor assesses a surcharge for each phone alert.
- Pager – For this option, Dotcom-Monitor calls the pager number and enters a numeric code. These codes are preset for specific monitored devices and show which monitored device is experiencing a problem.
- SNMP trap – The Simple Network Management Protocol (SNMP) alert sends an SNMP trap to an SNMP management console or server. This option integrates Dotcom-Monitor alerts directly into an IT management system, so alerts are treated and routed like any other alert within an enterprise. Currently, Dotcom-Monitor supports SNMPv1. Dotcom-Monitor has a registered EnterpriseOID, which is 31201. Alerts are sent as an Enterprise type, which is value six. For custom bit, an Error alert is value one; an Uptime alert is value two; and a Test alert is value three. Alerts are sent over the Internet on a standard SNMP port.

Notification Groups

A notification group is a grouping of notification addresses assigned to a monitored device. For example, a notification group could contain e-mail addresses, SMS addresses and phone numbers as notification addresses. There is no limit on the number of notification addresses assignable to a group, and there is no limit on the number of notification groups per account. Notification groups are visible under the Device>Edit screen. Multiple notification groups can be assigned to one monitoring device, and changes take effect immediately.

Notification Templates

Dotcom-Monitor uses a default format for alert notifications but allows modification for any type of notification device. Users can create custom templates with a set of variables that Dotcom-Monitor provides. Templates can be created for any notification address. Once templates are created, they appear on the Group Notification screen.

Scheduler

The scheduler allows assigning specific activation periods to notification groups, which enables on-call coverage between specific groups of persons or disables alerts during specific time periods. Dotcom-Monitor allows for multiple schedules within the same account. Once a schedule has been created, it can be assigned to a notification group.



As an example, three schedulers could be created as follows:

- Scheduler 1 – 08:00–15:59, Monday – Friday
- Scheduler 2 – 16:00–23:59, Monday – Friday
- Scheduler 3 – 00:00–07:59, Monday – Friday, all-day Saturday and Sunday

In the following example, there are three groups in the account with the following notification types:

- Notification Group A – E-mail, Phone
- Notification Group B – E-mail, SMS, Phone
- Notification Group C – Wireless e-mail, SMS, Phone, SNMP trap

Using these examples, Scheduler 1 could be assigned to Notification Group A, so the individuals whose e-mail and SMS addresses are specified in the notification device will receive e-mail and phone alerts Monday through Friday from 08:00–15:59 only.

If no schedule is assigned to a group, it is assumed that the group is eligible for notifications 24/7.

Filters

Filters are used to define error conditions. By default, any problem that Dotcom-Monitor detects is an error, but notifications can be blocked using filters, as follows:

- Error is reported for less than (X) minutes - This filters problems based on the frequency of an occurrence. For example, a five-minute setting filters out any problems that last for less than five minutes. Additionally, this option might be used for a brief rebooting of a web server when no alert notifications are desired.
- Error if it is not confirmed by (X) monitoring locations – This filters errors based on the number of monitoring stations reporting the error. For example, a single monitoring station might not connect to a specific URL but other stations do connect, which signals that the problem lies with a backbone provider for that single station. Dotcom-Monitor recommends setting this filter value to two or higher to help filter out problems that are occurring on a specific backbone.
- Error detected in more than (X) tasks – This filters alerts based on the number of task errors occurring in a monitored device. For example, a monitoring device might consist of tasks that access three web servers in a server farm. If two of the servers fail, the device will still work as constructed using only the remaining server. By default, Dotcom-Monitor would send a notification because the two servers are unavailable, but the monitoring device is still performing correctly only on a single server. If the filter is set at two, a notification is sent only when two tasks in the device fail.
- Error if owner device is down – This filter allows the specification of a parent device so that the alerting is modified should the parent device experience problems. An owner device is one on which other devices are dependent; it is a primary or parent device on which dependencies are built. For example, 10 different websites may be monitored as 10 different monitoring devices, but all the websites may be dependent on a single router. If the router fails, all 10 websites would become unavailable, and, by default, Dotcom-Monitor would send an alert for each website as an individual monitoring device.



- Errors that meet below conditions will be ignored – This option filters out certain user-configurable errors. For example, DNS errors could be filtered out based on who is responsible for DNS server operations.

Filters are assigned to devices and notification groups.

Escalation

The escalation feature enables selective notification based on the duration of an error. For example, once an error has been detected and is cleared through any filters that may have been created, a specific group can be immediately notified. If the error condition persists for a specified duration, an alert could be sent to a secondary group to escalate the issue. A third group could also be notified if the error condition still exists after a specified amount of time. The escalation feature is located in the Notifications options under Device>Edit screen.

Throttling

Dotcom-Monitor's throttling option is used to limit the number of alerts sent in response to an error condition. Without this feature, the number of alerts from a single outage can become burdensome. For example, assume there are 10 monitoring devices with a monitoring frequency of once per minute, and a global outage occurs. By default, Dotcom-Monitor would send alerts at the rate of 10 per minute for the entire duration of the outage. Throttling is accomplished at the notification device level, and is found in the Advanced options under Device>Edit. Additionally, SMS alerts could be throttled down to once every 60 minutes throughout the duration of an event.

Uptime Alerts

This option generates an alert to all addressees when a problem is resolved, and the service-affecting event is no longer detected.

Setup Order

To setup the following options, we suggest following this order:

1. Setup templates.
2. Setup filters.
3. Setup schedules.
4. Create a notification group.
 - Assign a schedule to the group.
5. Add notification addresses to the group.
 - Assign templates to each address.
6. Create a monitoring device.
 - Assign filters.
 - Assign notification groups.
 - Create an escalation procedure.
 - Setup Uptime alert(s).
 - Configure throttling.