



Configuring Network Availability Monitoring

With Sentry-go Quick & Plus! monitors

© 3Ds (UK) Limited, January, 2014

<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

Any organisation that has a group of PCs, either desktops or servers networked together, will know the importance of ensuring the network is both healthy and allowing access to each resource. Without monitoring, the first sign of trouble is when a user can't access the remote resource they are looking for but with Sentry-go, you can easily automate this process, alerting you both visually or by other means when a remote device goes off-line or is otherwise unavailable.

This guide gives full details of how you can configure network availability monitoring using Sentry-go.

In this guide

System requirements	2
Recommended monitoring settings	2
Monitoring network availability	3
Setting timeout & retry values	5
Configuring network availability monitoring.....	6
Testing the configuration.....	7
Ignoring a device from a default scan	7
Configuring an automatic response	7
Configuring an alert.....	7
Web reporting with this monitoring component.....	8
The network status report	8
More Information	9

System requirements

This component is fully compatible with both Sentry-go Quick Monitors v6 and above, and Sentry-go Plus! v6 monitors and above.

Recommended monitoring settings

It is recommended that all servers are periodically monitored for network access.



To use this monitoring component, you must allow PING network packets to flow between your monitor and the target network device(s).

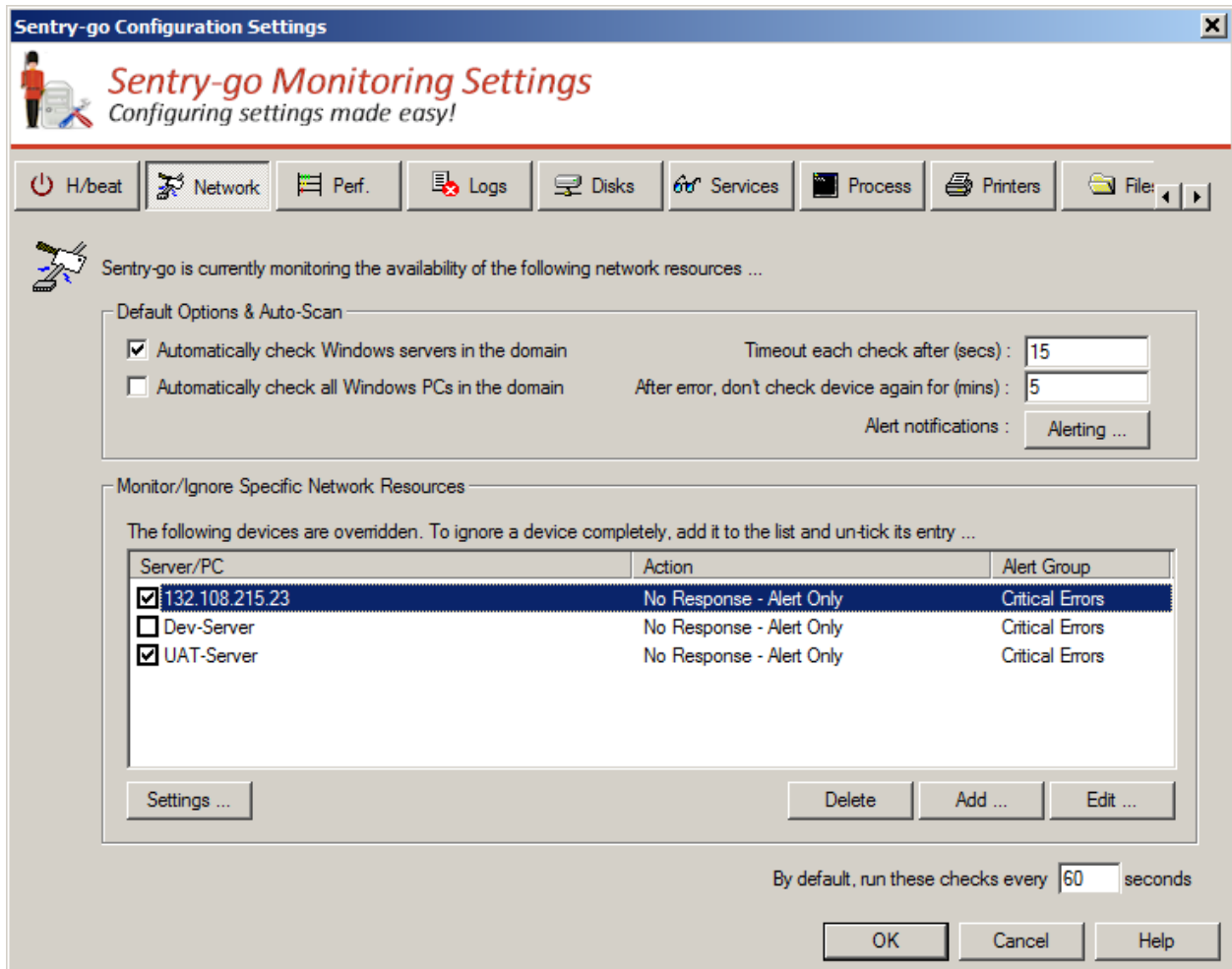
Some organisations implement firewalls to protect network access. If your firewall is configured to prevent PING traffic from accessing the device, this monitoring component will not work.

In this case ...

- Enable PING traffic through the firewall (or consult your network administrator)
- Use an alternate monitoring option – such as the TCP/IP port monitor to verify access via a different (named) port.

Monitoring network availability

To ensure your Sentry-go monitors are responding as expected each one emits heartbeat information. One or more monitors can verify this information to determine if any failures currently exist. To set up monitoring, configure the appropriate monitor and select the “Network” tab.



This window is split into two. The top half shows “auto-scan” options while the lower half lists any overridden or excluded devices. From here you can monitor new devices or edit the settings for those already defined.

Default Options & Auto-Scan

The values here determine how the Sentry-go Network monitoring component will perform its checks and the features it will use.

Automatically check Windows servers in the domain

Tick this option to allow Sentry-go to periodically scan for all "servers" in the domain and automatically monitor connectivity to them. If a new server is added to your network, this feature will ensure it is automatically mapped and monitored without the need to add it to the list.



By default, if you enable this option, all servers will be monitored. If, however, you have specific servers that should be excluded - e.g. development or testing servers that may legitimately be unavailable, simply add them to the list below and "un-tick" them in that list. Un-ticked items in the list are automatically ignored from the scan.

A Windows server is a Windows machine defined as running a server-based Operating System.

Automatically check all Windows PCs in the domain

Tick this option to allow Sentry-go to periodically scan for all Windows PCs in the domain and automatically monitor connectivity to them. If any PC is added to your network, this feature will ensure it is automatically mapped and monitored without the need to add it to the list.



Please use this option with caution.

This option is designed for environments that have a specific requirement, such as a customer-facing (live) domain. On a large domain, ticking this option will cause all PCs to be scanned which will take time and result in large numbers of alerts being produced when PCs are switched off.

Treat errors as

The value selected here indicates the Alert group assigned to the corresponding alert that is raised in the event any automatically monitored device should be unavailable. The Alert Group is used by the monitor to determine which System Administrators should be notified and/or Scripts run in response to the triggered alert.

Timeout each check after

The value here indicates how long an individual check will wait before a lack of response is considered a failure. If the device has not responded to a PING within this timeframe, it is considered to be unavailable.



Typically this will be 10 seconds, but may be altered if you have a slow link or using dial-up to connect to remote servers etc.

After error, don't check device again for (mins)

When a device fails to respond & you trigger an alert, this value allows the device to be ignored from future scans for the specified period of time. This can be used to give the Administrator time to investigate the problem further before being notified again and prevents continuous notifications being sent.

By default, run these checks every (secs)

This value specifies how often, in seconds, the network scan is performed.

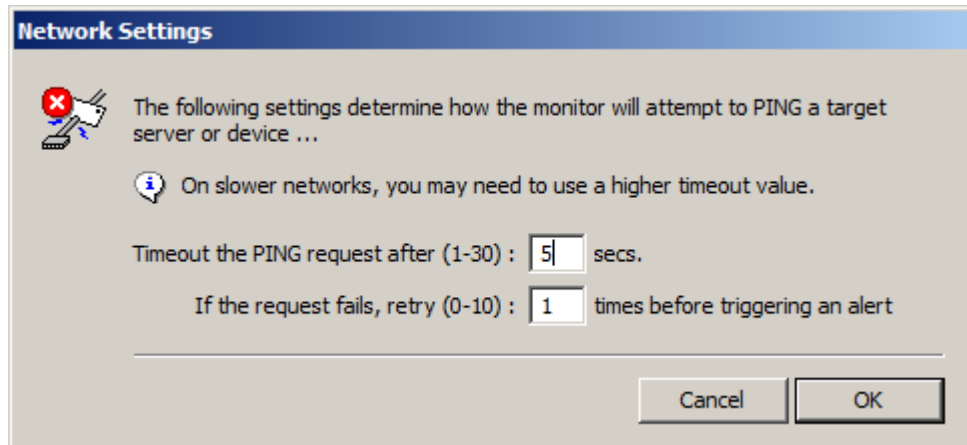
Settings

Click this button to view and configure default timeout & retry values – see below.

Setting timeout & retry values


By default, Sentry-go will timeout an individual access attempt after 5 seconds and retry connectivity once following a failure. However, if you are running on a slower network, or wish to configure these values differently, you can do so by clicking the “Settings” button from the main window.

The following dialog will be shown ...




Timeout the PING request

This value indicates how many seconds the PING command will wait before timing out if no response is received from the remote device or server.

 On some slower networks, the value entered here may need to be higher.

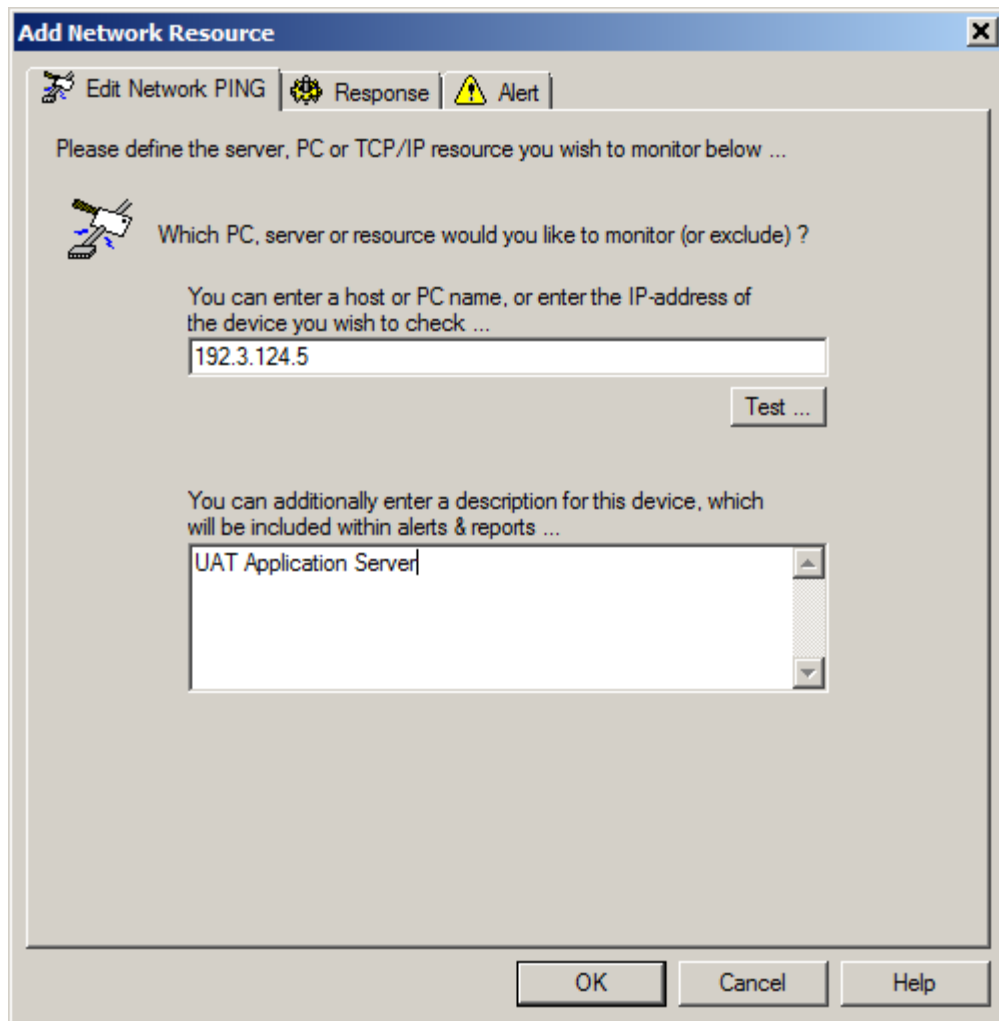
If the request fails, retry

This value indicates how many times the PING is run in succession before an alert is triggered. If the PING fails, the command is immediately retried up to the maximum of times entered here. If after this the remote device still fails to respond, an alert is triggered.

 To guard against false alerts, it is recommended that at least one retry attempt is made when specifying this value.

Configuring network availability monitoring

To monitor a specific server, PC or device with a specific IP-address, select the Add or Edit option from the main window ...



From here you can define the device you wish to check over the network.

Which PC, server or resource would you like to check ...


Enter either the network name (e.g. the name of the server) or the TCP/IP address of the device you wish to verify. This name will be used when Sentry-go attempts to PING the device.

Description ...

Additionally you can optionally enter a description for the resource. This will be included in alert messages and web reports and allows you to put a name to an IP address, for example.

Testing the configuration

Once defined, you can optionally check the configuration by clicking the “Test” button. When selected, the Client Console connects to the target monitoring server (the server being configured) in order to run the test, the results of which are then displayed in the resulting web page.

 In order to check the configuration, the target Sentry-go monitor must be running with web reports enabled.

The parameters, along with the test results are shown on the web page. In some cases, errors may be obvious and easily corrected; in others, additional diagnostic information may be found in the Sentry-go log file, accessible on the server or via the web reports menu.

For more information on the Sentry-go log file, please see the “Configuring Logging Options” guide.


Ignoring a device from a default scan

In some cases, you may wish to automatically scan for devices, such as servers (the auto-scan option) but permanently exclude one or more PCs/servers from the check. To do this, add these PCs/servers to the lower list, and ensure there is no “tick” or check against the entry in the list.

Configuring an automatic response

In the event an error is detected, Sentry-go can be configured to optionally respond automatically - i.e. to take action itself.


To configure this, select entry from the list and click Edit. On the resulting window, select the “Response” tab.

 For more information on the options available as well as details on how to configure automatic responses, please see the “Configuring Automatic Responses” guide.

Configuring an alert

In the event an error is detected and either no automatic response is defined or the response doesn’t resolve the fault, an alert will be triggered. Depending on the monitor’s general settings, you can either notify one or more contacts individually, or specify the alert group you wish to inform.

To configure these options, select the entry from the list and click Edit. On the resulting window, select the “Alert” tab.

 For more information, please see the “Configuring Sentry-go Alerts” guide.

Web reporting with this monitoring component

In addition to the standard web reports, this component provides the following additional reports. These can be accessed directly from the URL, or from the monitor's home page.

The network status report

URL: *http://<Server Name>:<Port>/SgoMntrNetworkStatus.sgp*

This report gives at a glance status of all monitored servers and/or PCs. It also shows the latest IP address of each server and/or the reason for the connectivity failure.

The screenshot displays the Sentry-go Monitoring System v5 Web Reporting interface in a Windows Internet Explorer browser window. The browser title is "WALTON-64 - Sentry-go Monitoring Service - Network Summary - Windows Internet Explorer". The address bar shows the URL: "http://walton-64:1000/SgoMntrNetworkStatus.sgp?btnRefresh=Refresh+Status".

The main content area features the Sentry-go logo (a red soldier figure) and the text "Sentry-go Monitoring System v5 Web Reporting". The copyright information is "© 3Ds (UK) Limited http://www.Sentry-go.com".

The report details include:

- Server: WALTON-64
- Licence: Demonstration (Shareware)
- Generated on: 4th Nov. 2009 at 17:09:52
- System Health: 40% check success (indicated by a red-to-green gradient bar)

Navigation links are provided: Home, Alerts, Status, Activity, and Logout. There are also checkboxes for "Hide Header", "Show Details", and "Refresh automatically".

The "Network Access Summary" section includes a "Refresh Status" button and a table of monitored servers:

125.2.5.12	MyServer	YourServer	WALTON-64
WALTON-CODE	WALTON-PDC		

The footer of the page displays the "Sentry-go" logo. The browser status bar at the bottom shows "Done", "Trusted sites", "Protected Mode: Off", and "100%" zoom.

More Information

If you need more help or information on this topic ...

- Read all [papers/documents on-line](#).
- Watch [demonstrations & walkthrough videos on-line](#).
- Visit <http://www.Sentry-go.com>.
- Contact our [Support Team](#).



*Sentry-go, © 3Ds (UK) Limited, 2000-2013
East Molesey, Surrey. United Kingdom
T. 0208 144 4141
W. <http://www.Sentry-go.com>*