

# The Sentry-go Monitoring System Monitoring Network Availability

Last Updated Wednesday, 03 November 2010

© 3Ds (UK) Limited  
<http://www.Sentry-go.com>

*Be Proactive, Not Reactive!*

---

## Table of Contents

Symbols .....	2
Background.....	2
Recommended Monitoring Settings .....	2
Quick Facts.....	3
Monitoring Network Availability .....	3
Setting Timeout & Retry Values.....	6
Configuring Network Availability Monitoring.....	7
Testing the Configuration.....	8
Temporarily Ignoring a Configured Check.....	8
Configuring an Automatic Response .....	8
Web Reporting with this Monitoring Component .....	9
The Network Status Report .....	9
More Information, Help & Support .....	10

---

## Symbols

Thank you for choosing Sentry-go® as your monitoring solution for Windows. In this guide, the following symbols are used to denote specific items ...



Important information which should be noted – it may affect what you are trying to do.



Additional information relating to the operation being described is shown.

---

## Background

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.

---

## 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.

---

## Quick Facts

Here is a summary of the options available with this component. They are discussed in more detail in the pages that follow ...

Component :	Network Availability Monitor
Aim/Description :	To provide periodic monitoring of key network resources such as servers, desktops or TCP/IP devices ensuring they are accessible across the network from the server running Sentry-go.
Main Monitoring Features :	<ul style="list-style-type: none"><li>• Opt-in/out monitoring of Windows servers</li><li>• Opt-in/out monitoring of Windows PCs</li><li>• Opt-in/out monitoring of TCP/IP devices (using IP address)</li><li>• Auto-scan for both Windows servers &amp; desktops</li></ul>
Periodic Monitoring :	✓
Scheduled Monitoring :	
Local Monitoring :	
Dial-up Support :	
Alerting :	All alerting & auto-response options available
Web Reports :	Status report, "at a glance" Network Status Report
External software req's :	TCP/IP, network link, PING enabled connectivity (firewall)

---

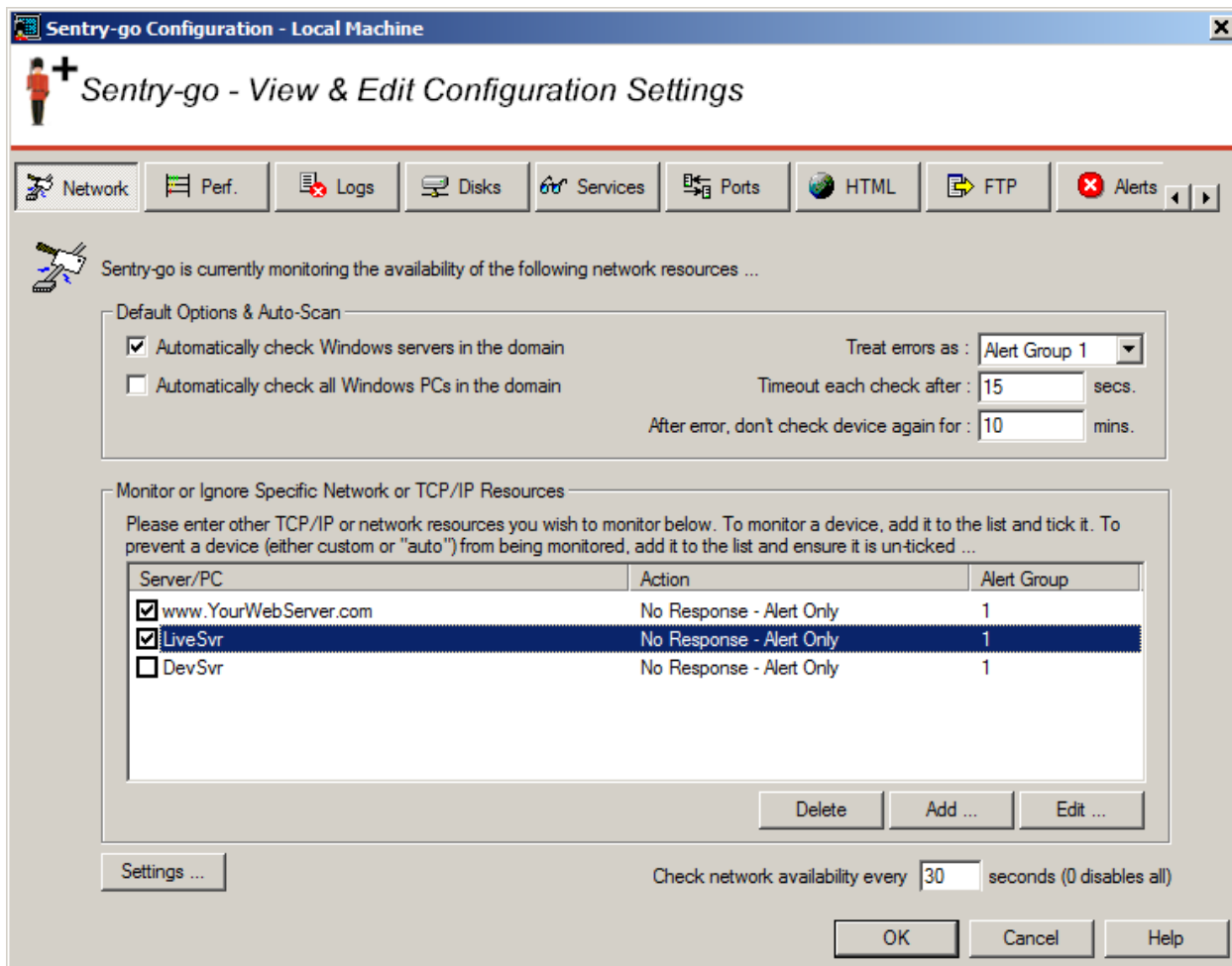
## Monitoring Network Availability

To monitor network availability simply select the Sentry-go monitor from the Client Console with the right mouse button and click "Configure".

A window containing a number of tabs will be displayed. To monitor network availability, select the "Network" tab. From here, you can configure the following ...

- To automatically scan for & monitor Windows servers
- To automatically scan for & monitor other Windows machines (e.g. desktops)
- To monitor a specific device (using its name or IP address)
- To exclude a specific device from the check
- How often network availability monitoring should be performed.
- How long the command should wait before timing out, when attempting to contact the remote resource
- How many retry attempts the monitor should make before triggering an alert
- Temporarily disable the monitoring of one, more or all devices.

The resulting window will have the auto-scan options selected as well as any specifically listed 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.

## Check network availability every (secs)

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

## Settings

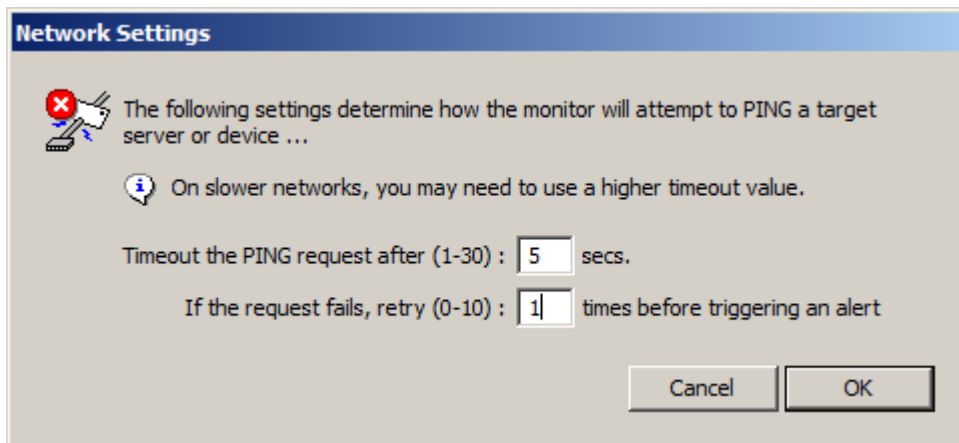
Click this button to view and configure default timeout & retry values – see below.

---

## 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

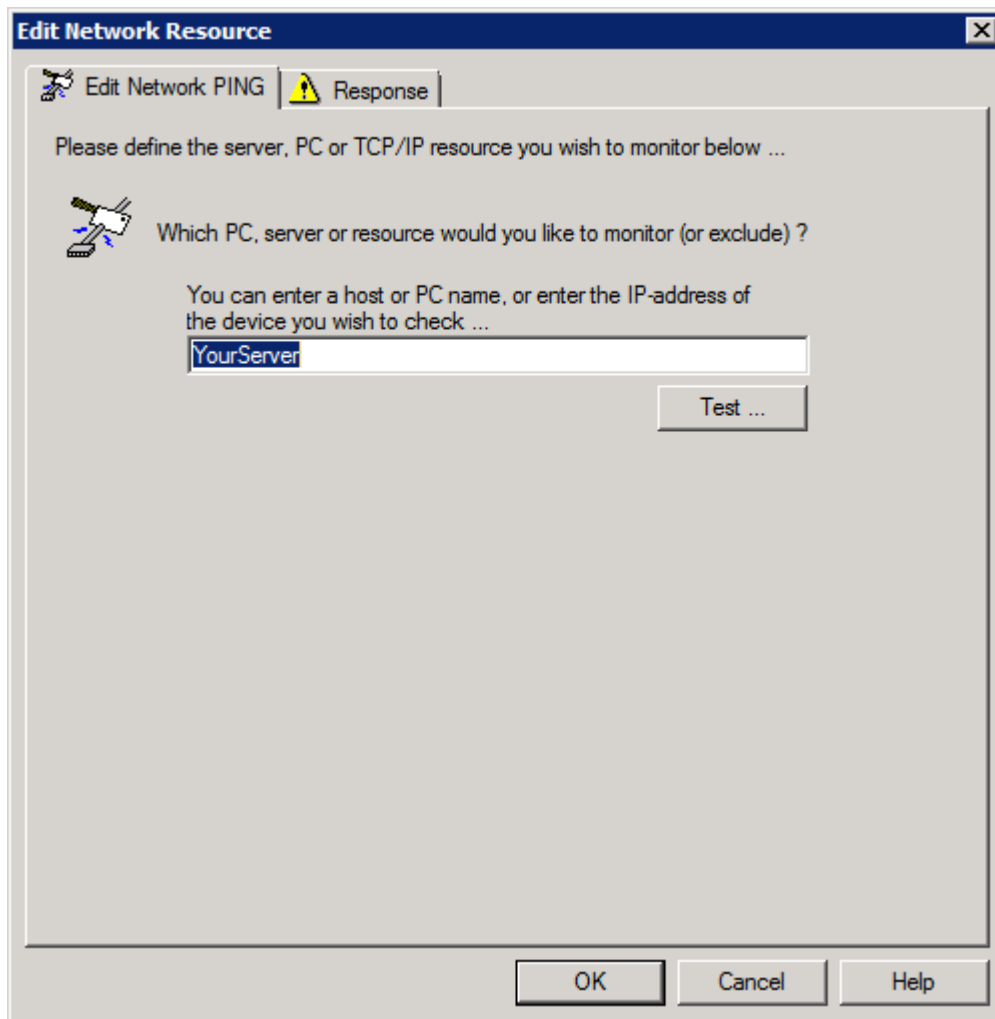
This value indicates how many times the PING is run in succession before an alert is triggered. If the PING fails, the command is immediately retried up to the maximum of times entered here. If after this the remote device still fails to respond, an alert is triggered.

 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 new disk or edit an existing one, 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.

---

## 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 Plus! Log file, see [Sentry-go - Configuring Logging Options](#).

---

## Temporarily Ignoring a Configured Check

In some cases, you may wish to exclude a check from monitoring without removing it permanently. To do this, simply remove the “tick” or check against the entry you wish to ignore in the main list.

---

## Configuring an Automatic Response

In the event an error is detected, an alert will be triggered. In this case, Sentry-go can be configured to either respond automatically (i.e. take action itself), alert one or more Administrators, or both.

To configure what the monitor should do in the event an error is detected, select the 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 alerts & responses, see [Sentry-go - Configuring Alert & Automatic Response Options](#).

## Web Reporting with this Monitoring Component

In addition to the [standard Sentry-go 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

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.

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

The screenshot shows a web browser window titled "WALTON-64 - Sentry-go Monitoring Service - Network Summary - Windows Internet Explorer". The address bar contains the URL `http://walton-64:1000/SgoMntrNetworkStatus.sgp?btnRefresh=Refresh+Status`. The page content includes the Sentry-go logo, the title "Sentry-go Monitoring System v5 Web Reporting", and the text "© 3Ds (UK) Limited http://www.Sentry-go.com". Below this, it displays "Server : WALTON-64", "Licence : Demonstration (Shareware)", and "Generated on : 4th Nov. 2009 at 17:09:52". A "System Health" indicator shows a 40% check success rate with a corresponding progress bar. Navigation links for Home, Alerts, Status, Activity, and Logout are present, along with checkboxes for "Hide Header", "Show Details", and "Refresh automatically". The "Network Access Summary" section features a "Refresh Status" button and a table of server status:

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

The footer of the page displays the "Sentry-go" logo and the text "Done" on the left and "Trusted sites | Protected Mode: Off" and "100%" on the right.

---

## More Information, Help & Support

More information can be found in the guides that accompany the Sentry-go software. You can also access the following resources ...

- For the very latest information & product updates, please visit <http://www.Sentry-go.com>
- For sales advice, please e-mail [Sales@Sentry-go.com](mailto:Sales@Sentry-go.com)
- For technical support, please e-mail [Support@Sentry-go.com](mailto:Support@Sentry-go.com)



**3Ds (UK) Limited**  
*Design, Develop, Deliver Solutions!*

69, Esher Road,  
East Molesey,  
Surrey.  
KT8 0AQ  
<http://www.3Ds.co.uk>