Be Proactive, Not Reactive!

Configuring Windows Process Monitoring

With Sentry-go Quick & Plus! monitors

http://www.Sentry-go.com

Although many Windows are implemented as Windows Services, and therefore monitored as such, there may be times when you may wish to verify that one or more standard applications are either running or not running (e.g. an unauthorised Setup installation). To do this, you can monitor one or more Windows processes, typically the EXEs themselves.

In this guide

System requirements

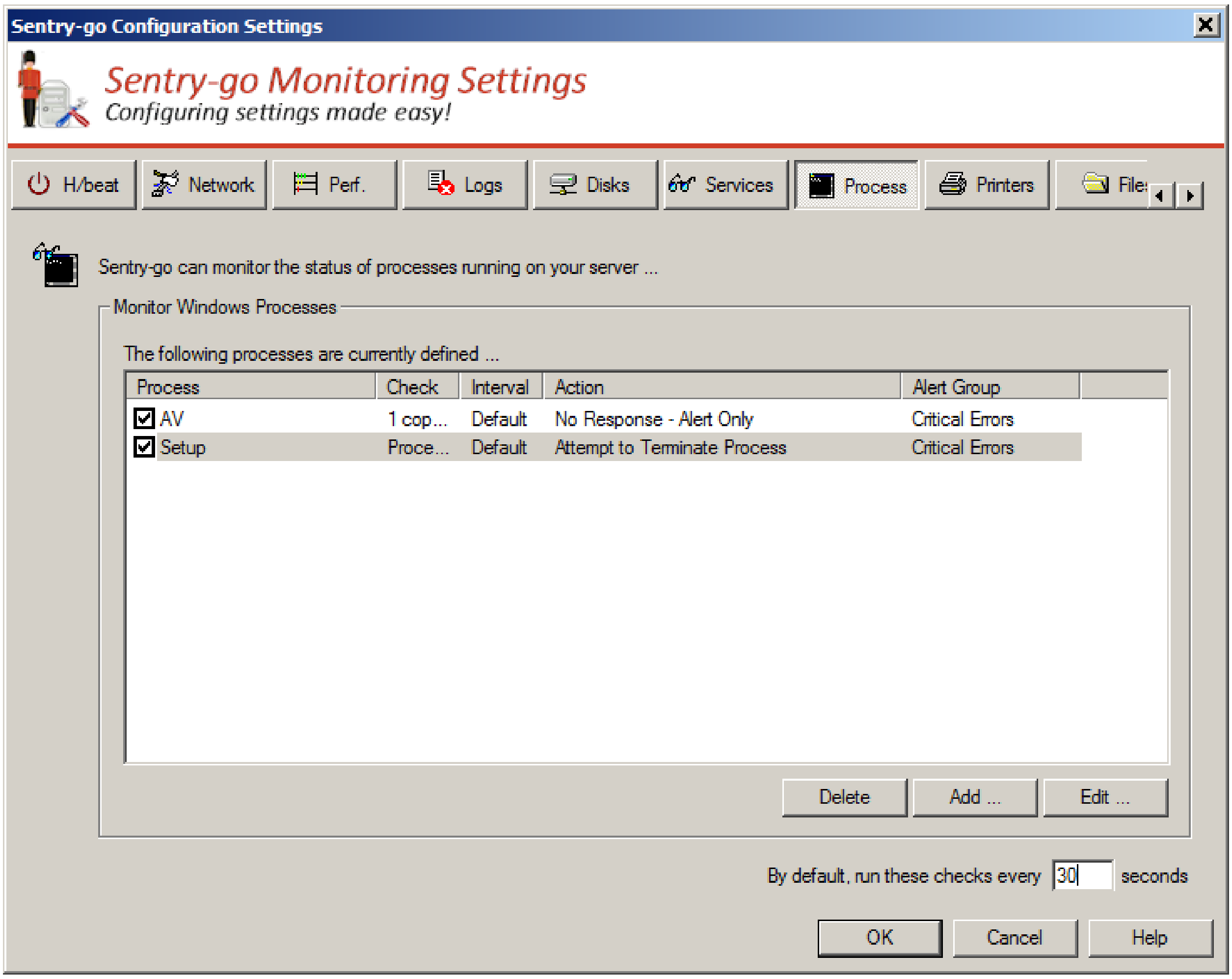
This component is fully compatible with both Sentry-go Quick Monitors v6 and above, and Sentry-go Plus! v6 monitors and above.

Recommended monitoring settings

It is recommended that any critical processes that are not implemented as Windows services are monitored. It is also recommended that processes that are known to potentially cause conflicts – such as unauthorised Setup routines being run are monitored & logged etc.

Monitoring Windows processes

To set up monitoring, configure the appropriate monitor and select the “Process” tab.


Sentry-go Configuration Settings
Sentry-go Monitoring Settings
Configuring settings made easy!
H/beat
Network
Perf.
Logs
Disks
Services
Process
Printers
File:
Monitor Windows Processes
Delete
Add ...
Edit ...
OK
Cancel
Help

Sentry-go can monitor the status of processes running on your server ...

The following processes are currently defined ...

Process	Check	Interval	Action	Alert Group
☑ AV	1 cop...	Default	No Response - Alert Only	Critical Errors
☑ Setup	Proce...	Default	Attempt to Terminate Process	Critical Errors

By default, run these checks every 30 seconds

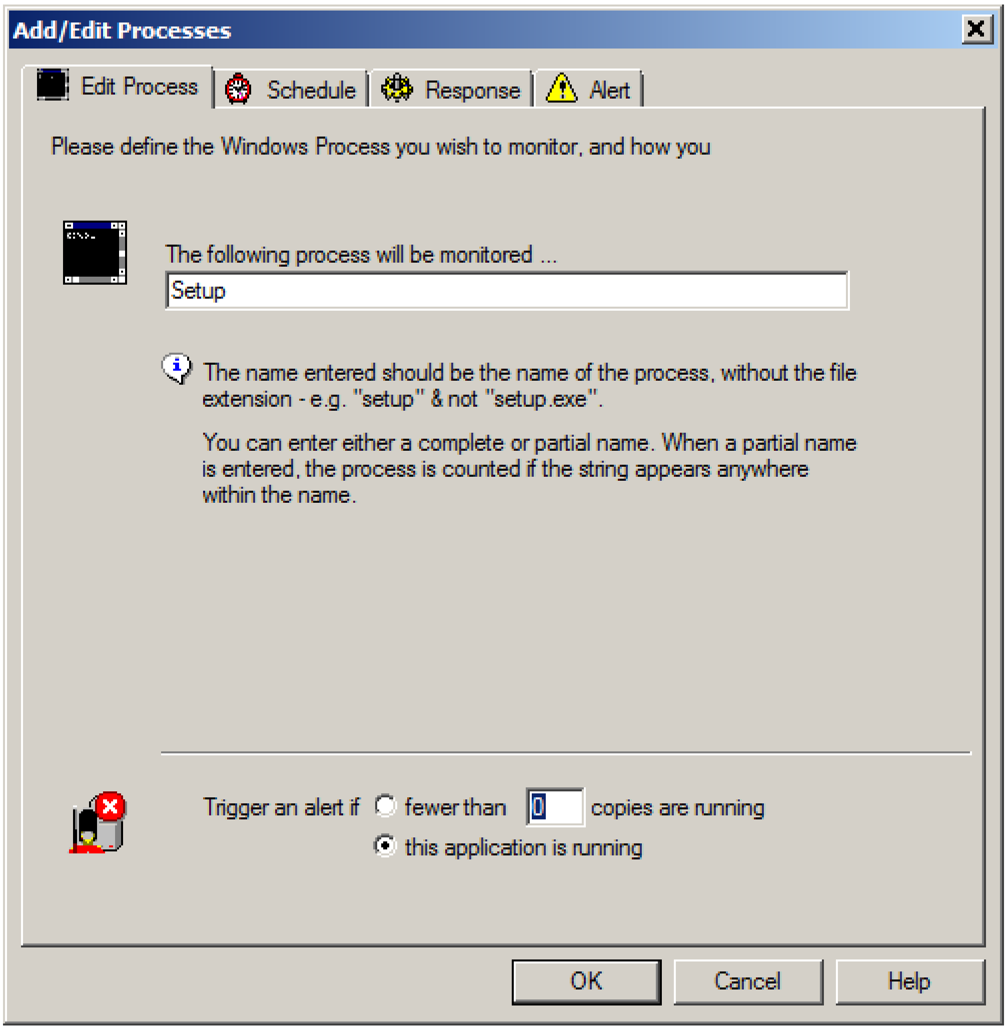
By default, runs these checks ever every (seconds)

This value specifies how often, in minutes, Sentry-go should run the above checks and applies to all processes configured to be monitored.

Shadow events may also be used to monitor processes. See the “Sentry-go Shadow Events” guide for more information.

Configuring process monitoring

To monitor a new process, or edit an existing one, select the Add or Edit option from the main window.



Please define the Windows Process you wish to monitor, and how you

The following process will be monitored ...

Setup

The name entered should be the name of the process, without the file extension - e.g. "setup" & not "setup.exe".

You can enter either a complete or partial name. When a partial name is entered, the process is counted if the string appears anywhere within the name.

Trigger an alert if ○ fewer than 0 copies are running

● this application is running

Please enter the name of the process you wish to monitor

Enter the name, without any file extension that you wish to monitor.

Do not include the file extension with the file name – e.g. specify Setup, not Setup.exe

The process is identified by the name specified. If a partial name is included, the process will be identified as running if any process contains the partial name entered.

Trigger an alert if fewer than X copies are running

Select this option if you want to check that the given number of copies of the above process are running. If no copies, or fewer copies than the number specified are found to be running, an alert will be triggered.

Trigger an alert if the application is running

Select this option if you want to check that the given process is not running. If any copies of the process are found to be running, an alert will be triggered.

Scheduling a check

By default, each check is performed periodically at regular intervals throughout the day. The frequency of these checks is determined by the value specified at the bottom of the main list.

However, there may be times when you wish to perform the check at a different time, maybe at a set time each day, or on certain days etc. To do this, select the “Schedule” tab.

For more information, please see the “Sentry-go Monitoring Schedule” guide.

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, Sentry-go can be configured to optionally respond automatically - i.e. to take action itself. This might be, for example, to terminate an unauthorized application.

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

ℹ 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.

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

Web reporting with this monitoring component

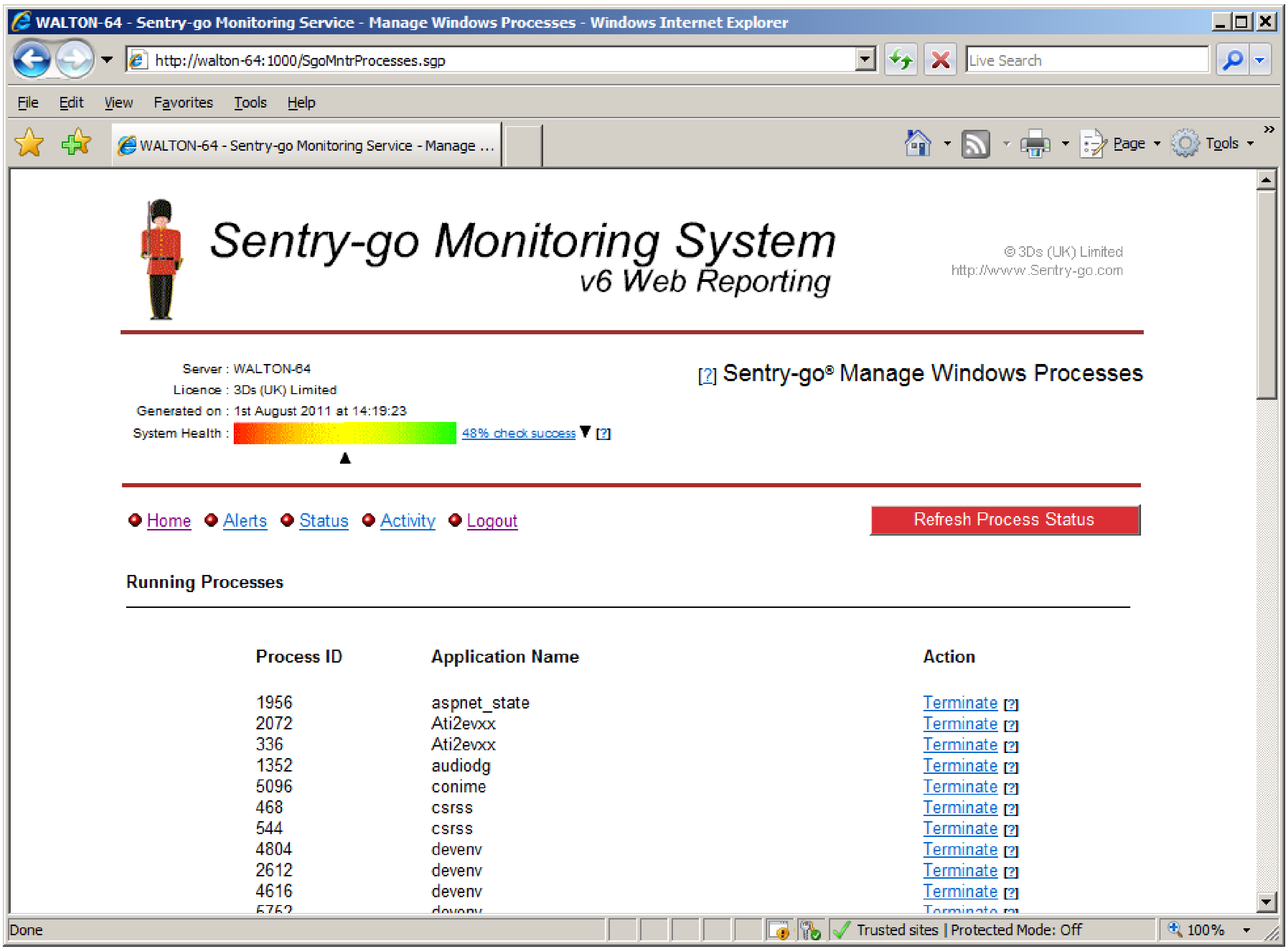
In addition to the standard Sentry-go web reports, this component provides the following additional reports. These can be accessed directly from the URL, or from the monitor’s home page.

The manage Windows processes report

URL: http://<Server Name>:<Port>/SgoMntrProcesses.sgp

This report lists all running processes on the monitored server and optionally allows you to terminate them direct from your web browser.

Care should be taken when terminating processes. No warning will be given to any end user & any unsaved user or system data used by that process will be lost.


WALTON-64 - Sentry-go Monitoring Service - Manage Windows Processes - Windows Internet Explorer
http://walton-64:1000/SgoMntrProcesses.sgp
Live Search
File
Edit
View
Favorites
Tools
Help
WALTON-64 - Sentry-go Monitoring Service - Manage ...
Page
Tools
Sentry-go Monitoring System
v6 Web Reporting
© 3Ds (UK) Limited
http://www.Sentry-go.com
Home
Alerts
Status
Activity
Logout
Refresh Process Status
Done
Trusted sites | Protected Mode: Off
100%

Server : WALTON-64
Licence : 3Ds (UK) Limited
Generated on : 1st August 2011 at 14:19:23
System Health : 48% check success [?]

[?] Sentry-go® Manage Windows Processes

Running Processes

Process ID	Application Name	Action
1956	aspnet_state	Terminate [?]
2072	Ati2evxx	Terminate [?]
336	Ati2evxx	Terminate [?]
1352	audiodg	Terminate [?]
5096	conime	Terminate [?]
468	csrss	Terminate [?]
544	csrss	Terminate [?]
4804	devenv	Terminate [?]
2612	devenv	Terminate [?]
4616	devenv	Terminate [?]
5752	devenv	Terminate [?]

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.

East Molesey, Surrey. United Kingdom
T. 0208 144 4141
W. http://www.Sentry-go.com