

The Sentry-go Monitoring System

Monitoring Windows Processes

Last Updated Wednesday, 04 November 2009

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

Be Proactive, Not Reactive!

Table of Contents

- Symbols2
- Background.....2
- Recommended Monitoring Settings2
- Quick Facts.....3
- Monitoring Windows Processes3
- Configuring Process Monitoring.....5
- Temporarily Ignoring a Configured Check.....7
- Configuring an Automatic Response7
- Web Reporting with this Monitoring Component8
- The Manage Windows Processes Report.....8
- More Information, Help & Support.....9

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

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.

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.

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 :	Windows Process Monitor
Aim/Description :	To monitor the running of processes on the local server.
Main Monitoring Features :	<ul style="list-style-type: none">• Verify key processes are running & restart them if not.• Verify unauthorised processes are not running and report and/or terminate them if they are.
Periodic Monitoring :	✓
Scheduled Monitoring :	✓
Local Monitoring :	✓
Dial-up Support :	
Alerting :	All alerting & auto-response options available
Web Reports :	Status report
External software req's :	None

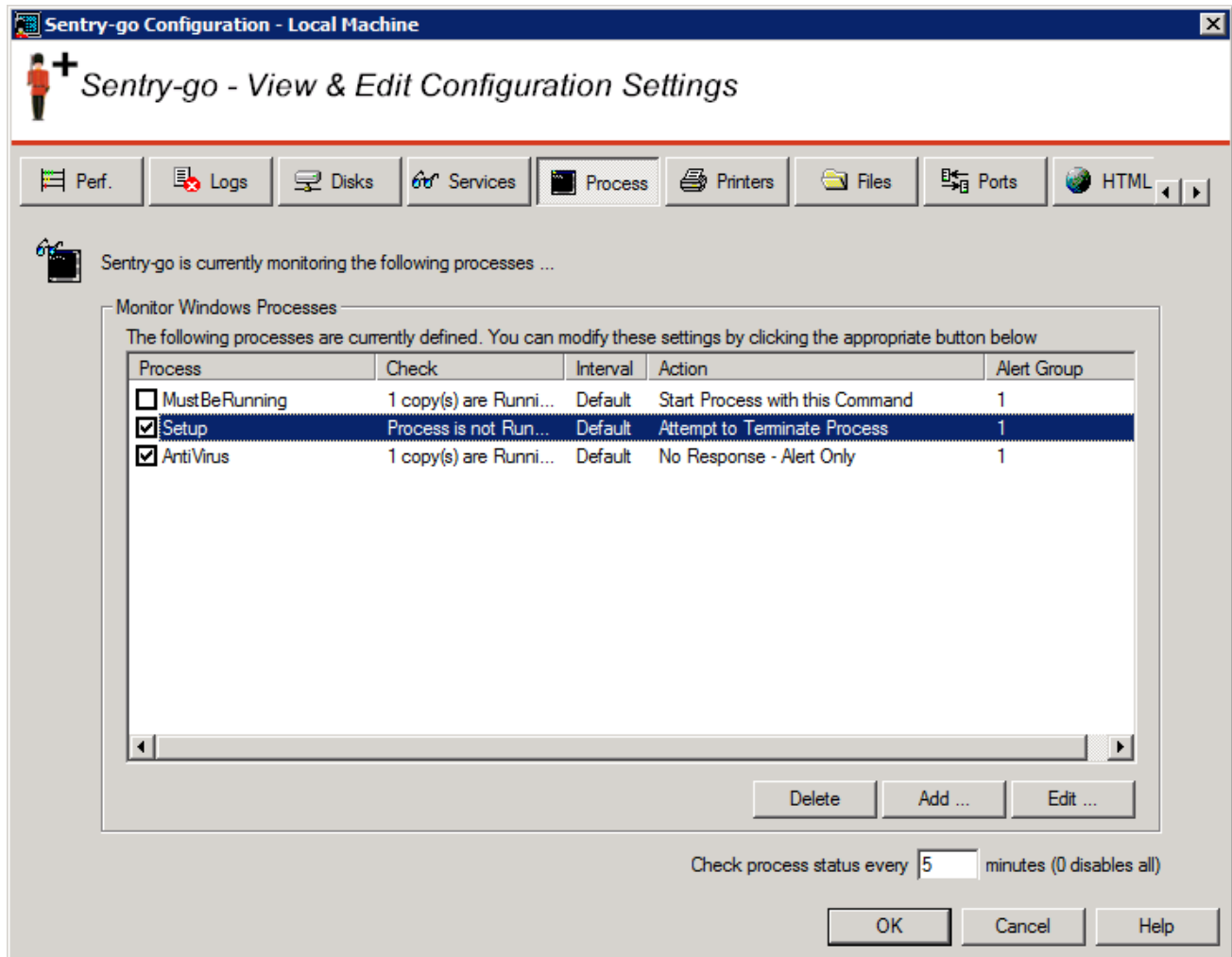
Monitoring Windows Processes

To monitor Windows Processes 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. Select the "Processes" tab. From here, you can configure the following ...

- Ensure that X no. copies of one or more processes are running
- Ensure copies of a particular process are not running.
- Temporarily disable the checking of one or more defined processes.

The resulting list will show any processes that are specifically being monitored or ignored. From here you can add, edit or delete a defined item in the list.

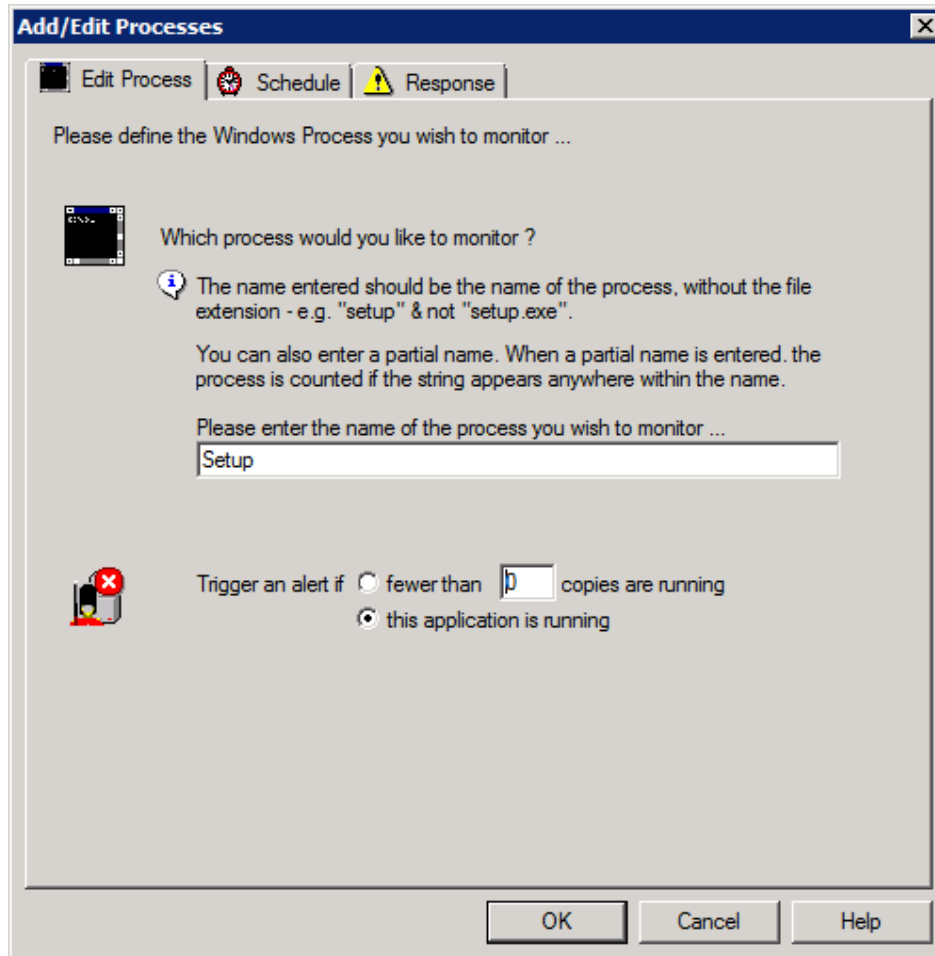


Check process status every (mins)

This value specifies how often, in minutes, Sentry-go should run the above checks and applies to all processes configured to be monitored. It is recommended that this value be set to no less than 5 minutes.

Configuring Process Monitoring

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



Please enter the name of the process you wish to monitor

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

- ⚠ Do no 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

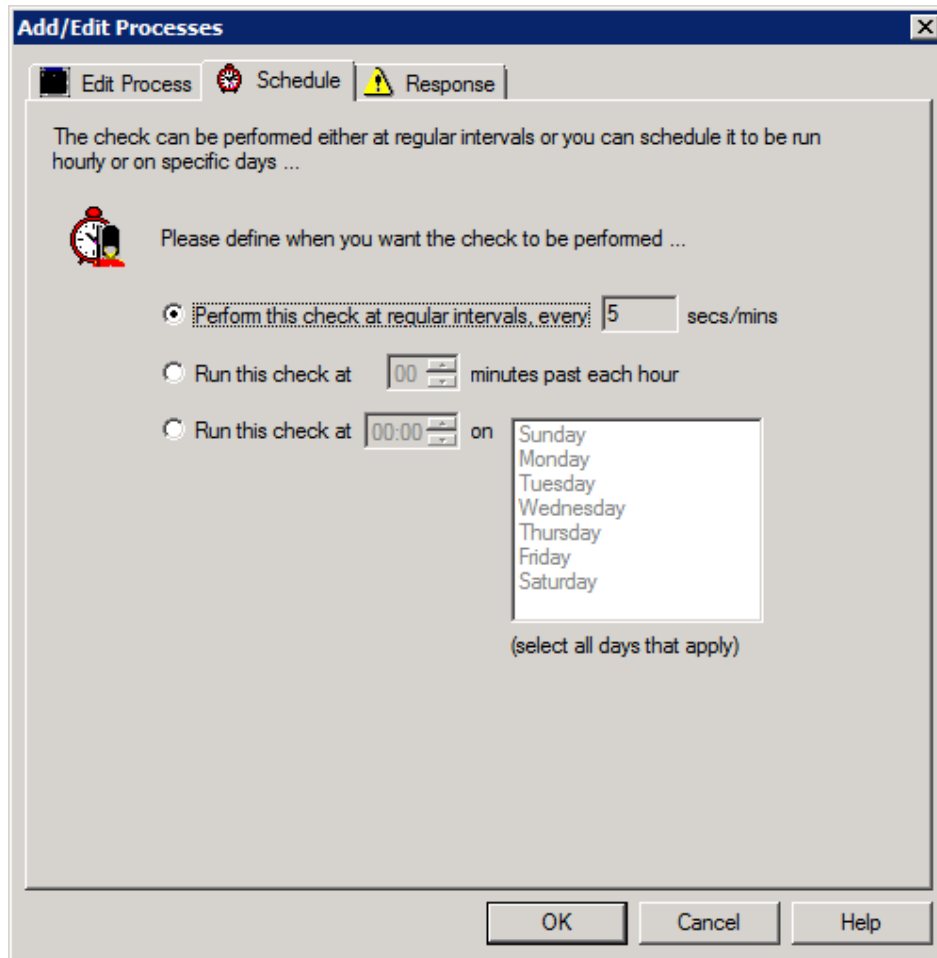
Select this option if you want to check that the given number of copies of the above process are running. If no copies, or fewer copies than the number specified are found to be running, an alert will be triggered.

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.

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.



From here you can define exactly when the check is to be performed.

Perform this check at regular intervals, every (mins)

Select this option to use the default interval specified at the bottom of the on the main list window. In this case the check will be performed every X minutes.

Run this check at HH:MM and every hour thereafter

Select this option to run the check at the specified time past each hour. In this case, only the minutes (MM) are used to determine when the check is to be performed.

Run this check at HH:MM On [Days]

Select this option to run the check at the specified time on the given days. In this case, the check will be performed at the given time if the associated day has been selected. Select all days that apply.

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 Manage Windows Processes Report

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.

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

The screenshot displays the Sentry-go Monitoring System v5 Web Reporting interface. The browser window title is "WALTON-64 - Sentry-go Monitoring Service - Manage Windows Processes - Windows Internet Explorer". The address bar shows the URL "http://walton-64:1000/SgoMntrProcesses.sgp". The page header includes the Sentry-go logo, the text "Sentry-go Monitoring System v5 Web Reporting", and the copyright information "© 3Ds (UK) Limited http://www.Sentry-go.com". The main content area shows the server name "WALTON-64", the license "Licence : Demonstration (Shareware)", and the generation time "Generated on : 4th Nov. 2009 at 18:00:19". A system health indicator shows a green bar with "31% check success" and a dropdown arrow. Below this is a navigation menu with links for Home, Alerts, Status, Activity, and Logout, and a red "Refresh Process Status" button. The "Running Processes" section contains a table with the following data:

Process ID	Application Name	Action
0	Idle	Terminate [?]
4	System	Terminate [?]
432	smss	Terminate [?]
500	csrss	Terminate [?]
564	wininit	Terminate [?]
576	csrss	Terminate [?]
608	services	Terminate [?]
620	lsass	Terminate [?]
628	lsm	Terminate [?]
680	winlogon	Terminate [?]
824	svchost	Terminate [?]
884	svchost	Terminate [?]
924	svchost	Terminate [?]

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
- For technical support, please e-mail Support@Sentry-go.com



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

69, Esher Road,
East Molesey,
Surrey.
KT8 0AQ

<http://www.3Ds.co.uk>