



Using Sentry-go Shadow Events

Last Updated Thursday, 19 April 2012

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


Be Proactive, Not Reactive!

Introduction

For the majority of monitoring tasks, Sentry-go works based on both the monitoring components installed & the time scheduled for the configured checks to run. Depending on the check, this time might be a regular interval of just a few seconds or minutes, a given time past each hour, or a set time on specific days.

In most cases this will be sufficient. However, in some circumstances, it might be less suitable. For example, if a forbidden application is run, you really want to take action, or be informed immediately, not after 5 minutes when the next scan is run. Likewise, because an application could run for only a short period of time, you may miss the alert altogether, as, when the process list is verified, it is no longer running.

For this and similar reasons, Sentry-go has the option of additionally using “Shadow Events”. This logic works on top of standard monitoring components and allows the monitor to utilise notifications in addition to standard scan-based checks. Put simply, for specific tasks the monitor “shadows” the O/S, allowing it to respond immediately to a particular event.

 Shadow Events work in conjunction with routine monitoring & combine their results with the checks configured. Once enabled, you do not need to configure them separately.

If Shadow Events are disabled, standard periodic monitoring will remain unaffected.

Using Shadow Events

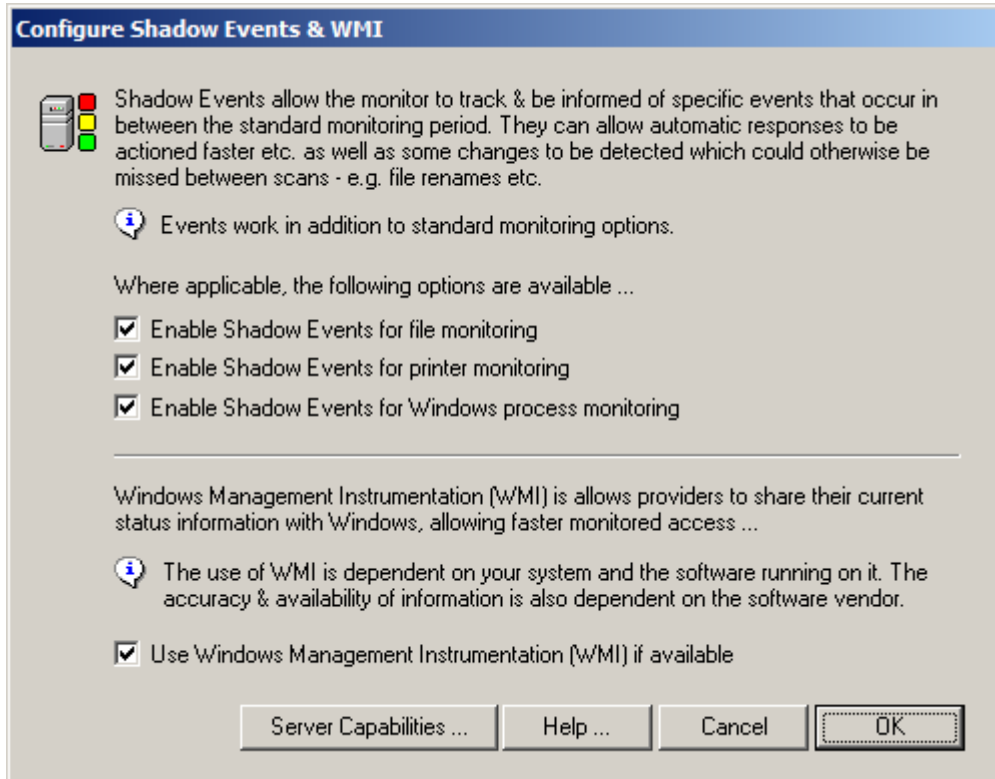
Shadow Events are available for the following monitoring components ...

<i>Monitoring Component ...</i>	<i>Configuration ...</i>
<i>File monitoring</i>	<p>Using Shadow Events enables the file monitoring component to trap the renaming of files & other file deletions that might otherwise not be detected during a standard interval-based monitoring. For example, the deletion & re-creation of a file within the scan period.</p> <p>Shadow Events are available for all checks that monitor locally named files & directories. They are not used on remote files and files containing place-markers such as dates.</p>
<i>Process monitoring</i>	<p>Shadow Events allow the process monitoring component to detect the starting & stopping of processes at the time the action occurs. When triggered, the monitor automatically runs a scan (in between the standard monitoring time) in order to determine if any alerts or actions should be run. If there are, these will be run immediately rather than waiting for the next scan interval.</p> <p>For example, if your anti-virus application stops or fails, it can be restarted straightaway. Alternatively, if someone attempts to run Setup and you wish to prevent it from running, action can be taken to terminate it.</p>
<i>Printer monitoring</i>	<p>Shadow Events allow the printer monitoring component to detect changes to jobs in the print queue.</p> <p>In particular it is used to detect jobs that exceed their permitted size (in either size or no. pages) and can therefore be used to notify you (or take action such as pause or delete the job) as soon as the issue is detected rather than waiting for the next scan interval.</p>

Configuring Shadow Events

Shadow Events are available as part of the appropriate monitoring component. If enabled, they work transparently to both the end user and System Administrator.

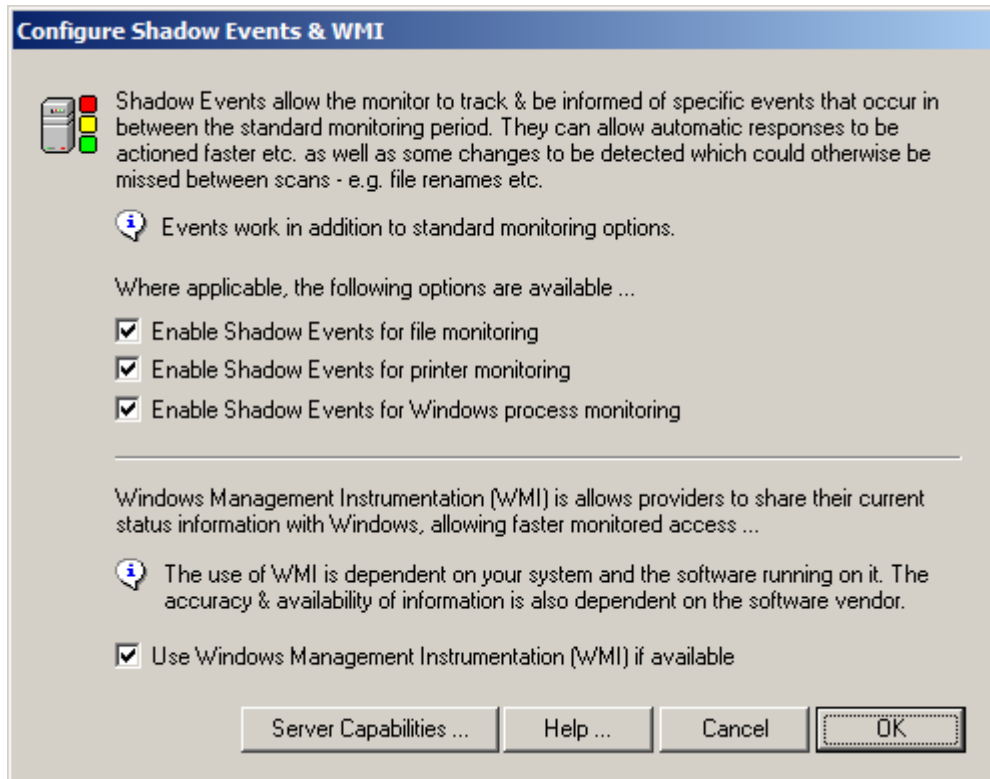
You can enable & disable them from the Client Console or Easy Access Utility by configuring the appropriate monitor & selecting the “Settings” tab. From there, click the “Events” button to display configuration options.



Using WMI

WMI, or Windows Management Instrumentation is a technology made available by Windows. Puts simply, it allows the O/S, as well as other providers to publish statistical information that other tools, such as Sentry-go can use.

For specific monitoring tasks – e.g. process events & printer monitoring, Sentry-go will use WMI if it is enabled (above) and available on the server. However, if WMI is not installed, or for whatever reason it is disabled, standard monitoring will continue to function without issue.



Reasons for Disabling WMI

WMI is a technology that enables Microsoft, as well as 3rd party applications to record & publish data. The actual data available is therefore dependent on (i) the software installed on your server and (ii) the vendor of that software. This software is also used to provide the information – a problem in one of these products may render WMI inactive or in the worst case, cause it to fail altogether.

In extreme situations, WMI is designed to restart automatically. Sentry-go will attempt to detect such conditions and re-request WMI access as required. However, if you do notice or suffer from continual WMI-related issues on your server (e.g. as shown in Event log errors), you can control its use by Sentry-go using the option here.

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

