

The Sentry-go Monitoring System Monitoring HTML Site & Content Availability

Last Updated Wednesday, 06 October 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 HTML Page & Content Availability | 3 |
| Configuring HTML Page & Content Monitoring | 5 |
| Testing URL Connectivity | 8 |
| Temporarily Ignoring a Configured Check..... | 9 |
| Configuring an Automatic Response | 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

Ensuring your web site & key pages are available to users and customers in a timely fashion is extremely important. Likewise, ensuring the pages delivered are correct is also of key importance. Checking these pages manually is a time consuming exercise, yet without performing them, the first report of any problems is usually in an e-mail from a user who can't get your site to work. If no report is made and the problem continues undetected, who knows how many users will be inconvenienced or potential customers go elsewhere ?

Sentry-go allows you to check one or more web pages either locally or remotely. In effect, the monitor runs as a background web browser, periodically checking the pages you define. When a check is made you can ...

- Check that the page is accessible, optionally within a given time.
- Check that the page returned contains the given text
- Check that the page returned doesn't contain specific text (e.g. error text)
- Check that the page returned hasn't been updated (based on the date returned by the server)
- Check that the page returned hasn't been changed updated (based on the page's content)

In addition, timings for each page retrieval can also be logged for later analysis.

Recommended Monitoring Settings

It is recommended that your web sites are monitored for availability (especially external, customer-facing sites) as well as verifying content delivery in a timely manner. For important sites, checking the actual content of the delivered page is also recommended to ensure errors are not being delivered to the browser.

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 : | HTML Page & Content Availability Monitor |
| Aim/Description : | To provide periodic monitoring of HTML pages, web sites etc., ensuring pages are delivered to the client in a timely manner & as expected web sites local hard drives, ensuring sufficient free disk space is available to support the environment. To mimic a user HTTP access function, using GET or POST requests. |
| Main Monitoring Features : | <ul style="list-style-type: none">• Verify the web page (HTML, ASP, ASPX etc.) page can be accessed• Verify the web page is returned in a timely manner• Verify the web page contains the expected text• Verify the web page does not contain a specified string• Verify that the last modified date hasn't changed• Verify that the HTML page's contents haven't changed |
| Periodic Monitoring : | ✓ |
| Scheduled Monitoring : | ✓ |
| Local Monitoring : | ✓ |
| Dial-up Support : | ✓ |
| Alerting : | All alerting & auto-response options available |
| Web Reports : | Status report |
| External software req's : | Microsoft Internet Explorer |

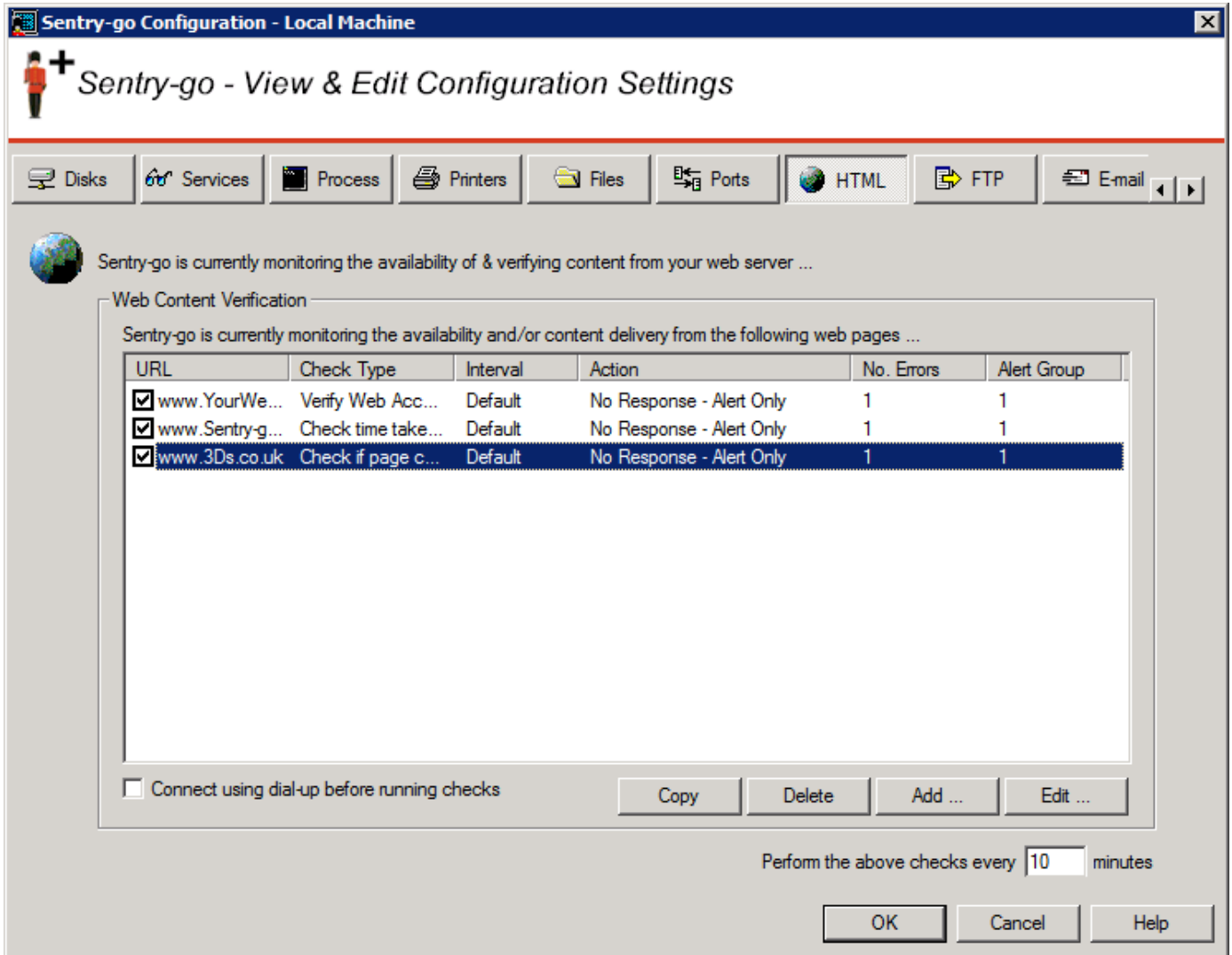
Monitoring HTML Page & Content Availability

To monitor HTML Page & Content 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 available disk space, select the "HTML" tab. From here, you can configure the following ...

- The monitoring of one or more web sites/page.
- What should happen in the check fails.
- How often each check should be run.
- Temporarily disable the monitoring of one, more or all sites/pages.

The resulting list will show the currently defined web sites/pages you are monitoring. From here you can monitor new sites or edit the settings for those already defined.



Connect using dial-up before running checks

Tick this option if your server isn't permanently connected to the network & you want Sentry-go to use dial-up to connect prior to running HTML checks.

For more information, please see [“Sentry-go - Configuring Dialup Networking”](#).

Web sites & access should be checked every (mins)

This value specifies how often, in minutes, Sentry-go should check that the defined web sites & URLs can be accessed and are delivering the appropriate page(s)/data etc. This value can be overridden for individual pages by scheduling those checks to run at specific times. To do this, select the “Schedule” tab from the Add/Edit window.

Configuring HTML Page & Content Monitoring

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

Add/Edit Monitored HTTP Page

Add or Edit a Web Page | Schedule | Response

Please enter the URL you wish to check availability & optionally content ...

In order to use this monitoring component, Microsoft Internet Explorer must be installed on the machine running Sentry-go

Which Web page would you like to check ?

Verify this page/URL :

Connect to this Port : Access using a :

Pass these parameters :

An alert will be triggered if the following condition is met ...

- The page cannot be accessed
- The page does not contain the text below
- The page contains the text below
- The page's last modified date changes
- The page's contents have changed
- Time taken to retrieve page (& assoc. files) exceeds secs.

Verify page contents against this keyword or phrase ...

OK Cancel Help

From here you can define which web site & URL you wish to check and how it should be verified.

Verify this Page (http:// or https://)

Select the type of access you wish to use for the page ...

- Select http:// for normal web site access over a non-secure connection. For most pages & sites, HTTP should be used.
- Select https:// for a connection using secure sockets. Only sites that have been configured to use a secure connection will work with this option.

Verify this Page (URL)

This is the full path (URL) of the page you wish to access and optionally verify. It should be entered in the format <Server>/<Page> - e.g. www.Sentry-go.com or www.Sentry-go.com/index.htm.

- ⚠ Be careful when specifying a page that contains frames. The frames page itself will be verified (e.g. for contents etc.) as opposed to the individual pages it contains. To check an individual page, specify its direct URL in this field instead of the frames page.

Do not include the http:// or https:// prefix in this field. The previous selection will tell Sentry-go how the page should be accessed.



Parameters can be specified for both GET and POST requests.

- For GET requests, parameters can be specified, as they would be from your web browser, as part of the URL itself – in the format ...

<Server>/<Page>?<Param1>=<Value>&<Param2>=<Value>

For example, www.MySite.com?txtName=Sentry&txtType=1

Do not encode the parameters. This will be done automatically at run time.

- For POST requests, parameters are passed using the parameters field below. See below for more information.

Connect to this Port

All web servers listen on a given port for inbound requests from client browsers. The default ports for a web server are port 80 for HTTP requests and 443 for secure connections. However, if your web server uses a different port, maybe for an intranet connection or where two or more web servers run from the same machine, this can be overridden here.



If in doubt, leave the defaults - i.e. 80 for HTTP and 443 for HTTPS pages.

Testing URL access

Once defined, click the “<->” button to verify that the server/URL specified can be accessed by the monitor, given the options entered. See below for more details.

Pass these parameters

If the request type is a POST and you wish to pass additional parameter information to the target page, you can enter them here.




When entering parameters, use the following format ...

<Param1>=<Value>&<Param2>=<Value> etc.

Do not enter the “?” and do not encode the parameters. They will be encoded automatically at run time.

Trigger an alert if the page cannot be accessed

Select this option if you simply wish to ensure that the web server & the web page is available & being delivered by the web server.


-  Redirected pages are handled automatically by the monitor. If your page one or more redirects, Sentry-go will attempt to resolve these before determining whether access is available or not.

Some sites or ISPs display a more friendly message if access to a site is unavailable. If a failed access results in such a web page being displayed, the “access “ check will succeed and not trigger an alert, even though the target page was unavailable.

If your server connects using such a method, we recommend verifying the contents of the page (below) to ensure known text is being presented. Using this method, you can verify that the actual page being displayed is the one you expect to see.

Trigger an alert if the page does not contain the text below


Select this option if you wish to check that the returned page contains some known text. Enter the appropriate text in the field below. If this text is not found in the returned page, an alert will be triggered.

-  In order to trigger an alert correctly, the text entered must not appear in any error page generated by your web site. A unique text string, rather than a single word is recommended for this text.

If the text contains HTML tags (e.g. for formatting etc.), you must take these into account when entering the text here. The check succeeds or fails based on an exact text-based match, though the check is not case sensitive.

Trigger an alert if the page contains the text below


Select this option if you wish to check for an error (or error text) being returned. Enter the appropriate text in the field below. If this text is found in the returned page, an alert will be triggered.


-  In order to trigger an alert correctly, the text entered must not normally appear in the page that should be shown by the URL. A unique text (error) string, rather than a single word is recommended for this text.

If the text contains HTML tags (e.g. for formatting etc.), you must take these into account when entering the text here. The check succeeds or fails based on an exact text-based match, though the check is not case sensitive.

Trigger an alert if the page's last modified date changes


Select this option if you wish to be informed when the page's last modified date changes from one check to another. This can be useful if you want to ensure no unauthorised changes are being made.

-  Some pages (such as dynamic pages) do not generate a last modified date. In this case, you must verify the page using an alternate method.

-  To check the information available for a given page, enter the URL and click the “<->” button to test HTTP or HTTPS access. If successful, the resulting page’s headers are shown, allowing you to see which fields are returned (e.g. the “Last-Modified” header etc.)


Trigger an alert if the page's contents have changed

Select this option if you wish to be informed when the page's contents change from one check to another. As with the above check, this can be useful if you want to ensure no unauthorised changes are being made (but with this check, no reliance on the last modified date).

 Do not select this check for dynamic pages that change content each time the page is retrieved.

Trigger an alert if the time taken to retrieve the page


Select this option to ensure that the page (and any tagged graphics) is returned within the number of seconds specified. If the time taken exceeds this value, or any of the associated tags cannot be accessed, an alert will be triggered.

 This check scans the page and attempts to load tags. Other types of tag, such as files or hyperlinks (<A>) are not verified. To verify the accessibility of other links etc., you should define them as separate monitoring checks.

If the target link (the SRC directive from the tag) is unavailable or cannot be accessed, an alert is also triggered.

Testing URL Connectivity

Before saving your settings, you can optionally check connectivity to the defined web server & the target URL by clicking the “<->” 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 monitoring check itself is not run, only connectivity to the web server & access to the defined URL (using the method specified) is verified at this stage.

The parameters, along with the test results are shown on the web page.

- If successful, the web page's HTTP headers & raw contents are displayed. You can use these to help determine the information available from the site and the types of verification you might wish to perform.
- If an error occurs, details will be displayed. In some cases, these errors may be obvious and easily corrected – e.g. a misspelled URL; 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, 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](#).

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>