



Configuring General Settings for Sentry-go Quick & Plus! Monitors

© 3Ds (UK) Limited, October, 2013
<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

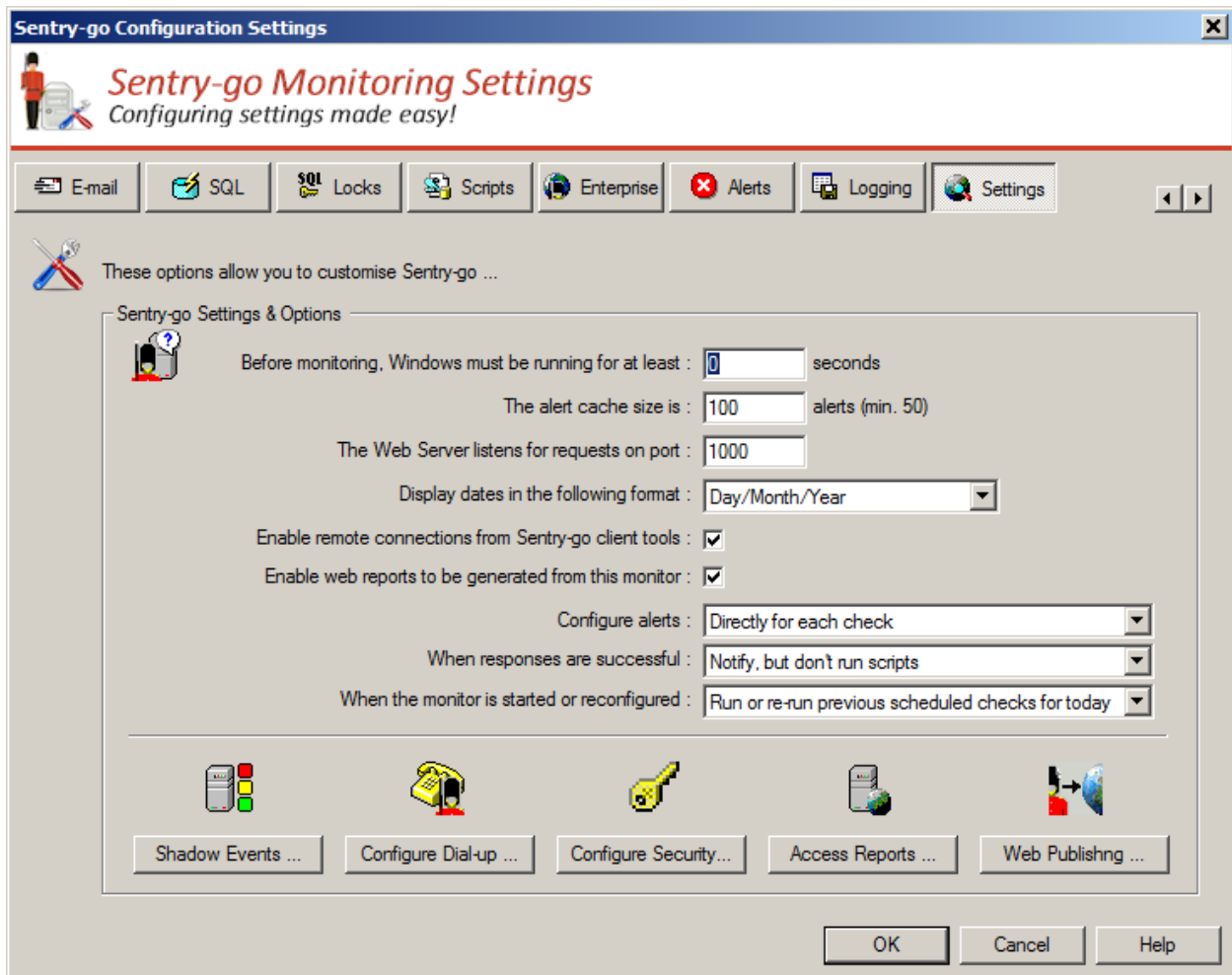
This guide describes the general settings available for the Sentry-go Quick & Sentry-go Plus! monitors.

In this guide

Configuring general settings	2
Configuring shadow events.....	6
Configuring dial-up networking	7
Configuring security settings	8
Security settings.....	9
Restricting client tool access.....	11
Configuring web publishing.....	13
More Information	14

Configuring general settings

To configure Sentry-go's general settings, select the "Settings" option from the configuration utility's button bar ...



Each option is described below.


Before monitoring, Windows must be running for ...

The Sentry-go monitor itself runs as a Windows service which is typically started automatically with other services when Windows starts up. When the server is started, however, some services and resources can take differing times to start and may also be launched in different sequences. This, in turn, can cause false alerts to be triggered by monitoring software which detects failures in services that have yet to start.

To guard against this problem, you can set this value, which is the time that must pass before monitoring commences - i.e. to allow other services to start. The value entered here is the number of seconds after Windows start-up that must elapse before monitoring commences.



The alert cache size is

This value specifies how many alerts will be saved at any one time on the local machine. The more alerts cached, the more will be shown on the Recent Alerts report. The most recent alerts are saved.

-  A minimum of 50 alerts can be saved as this cache also feeds the Recent Alerts web report. The higher this value, the more disk space will be required on the disk containing the Sentry-go directory.

The Web Server listens for requests on port


This read-only/read-write value shows the port on which the local embedded web server is listening for requests. The value shown is the value that should be used when connecting to the web server directly from the browser using a URL.

-  The default value is 1000 – e.g. `http://YourServerName:1000/SgoMntrHome.htm`.
-  When connected to the local machine, the listen port can be updated if required. When changing this value, the following should be noted ...
 - Always ensure no other software or monitor is using the port you wish to assign. If two systems attempt to use the same port, the second will fail and connectivity will be lost. Care should therefore be taken when updating this value.
 - This value can only be changed when configuring the local server. The value is read-only when configuring remotely.
 - Existing web sessions using the original port will need to be reconfigured to use the new port/URL.
 - If client tool requests are also enabled, these too will use this port. Again, if the port is changed, existing registrations will need to be updated for each client tool in order for the system to function correctly.

Display dates in the following format


The setting of this option determines the format of dates displayed by the monitor. It will be defaulted to the appropriate value by the Setup Wizard but can be changed to one of the following values here ...

- Day/Month/Year
Dates are presented in the UK date format - dd/mm/yyyy.
- Month/Day/Year
Dates are presented in the US date format - mm/dd/yyyy.

-  This setting also affects the date format used within place-marker variables, such as `<$$TIMELOGGED>`, with the exception of those using a named format - e.g. `<$$TIMELOGGED-MDY>`.


Enable remote connections from Sentry-go client tools

Check this option to allow the monitor to be accessed from a Sentry-go Client Console or Quick Monitor Access Utility. To prevent access from these client tools, uncheck this option.

 If enabled, you can further restrict who can access this monitor using the security features described below.

Enable web reports to be generated from this monitor

Check this option to enable the embedded web server and access information from your web browser. To prevent web access to this monitor, uncheck this option.

 If enabled, you can further restrict who can access this monitor's web reports using the security features described below.

Configure alerts

This options allows you to determine how alerts are configured within the monitor. It can be set to one of the following values ...


- **In groups**

Select this option to configure alerts, contacts & notification scripts into groups – e.g. critical errors, warnings, administrators etc. These groups are then notified as a whole when defining checks.

This option replicates the earlier default behaviour for monitors prior v6.3.

- **Directly for each check**

Select this option, alerts are still configured centrally, but listed & assigned directly for the individual monitoring checks. This is the default option.

 When changing between these two options, the configuration utility will automatically be restarted and settings saved. When the option is changed, alerts are either configured to use the first alert group (for groups) or removed from all existing configured checks (for direct alerting).

Once settings have been saved, it is recommended that you verify the alerts assigned to monitoring checks before proceeding.

When responses are successful

When Sentry-go takes automatic action in response to a problem (e.g. runs a command or script, restarts a service etc.), you can be alerted to the action in a number of ways. This allows you to be kept informed of all problems, even if the monitor has corrected the fault automatically ...

- **Do not notify.**

Select this option to run automatic actions without notifying any Administrators that the action has taken place.

- **Notify, but don't run scripts.**

Select this option to notify associated Administrators by e-mail or network message when automatic actions are run. All Administrators configured to receive the associated alert (i.e. based on the Alert Level) will be notified, but no scripts will be run.



This option allows you to be notified by standard methods, without incurring any additional costs for using pager notification services etc., which can be reserved for unrecoverable errors only.

- **Notify, including scripts.**

Select this option to notify associated Administrators by e-mail or network message and run associated scripts when automatic actions are invoked. All Administrators configured to receive the associated alert (i.e. based on the Alert Level) will be notified, and all scripts (again based on the Alert Level) will be run.

When the monitor is started or reconfigured

This option is used to determine how the monitor should handle scheduled checks (checks that are specified to run once, at a set time on a given day) when it is first started, restarted or reconfigured. You can specify one of the following options ...

- **Do not run previous scheduled checks for today.**

Select this option if you do not wish to run, or re-run checks that would have already been run based on the current time. In this case, the check is assumed to have been run previously at the designated time.

- **Run or re-run previous scheduled checks for today.**

Select this option if you wish the monitor to run, or re-run all checks that would have been run earlier based on the current time, even if they have been run previously.

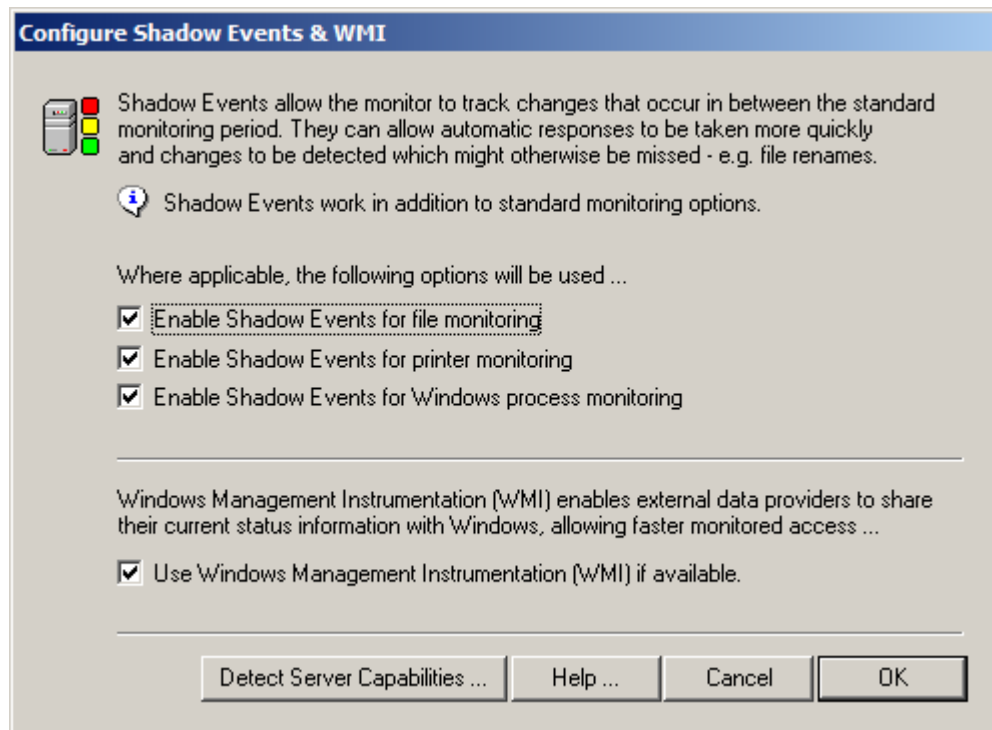



This is the default options and emulates the behaviour of previous Sentry-go versions.

Configuring shadow events

Sentry-go supports what are known as “shadow events” which allow monitoring components to utilise Windows events & notifications in addition to the standard scan-based checks. Using shadow events, the monitor can respond at the time a specific action takes place by being notified that the action has occurred.

To configure them, click the “Configure Events” button to display the following window which allows you to enable or disable the use of events for the monitoring components shown ...



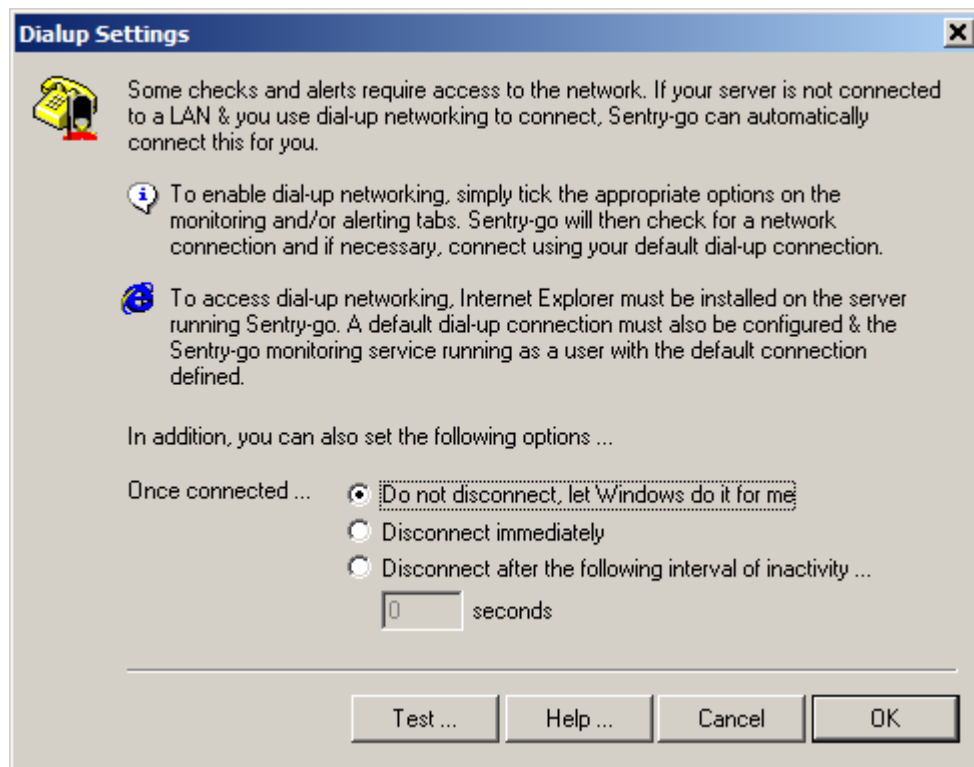
 Even if the above components are not installed or configured, the options above will still be shown. If the corresponding option is not installed, the setting here will have no effect.

Windows Management Instrumentation or WMI can also be enabled or disabled from here.

For more information please refer to “Sentry-go Shadow Events”.

Configuring dial-up networking

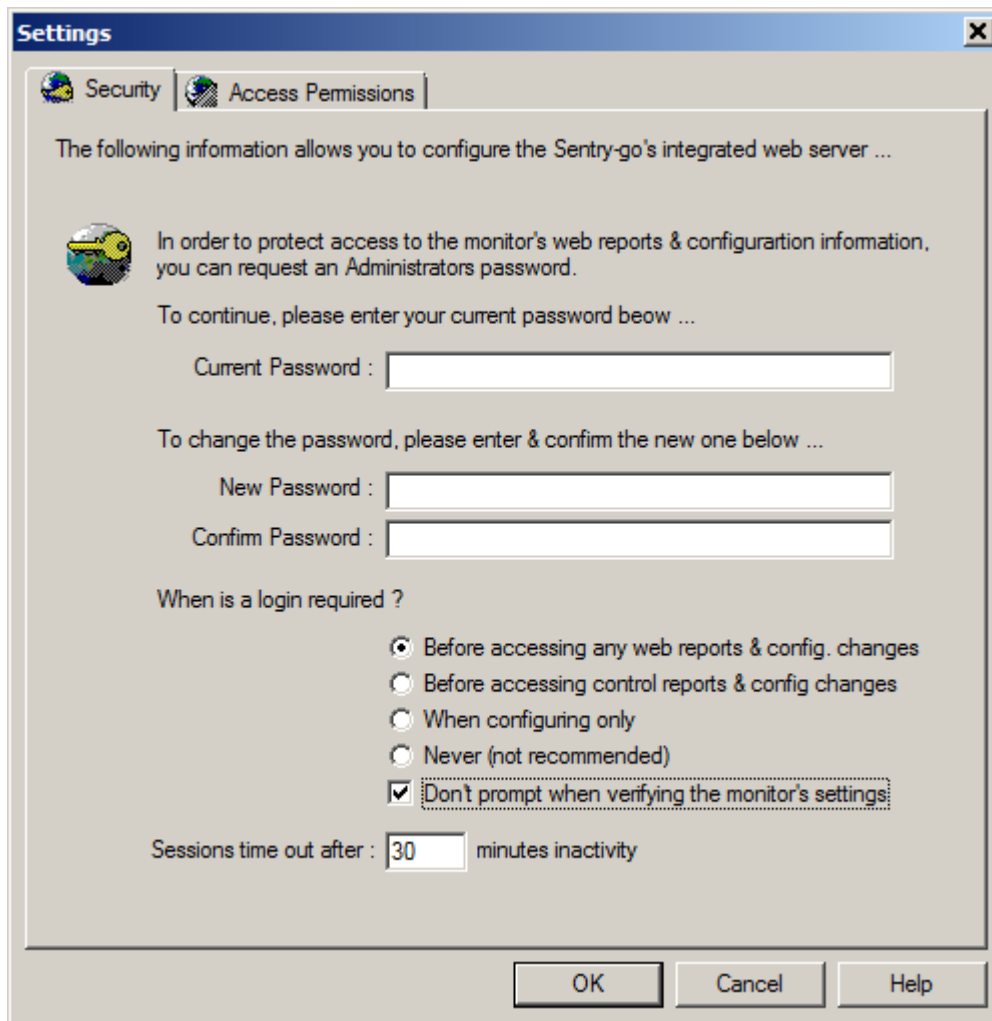
Although unlikely to be needed in most environments, Sentry-go supports the use of Windows dial-up in order to connect to the network. To configure this, click the "Configure Dial-up ..." button.



i For more information, please refer to "Sentry-go Dial-up Networking".

Configuring security settings

In addition to the general settings above, you can further refine security settings by clicking the “Configure Security ...” button. A window similar to the one below will be displayed, allowing you to configure both security & access permissions features ...



The screenshot shows a 'Settings' dialog box with two tabs: 'Security' and 'Access Permissions'. The 'Security' tab is active. The dialog contains the following elements:


- A title bar with the text 'Settings' and a close button (X).
- Two tabs: 'Security' (selected) and 'Access Permissions'.
- Introductory text: 'The following information allows you to configure the Sentry-go's integrated web server ...'
- An icon of a globe with a keyhole.
- Text: 'In order to protect access to the monitor's web reports & configuration information, you can request an Administrators password.'
- Text: 'To continue, please enter your current password below ...'
- Text: 'Current Password :' followed by a text input field.
- Text: 'To change the password, please enter & confirm the new one below ...'
- Text: 'New Password :' followed by a text input field.
- Text: 'Confirm Password :' followed by a text input field.
- Text: 'When is a login required ?'
- A list of radio button options:
 - Before accessing any web reports & config. changes
 - Before accessing control reports & config changes
 - When configuring only
 - Never (not recommended)
 - Don't prompt when verifying the monitor's settings
- Text: 'Sessions time out after :' followed by a spin box containing '30' and the text 'minutes inactivity'.
- Buttons: 'OK', 'Cancel', and 'Help'.

Security settings

The first tab is used to control various aspects of the web server which is responsible for both web reporting and communication with client tools.

Current Password


Before you can change any administrator setting, you must enter the existing password on this field.

 If no password is currently defined, simply leave this field blank.

Depending on when passwords are enabled (see below), you will be prompted to enter this password when you wish to configure the Sentry-go monitor or display a Sentry-go web report

New Password

To change the administrator's password, simply enter the current value (if any) above, then the new one here.

 If you do not want to change the password, simply leave this entry blank.

Confirm Password


If you have entered a new password, you must confirm the value entered by re-keying it here.

When is login required ?

This option determines when a user will be asked to enter the password defined above. The following values are available ...


- **Before accessing any web reports & config. changes**

Select this option for the highest level of security. If selected, the user will be asked to login before any web report is displayed (except the home page and Configuration Verification Report). They will also be asked to login when they attempt to edit the monitor's configuration through the Console.

 The login page will be shown for all reports unless the user is already logged in. To timeout sessions automatically, see below.

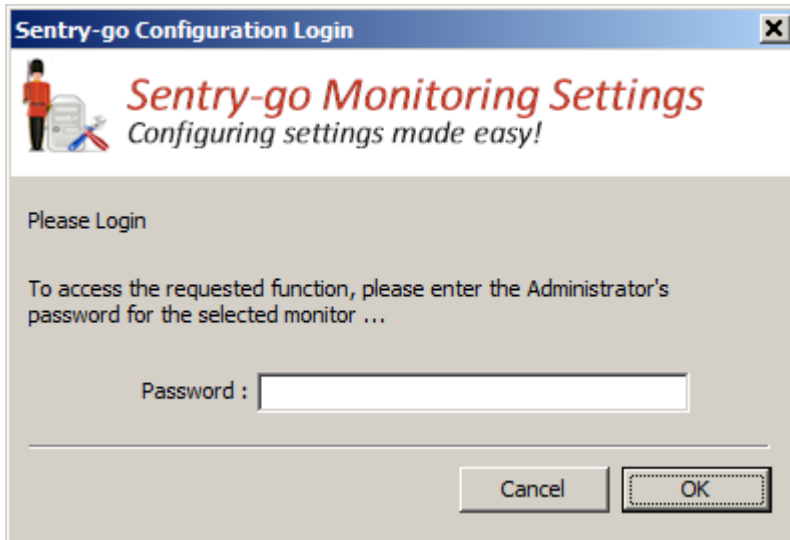
- **Before accessing control reports & config. changes**

Select this option to request user login for any report that allows changes to be made (e.g. service control, terminate SQL Server connection etc.) The user will also be asked to login when they attempt to edit the monitor's configuration through the Console.

 The login page will be shown for all reports unless the user is already logged in. To timeout sessions automatically, see below.

- **When configuring only**

Select this option to request user login only when they wish to edit the monitor's configuration through the Console. No login will be displayed for web reporting.



- **Never (not recommended)**

Select this option to disable logins and session timeouts.

- ⚠ This option is not normally recommended, especially if you allow access from the internet. It also allows anyone to potentially run the Console and access/edit the monitor's configuration settings unchecked.

- **Don't prompt when verifying the monitor's settings**

Select this option to disable logins when verifying monitoring, alerting & response settings from client tools. Ticking this option means you won't be prompted when displaying the monitor's verification web reports as a result of a client request.

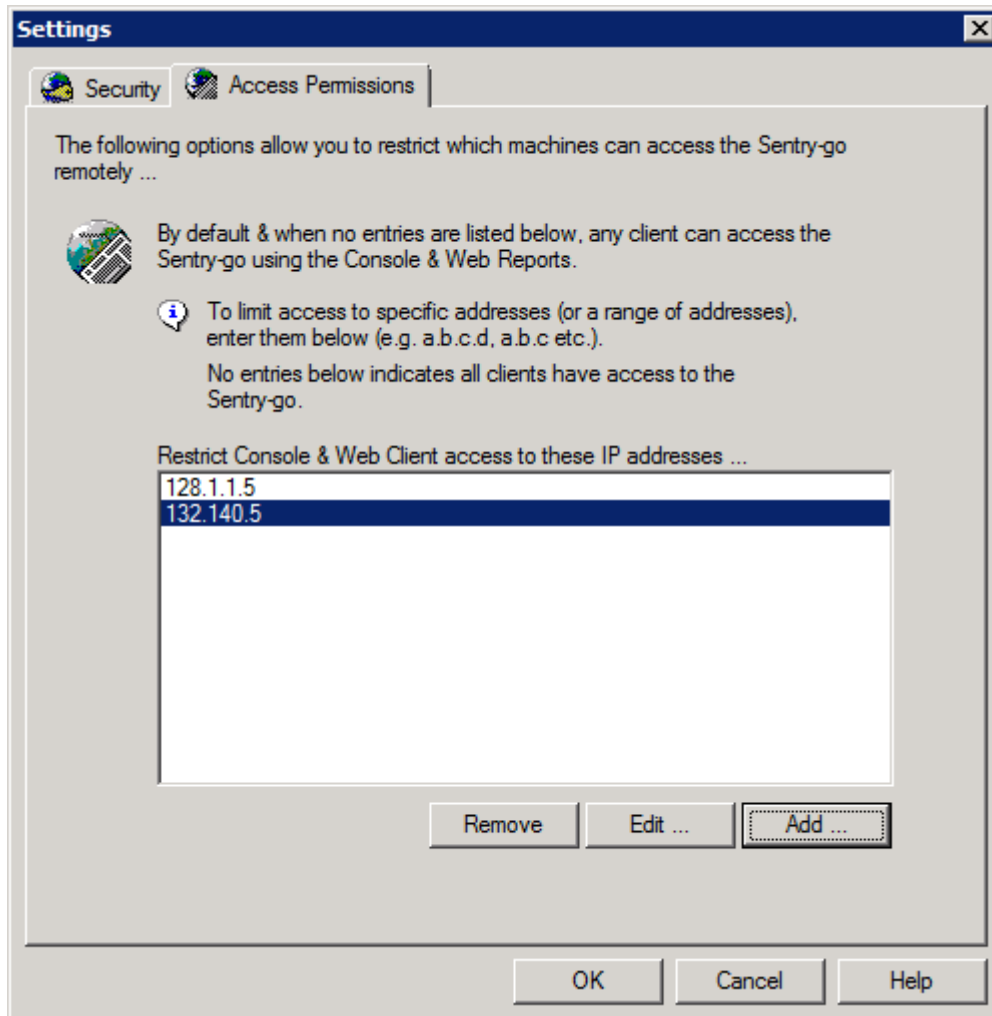
Sessions time out after ...

This option controls how long a web session remains active when no requests are made. The higher the value specified, the longer an existing logged on session remains (and the user not re-prompted for their password again) even if no requests are made.

- ℹ This option is not used if logins are not enforced (i.e. "Never" is selected above).

Restricting client tool access

The second “Access Permissions” tab allows you to control which PCs can access the Sentry-go monitor, both in terms of web reporting and from client tools.



By default, any client PC can connect to the Quick or Sentry-go Plus! monitor using either client tools or a web browser, assuming the integrated web server is enabled. However, if you want to restrict who can access the system, you can limit access to specific IP addresses or a range of IP-addresses by including them on this screen ...

- If no entries are listed here, all clients can access the monitor, subject to any other security restrictions.
- To allow access to a specific IP address, simply add its value to the list. For example ...

132.78.70.82
132.78.70.83
132.78.70.84

- To allow a range of IP-addresses, enter a partial address (the numbers that are common). For example ...

132.78.72

132.78.70

132.78.65



Use this option if your company uses DHCP where clients can receive different addresses within one or more given ranges.



Bear in mind that a PC may have more than one address – for example, the local server may have a static IP address such as 132.78.72.1, but will also have a local “loopback” address, 127.0.0.1.

If access fails yet you think the IP address is entered above (or within a valid range entered above), use IPConfig or an equivalent utility to check your IP addresses, and for local machines remember the standard 127.0.0.1 as well.

Configuring web publishing

In addition to its own integrated web server, Sentry-go allows you to periodically take snapshots of selected web reports & publish them to an external web server. This can be particularly useful if your monitors run within a firewall, yet you want external access to reports from your public-facing web server. To configure publishing, click the "Web Publishing ..." button..

Publish to External Web Server

The following information is used to publish Sentry-go's web reports to an external web server ...

The home page for generated reports will be :

Enable web publishing/synchronisation

Sync. web reports every : seconds

Synchronize images when monitor started

Include server name in published reports

Also publish Enterprise Option reports

Publish using Windows copy

Copy files to this directory :

(Specify full UNC path for remote location
- e.g. \\Server\ShareName)

The user running the Sentry-go monitoring service must have access to this local drive or share in order to synchronize files.

Publish using the FTP

FTP server :

Connect using dial-up before connecting

Connect to port :

Login (leave blank for none) : Password :

Copy files to this directory :

For more information, please refer to "Publishing Sentry-go Web Reports".

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](#).



*Sentry-go, © 3Ds (UK) Limited, 2000-2013
East Molesey, Surrey. United Kingdom
T. 0208 144 4141
W. <http://www.Sentry-go.com>*