



Configuring General Settings for Sentry-go

Last Updated Thursday, 19 April 2012

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



Be Proactive, Not Reactive!

Table of Contents

Symbols	2
Background.....	2
Configuring Settings	3
Configuring Shadow Events	7
Configuring Dial-up networking.....	8
Configuring Security Settings	9
Sentry-go Security Settings	10
Requesting Console Login.....	12
Restricting Client Access.....	13
Configuring Web Publishing	15
More Information, Help & Support.....	16

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.

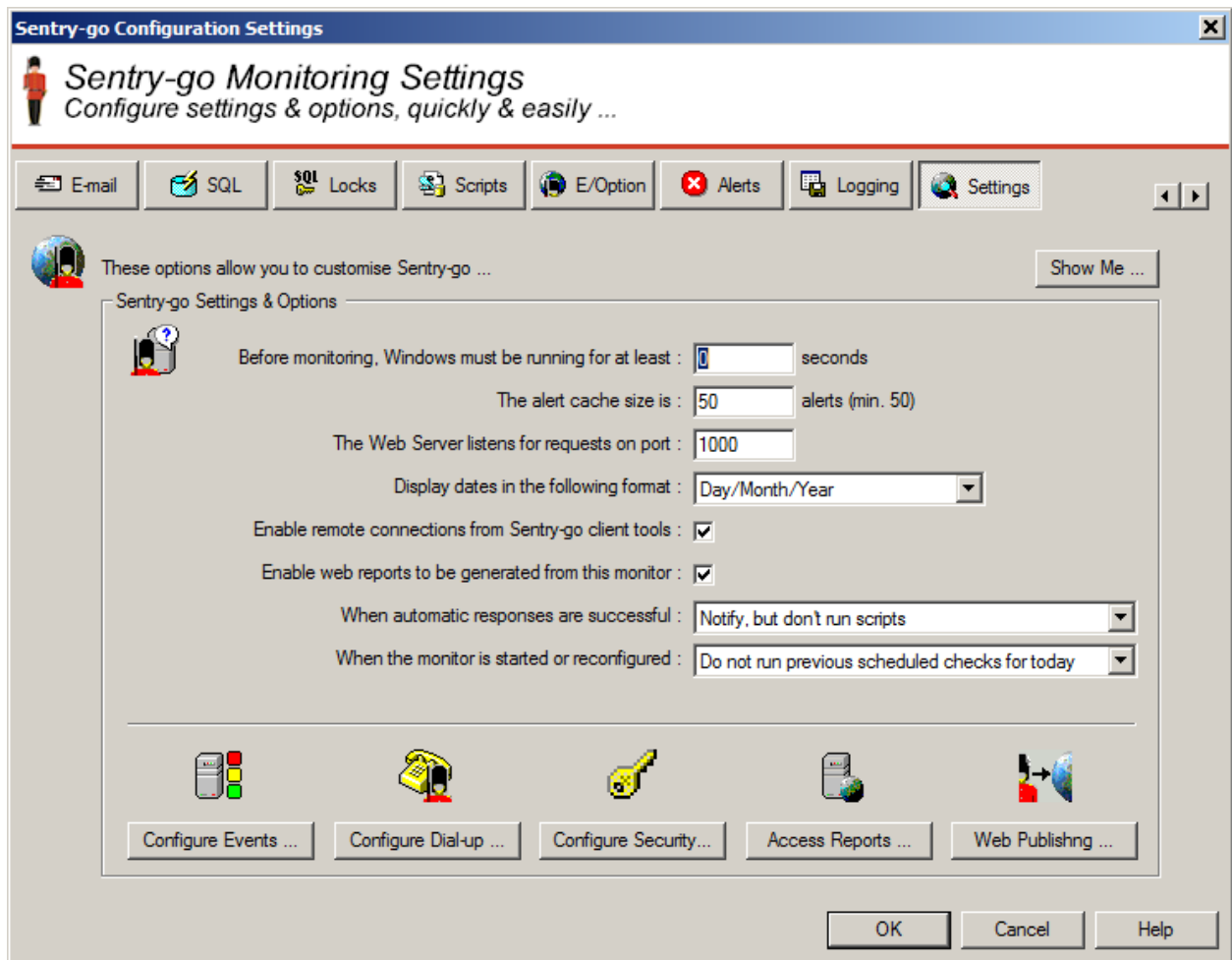
Background

In addition to monitoring & alerting functionality, other options can also be used to configure Sentry-go & the way it works. For example, you can configure ...

- General options such as date format and cache sizes
- The integrated web server
- Security features
- Publishing web reports to an external web server
- Dial-up networking

Configuring Settings

To configure Sentry-go's primary settings, simply select the monitor from the Client Console, or connect via the Easy Access Utility and click "Configure". A window containing a number of tabs will be displayed. From this window, click the "Settings" tab to display the following window ...



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 refreshed/reconfigured to use the new port/URL.
- If Client Console 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 Console 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 Quick 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 & Easy Access Utility and for it in turn to send triggered alerts to them etc. 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 by this Sentry-go 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.

When automatic action is 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.

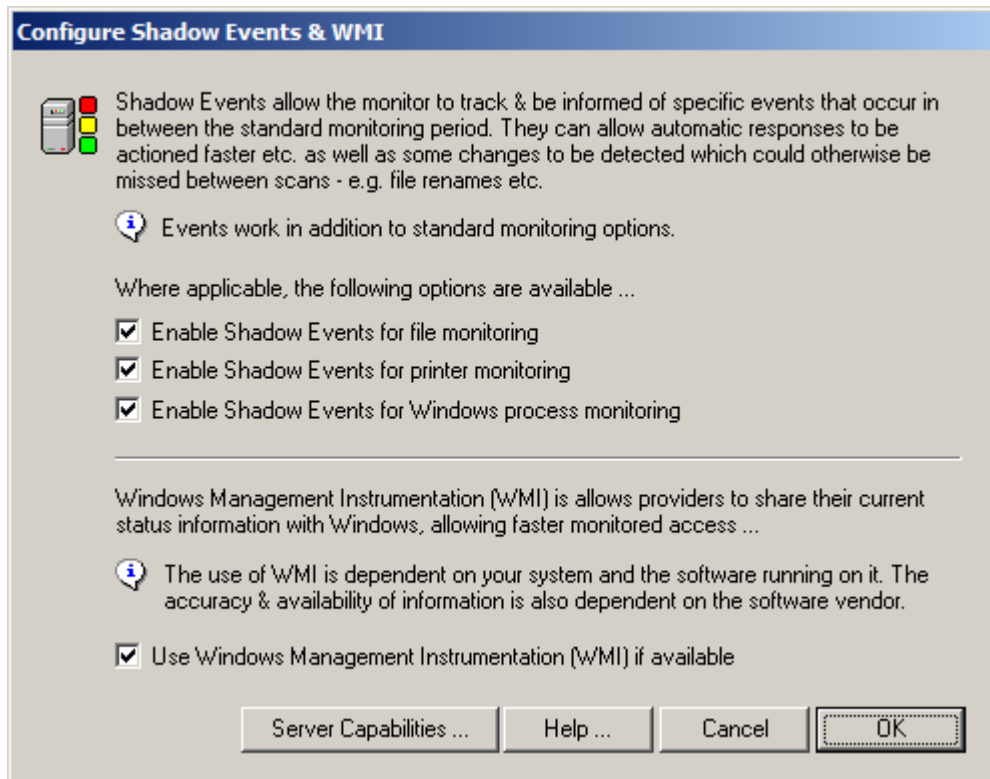
Select this option if you wish the monitor to run, or re-run all checks that would have been run earlier based on the current time, even if they have been run previously.


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

Configuring Shadow Events

Sentry-go supports the use of “Shadow Events”. For some components these allow the monitor to utilise notifications in addition to standard scan-based checks. Put simply, it allows the monitor to 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 ...



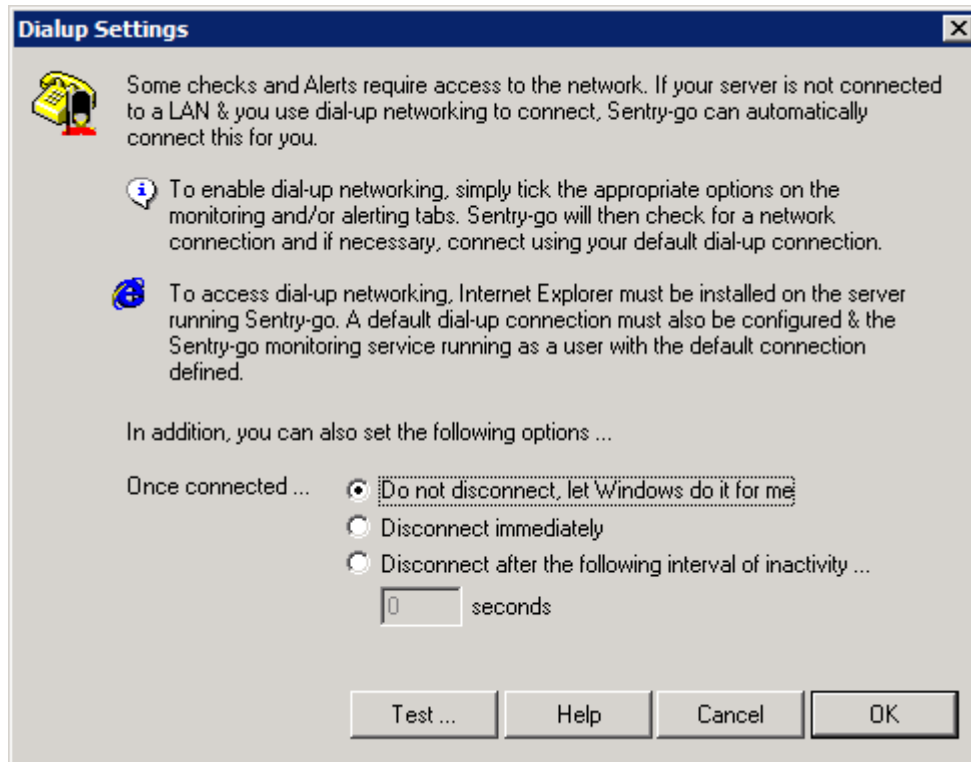
 Even if the above components are not installed or configured, the options above will still be shown. If the corresponding option is not installed, the setting here will have no effect.

WMI can also be enabled or disabled from here.

For more information on “Shadow Events” and their uses, please refer to [Sentry-go – Shadow Events](#).

Configuring Dial-up networking

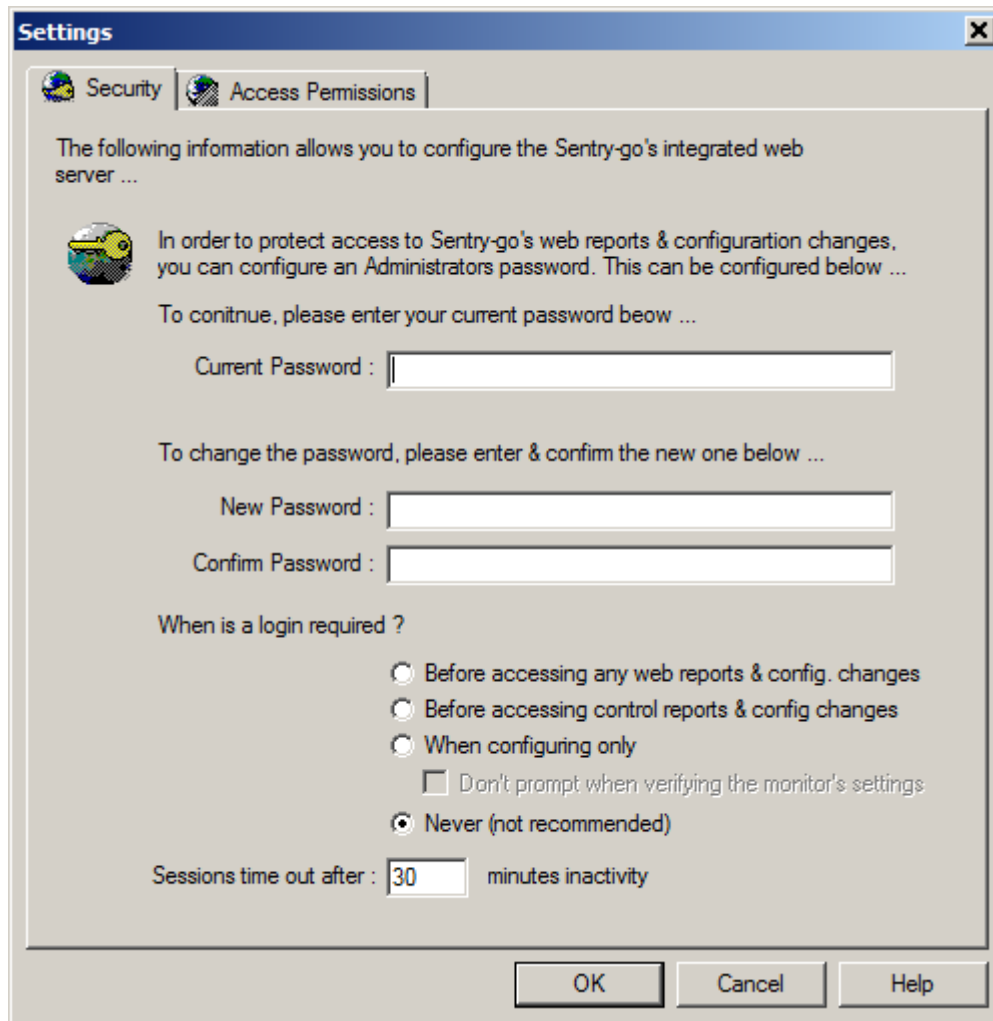
Sentry-go supports Windows dial-up in order to connect to the network. If your server is permanently connected to the LAN or you do not use dial-up, there is no need to configure these settings. If you do use dial-up, you can specify how the connection is to be handled once it has been used by clicking the "Configure Dial-up ..." button.



For more information, please refer to [Sentry-go - Configuring 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 Windows-style dialog box titled "Settings" with a close button (X) in the top right corner. It has two tabs: "Security" (selected) and "Access Permissions". The main content area contains the following text and controls:

The following information allows you to configure the Sentry-go's integrated web server ...

 In order to protect access to Sentry-go's web reports & configuration changes, you can configure an Administrator's password. This can be configured below ...

To continue, please enter your current password below ...

Current Password :

To change the password, please enter & confirm the new one below ...

New Password :

Confirm Password :

When is a login required ?

- Before accessing any web reports & config. changes
- Before accessing control reports & config changes
- When configuring only
- Don't prompt when verifying the monitor's settings
- Never (not recommended)

Sessions time out after : minutes inactivity

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Sentry-go Security Settings

The first tab is used to control various aspects of the Web Server which is responsible for both web reporting and certain aspects of the Console.

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), it will be requested when ...

- You wish to configure the Sentry-go monitor
- You wish to display a Sentry-go web report

New Password

To change the Administrator's password, simply enter the current value (if any) above, and 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 ?

The options here determine when a user will be asked to enter the password defined above. This will be requested on the web report's login page and/or on the Console when a configuration change is requested. 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**

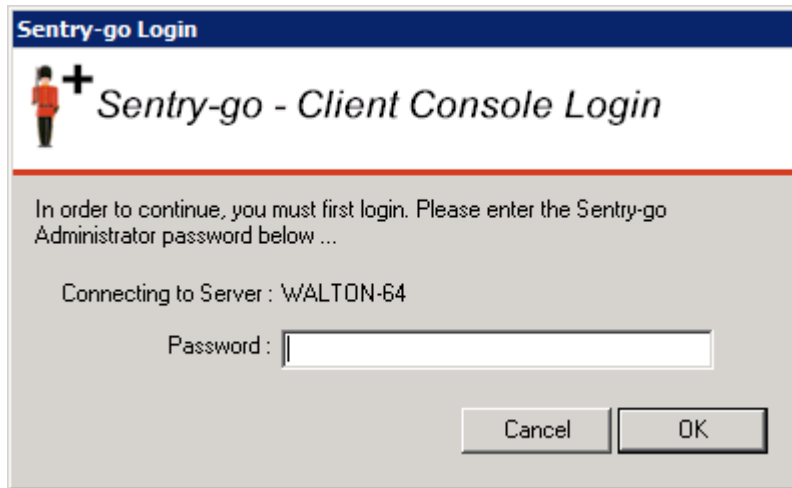
Select this option to request user login for any report that allows changes to be made (e.g. service control, terminate SQL Server connection etc.) The user will also be asked to login when they attempt to edit the monitor's configuration through the Console.



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.

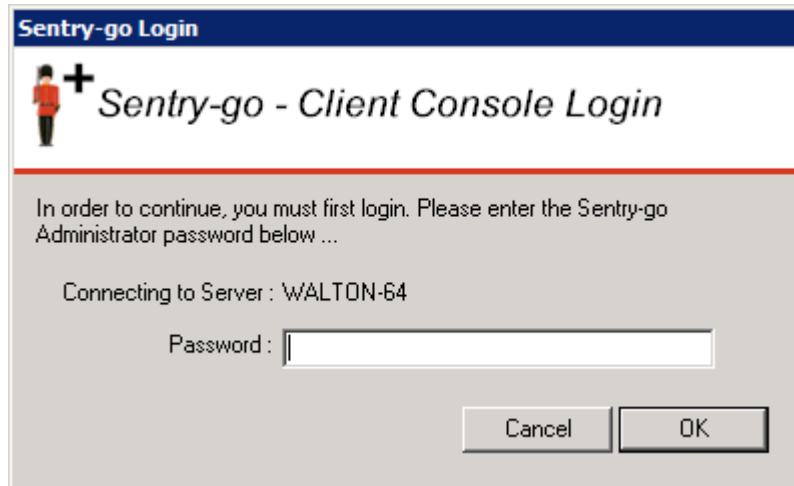
Sessions time out after ...

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.

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


Requesting Console Login

If an Administrator's password is defined & enabled, the following prompt will be displayed each time you click Configure for the monitor through the Console ...



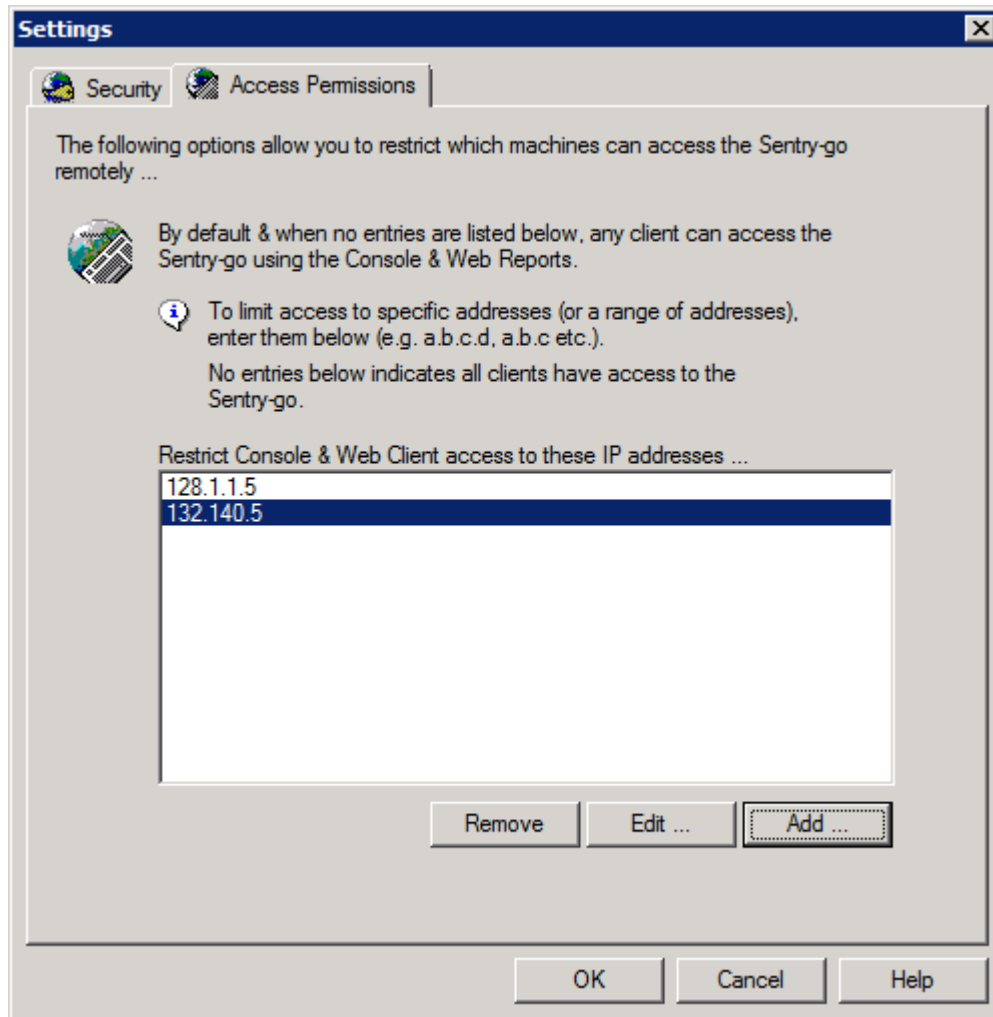
The image shows a dialog box titled "Sentry-go Login". The title bar is dark blue with the text "Sentry-go Login" in white. Below the title bar, there is a logo consisting of a red stick figure with a black plus sign to its right, followed by the text "Sentry-go - Client Console Login" in a black serif font. A horizontal red line separates the header from the main content area. The main content area has a light gray background and contains the following text: "In order to continue, you must first login. Please enter the Sentry-go Administrator password below ...". Below this text, it says "Connecting to Server : WALTON-64". There is a text input field labeled "Password:" with a white background and a black border. At the bottom right of the dialog box, there are two buttons: "Cancel" and "OK", both with a light gray background and a black border.

To proceed, enter the Administrator's password (as defined above) and click OK.

-  If you do not know the password you will be unable to configure the monitor. In this case please contact your System Administrator.

Restricting Client 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 the Sentry-go Client Console, if these options are enabled.



By default, a browser from any client PC with connectivity to the server can access Sentry-go's integrated web server assuming the web server is enabled. Also, if they are running the Console and the monitor has been registered, they will be able to access the monitor through there as well, again, assuming Console 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 listing them on this screen.


- If no entries are listed, all clients may access the monitor.
- To allow access to a specific IP address, simply add it's value to the list. For example ...

132.78.70.82
132.78.70.83
132.78.70.84

- To allow access to a group of 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 your external web server ...

 Use this option to copy Sentry-go dynamically generated web reports to another web server - e.g. synchronize reports with a web server outside your firewall. Standard web reports can be synchronized periodically as configured below.


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
 Publish Enterprise Option reports (if available)


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


 Connect using dial-up before connecting

FTP server :

Connect to port :

Login (leave blank for none) : Password :

Copy files to this directory :

 For more information, please refer to [Sentry-go - Publishing Web Reports](#).

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>