

The Sentry-go Monitoring System Monitoring TCP/IP Port Availability & The Windows Firewall

Last Updated Friday, 15 April 2011

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

Be Proactive, Not Reactive!

Table of Contents

| | |
|--|----|
| Symbols | 2 |
| Background..... | 2 |
| Recommended Monitoring Settings | 3 |
| Quick Facts..... | 4 |
| Monitoring the Windows Firewall..... | 5 |
| Monitoring TCP/IP Port Availability | 7 |
| Configuring TCP/IP Port Monitoring | 8 |
| Temporarily Ignoring a Configured Check..... | 10 |
| Configuring an Automatic Response | 10 |
| More Information, Help & Support | 11 |

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

TCP/IP Port Monitoring

TCP/IP ports are an important part of any internet or network communication. Services such as web, FTP or mail servers listen on "well known" ports for incoming requests. Browsers & mail clients in turn connect to the server using these ports. Once a connection is established, the request can be forwarded and actioned as appropriate. Checking that a port is ready to receive a new request is therefore an extremely effective way of establishing whether the underlying service is functioning correctly.

Manually checking each port is actually quite complex and time consuming and often involves a number of different client applications. With Sentry-go, the whole monitoring process is automated and run continually in the background. With this method, you can simply be informed of any failures and need not rely on affected users (or potentially customers) to report faults.

Windows Firewall Monitoring

Access to ports is often controlled or restricted using the Windows firewall, a system that ensures only enabled applications can access local resources from across the network and thus preventing suspicious or malicious code, such as viruses from accessing the server. The firewall and its continued running is therefore of vital importance on many systems.

With Sentry-go, the status of the Firewall can be periodically verified automatically and action taken if it is found to be disabled etc.

Recommended Monitoring Settings

It is recommended that all standard ports used by the server's services are checked to ensure they are available for inbound connections. The actual ports monitored will depend on the services running & the server's primary function.

For example ...

- Port 80 for inbound web server (HTTP) connections
- Port 443 for inbound secure web server (HTTPS) connections
- Port 21 for inbound file transfer server (FTP) connections
- Port 25 for outgoing e-mail (SMTP) connections
- Port 110 for incoming e-mail (POP3) connections
- Port 110 for incoming e-mail (POP3) connections



In general, any application that responds to TCP/IP requests will "listen" on a well known port, or one that it configures. Sentry-go's integrated web server for example listens for requests on a TCP/IP port. Other ports in addition to the list above may, therefore also need to be checked. The actual list will depend on the software installed & running on your server, including custom applications.

It is also recommended that the Windows Firewall be monitored and automatically re-enabled if found to be disabled.

Quick Facts

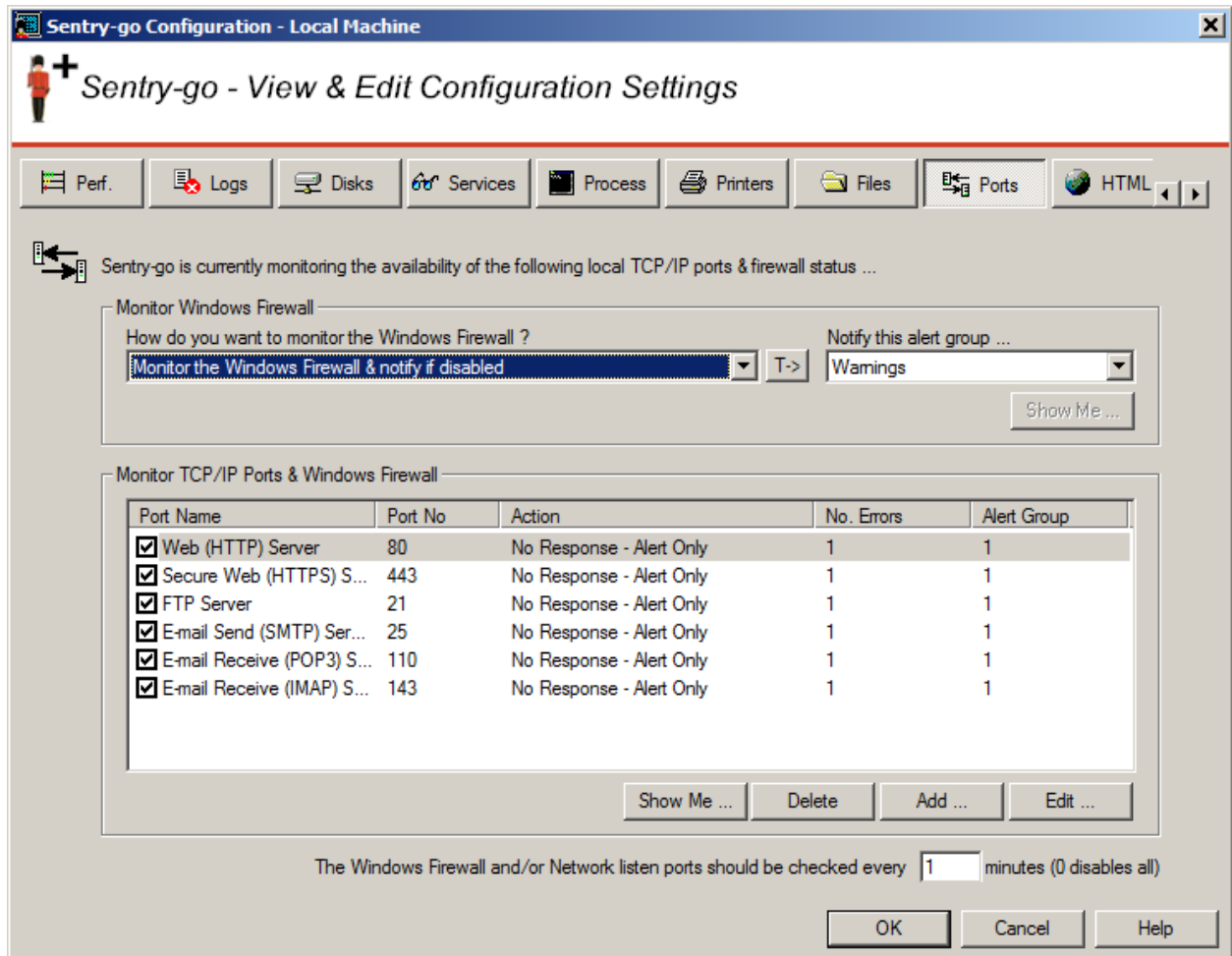
Here is a summary of the options available with this component. They are discussed in more detail in the pages that follow ...

| | |
|----------------------------|---|
| Component : | TCP/IP Port & Firewall Monitor |
| Aim/Description : | To provide periodic monitoring of the Windows Firewall and listening TCP/IP Ports, to ensure the underlying service is listening & responding to requests. |
| Main Monitoring Features : | <ul style="list-style-type: none">• Automatically monitor the status of the Windows Firewall• Verify the accessibility of a given port• Optionally send & receive a string identifying the target application listening on the port – e.g. an SMTP server |
| 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 the Windows Firewall

To monitor the current status of the Windows firewall, 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 “Ports” tab. From here, you can configure TCP/IP port as well as Windows Firewall monitoring ...



The top section of this window controls Sentry-go's automatic monitoring of the Windows firewall.

How do you want to monitor the Windows Firewall ?


This setting determines if Sentry-go should monitor the firewall and if it does, what should happen if the firewall is found to be disabled. It can be set to one of the following ...

- **Do not monitor the Windows Firewall**

Select this option to disable the checking of the Windows firewall. With this option, Sentry-go will not verify the firewall state at any time.

- **Monitor the Windows Firewall & automatically enable if disabled**

Select this option to enable the automatic checking of the Windows firewall. With this option, Sentry-go will periodically verify the firewall state and, if found to be disabled, automatically attempt to re-enable it.


 If the firewall cannot be enabled, an alert will be generated, based on the alert group specified.

- **Monitor the Windows Firewall & notify if disabled**

Select this option to enable the automatic checking of the Windows firewall. With this option, Sentry-go will periodically verify the firewall state and, if found to be disabled, notify one or more administrators based on the alert group specified.

- **Monitor the Windows Firewall & reboot the server if it can't be enabled**

Select this option to enable the automatic checking of the Windows firewall. With this option, Sentry-go will periodically verify the firewall state and, if found to be disabled, attempt to re-enable it. However, if it can't be enabled, the server is automatically rebooted.

 If the firewall is of paramount importance to the operation of your server, this option will help ensure the server's protection is not compromised.

After rebooting, if the firewall continues to fail, an alert will be generated. The monitor's automatic reboot protection ensures the server will continually be restarted in this case.

Notify this alert group

The value selected here indicates the Alert Group that will be triggered for any corresponding alert that is raised in the event the Windows Firewall should fail. The Alert Group is used by the monitor to determine which System Administrators should be notified and/or Scripts run in response to the triggered alert.

The Windows Firewall and/or Network listen ports should be checked every (mins)

This value specifies how often, in minutes, Sentry-go should check the status of the Windows Firewall and that defined ports are accessible for inbound network traffic.

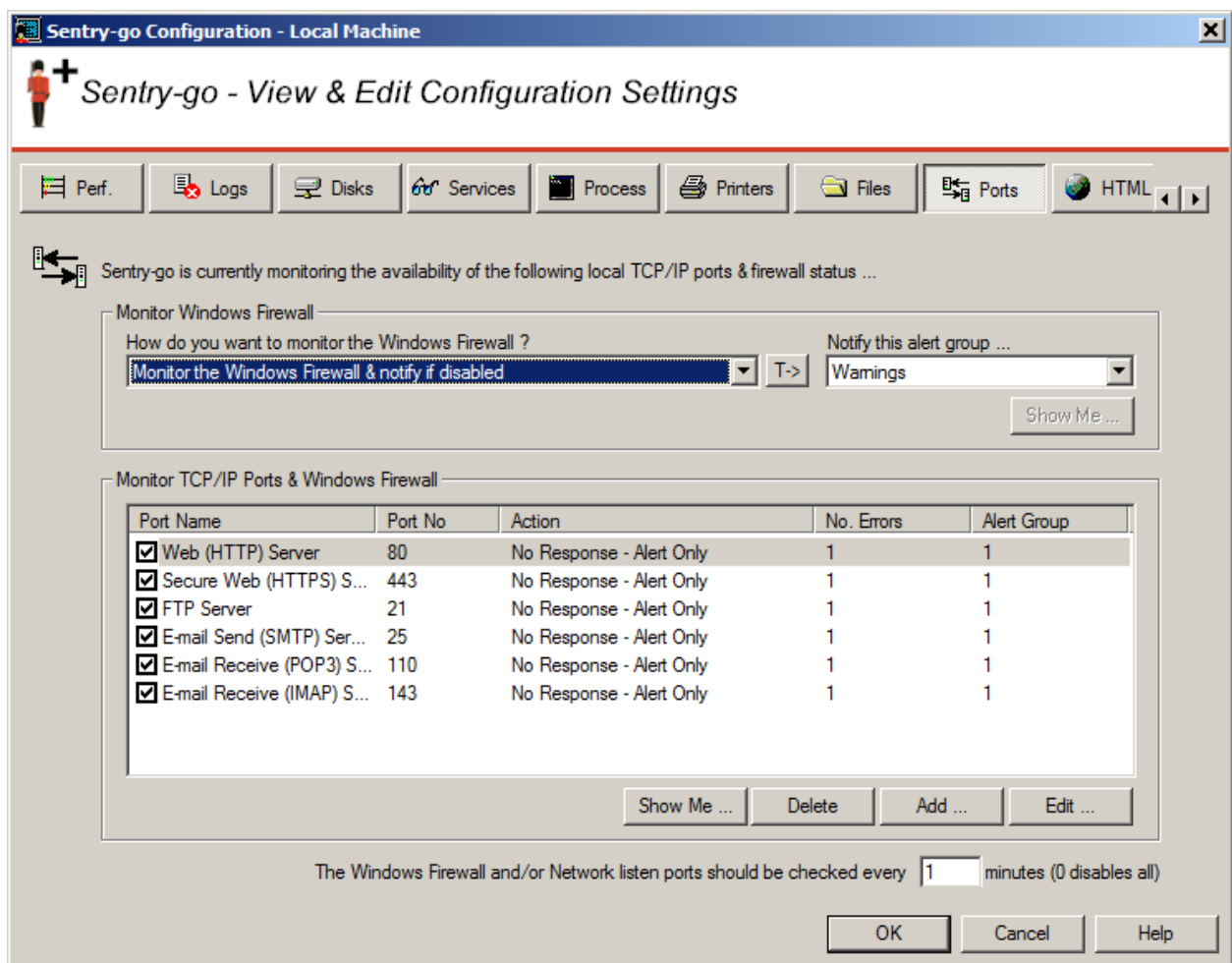
Monitoring TCP/IP Port Availability

To monitor TCP/IP Port access & 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 "Ports" tab. From here, the lower section allows you to configure the following ...

- The monitoring of one or more TCP/IP Ports.
- What should happen in the check fails.
- How often each check should be run.
- Temporarily disable the monitoring of one, more or all ports.

The resulting list will show all the currently defined ports which are currently being monitored (or temporarily ignored). From here you can add new monitored items, edit existing ones or delete them from the monitor's scan.

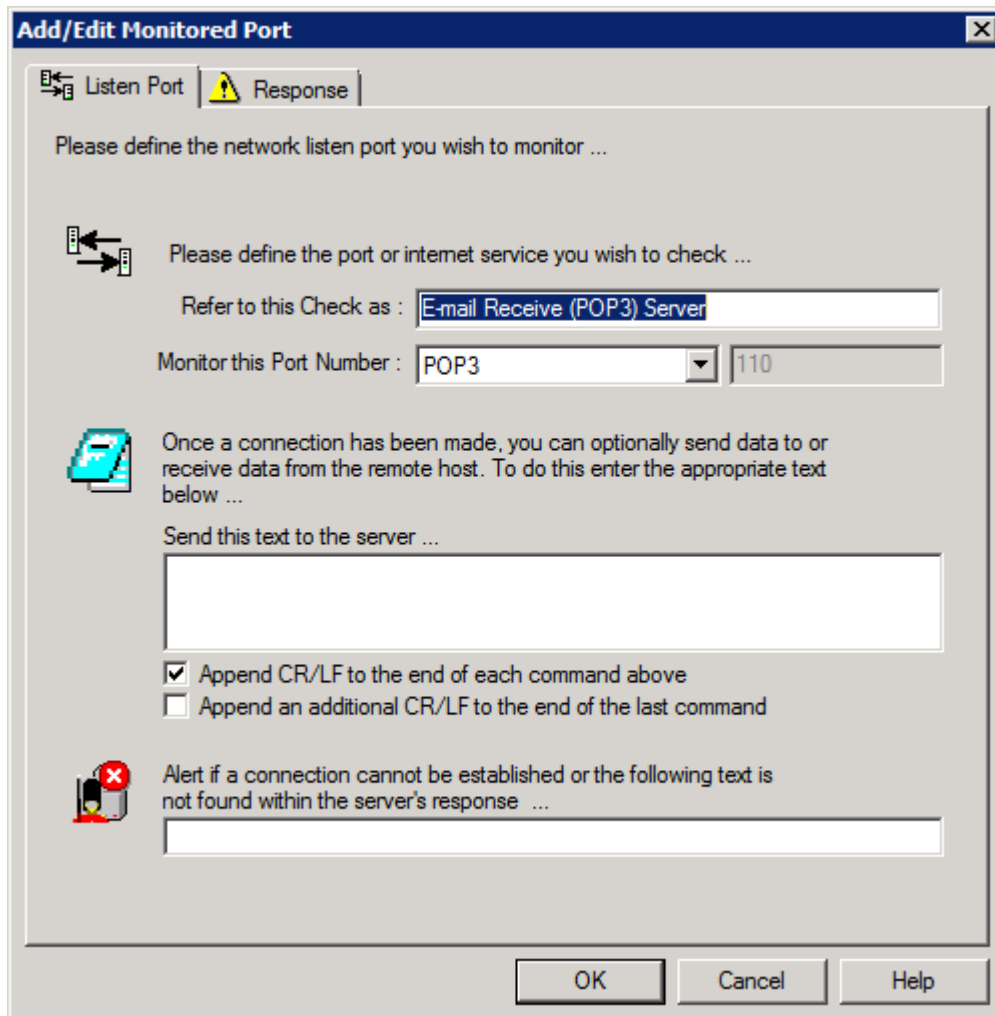


The Windows Firewall and/or Network listen ports should be checked every (mins)

This value specifies how often, in minutes, Sentry-go should check the status of the Windows Firewall and that defined ports are accessible for inbound network traffic.

Configuring TCP/IP Port Monitoring

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



Add/Edit Monitored Port

Listen Port | Response

Please define the network listen port you wish to monitor ...

Please define the port or internet service you wish to check ...

Refer to this Check as :

Monitor this Port Number :

Once a connection has been made, you can optionally send data to or receive data from the remote host. To do this enter the appropriate text below ...

Send this text to the server ...

Append CR/LF to the end of each command above

Append an additional CR/LF to the end of the last command

Alert if a connection cannot be established or the following text is not found within the server's response ...

OK Cancel Help


From here you can define which port the monitor should attempt to connect to and any additional parameters or checks it should carry out.

Refer to this check as

This is the name that you will refer to the check as on both web reports and in any alerts generated. It is recommended that a short and accurate description be placed here - e.g. Main E-mail Server.


Monitor this Port Number

This option defines the port you wish to verify. The selection box lists the main "well known" ports you are likely to use. Simply select the name of the service you wish to check and its default port will be assigned.

-  To select a different or custom port (or to monitor a standard service that is configured to use a custom port), select "(Other)", and enter the port number in the following field directly.


Send this text to the server (Optional)

After a successful connection has been made, you can further verify the remote server/service by sending a text command to it in order to initiate a response - e.g. HELO.

-  Many servers (e.g. POP3, IMAP etc.) are based originally on the UNIX platform and therefore the standard dictates that a Carriage Return/Line feed (CR/LF) combination be sent after a command, not a simply carriage return. To ensure this is sent, select the check box below.

Append CR/LF to the above command (Optional)

Some servers or remote services such as POP3 & IMAP require a Carriage Return/Line feed (CR/LF) to be sent after the command. This indicates the end of the particular command. To have Sentry-go append a CR/LF to your command, simply select this check box.

-  If the command continually seems to time out, yet the service is running & the command string is correct, then you should ensure that this option is enabled. If in doubt, it is recommended that this option is enabled.


Append an additional CR/LF to the last command (Optional)

In addition to the above, some services also require an additional CR/LF combination be sent. This indicates to them that no further commands are being sent and they can process/respond accordingly. To have Sentry-go append this additional CR/LF, simply select this check box.

Alert if this text is not found within the server's response (Optional)

Regardless of whether a command is sent to the server or not, you can also check the response returned - from either the initial connection or the above command. This is particularly useful in order to confirm that the correct service is responding to the request.

If the text entered here is not found within the response, an alert will be triggered. Only part of the returned text need be entered here.

-  To determine the appropriate text returned from the server, connect to the service using a Telnet client and note either the initial response (following the connection) or the response to the command entered above.

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>