



Configuring Sentry-go Monitoring Alerts

© 3Ds (UK) Limited, October, 2013

<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

Alongside monitoring itself, alerting is another important part of Sentry-go. Alerts are triggered in response to detected errors and allow you to be informed of the problem in a quick and convenient manner.

In this guide

Direct Alerts vs Alert Groups	2
Configuring alerts & contacts	3
Creating a new alert contact	4
Alerting via E-mail	5
Alerting via SMS/text message	8
Alerting via network message	11
Alerting using an “implicit” script	13
Alerting using a custom script, command, batch file or 3 rd party application	17
Example batch file or script	20
Example script for recording to a SysLog file.....	21
Example SMS script for gateway bureau, using e-mail	23
Example SMS script for gateway bureau, using http (web)	26
Specifying message text	28
Notifying based on schedule	29
Configuring alert groups.....	30
Triggering an alert from a check using direct alerts	31
Triggering an alert from a check using alert groups	32
Preventing repeated alerts with ACM	33
More Information	34

Direct Alerts vs Alert Groups

Sentry-go implements alerts in one of two ways, either “directly” or using “alert groups”.

- **Direct Alerts.**

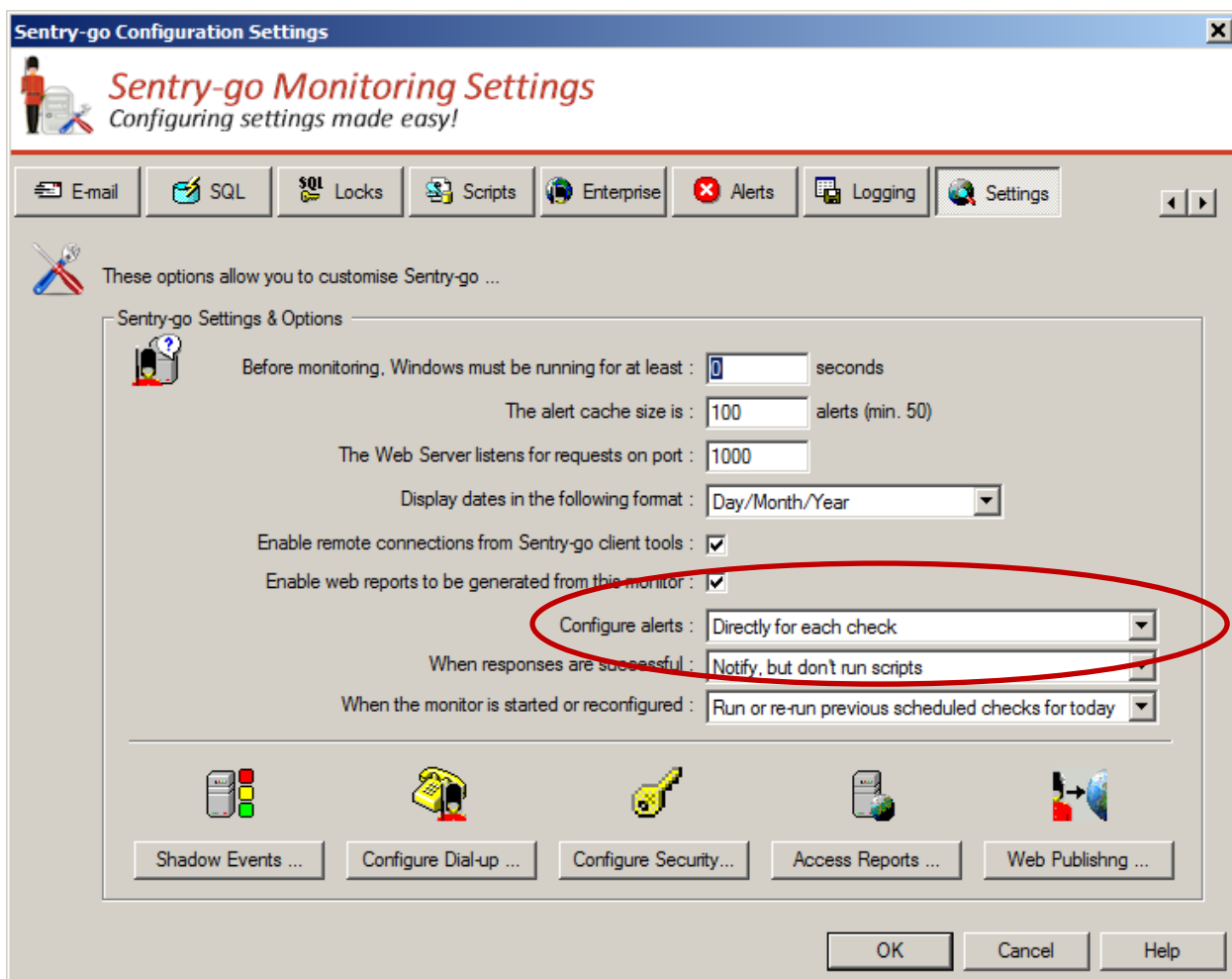
For smaller installations, direct alerts offer a quick & easy way to configure the monitor. In this mode you simply define your alerts once – e.g. contacts such as e-mails, network users, SMS or scripts and these are then listed against each monitoring check.

- **Alert Groups**

For larger installations, where you’re more likely to have teams looking after an area of your environment – e.g. network, databases, e-mail etc., you can further divide your alert contacts & scripts into one or more “groups”. These might be, for example, “critical errors”, “warnings” & “information” or “network”, “DBAs” & “app. team”.

In this mode, you still define your alerts but each contact is additionally assigned to one or more alert groups. When you then define your monitoring checks, instead of selecting the individual contacts you wish to notify for each check, you simply choose which alert group to notify. This in turn determines who will be notified when an alert is triggered.

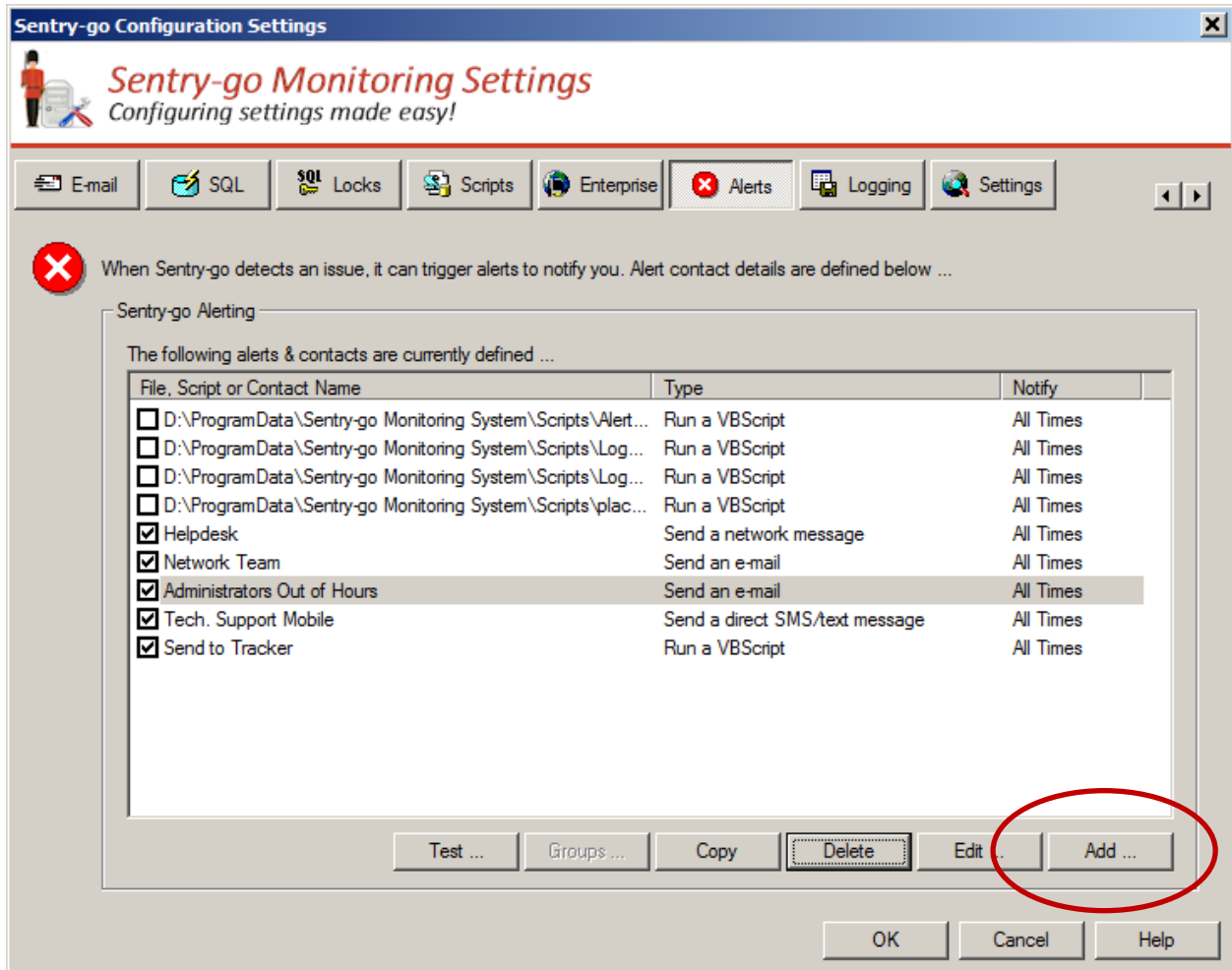
To determine the alerting method, configure the monitor and select the “Settings” tab. On this window you will see a selection indicating which alerting method you wish to use ...



Configuring alerts & contacts

Alerts are triggered in response to the failure of a monitoring check. You can define who to contact or which alert script to run for each check independently, using the “alert” tab or option for the check. This is described in detail later in this guide.

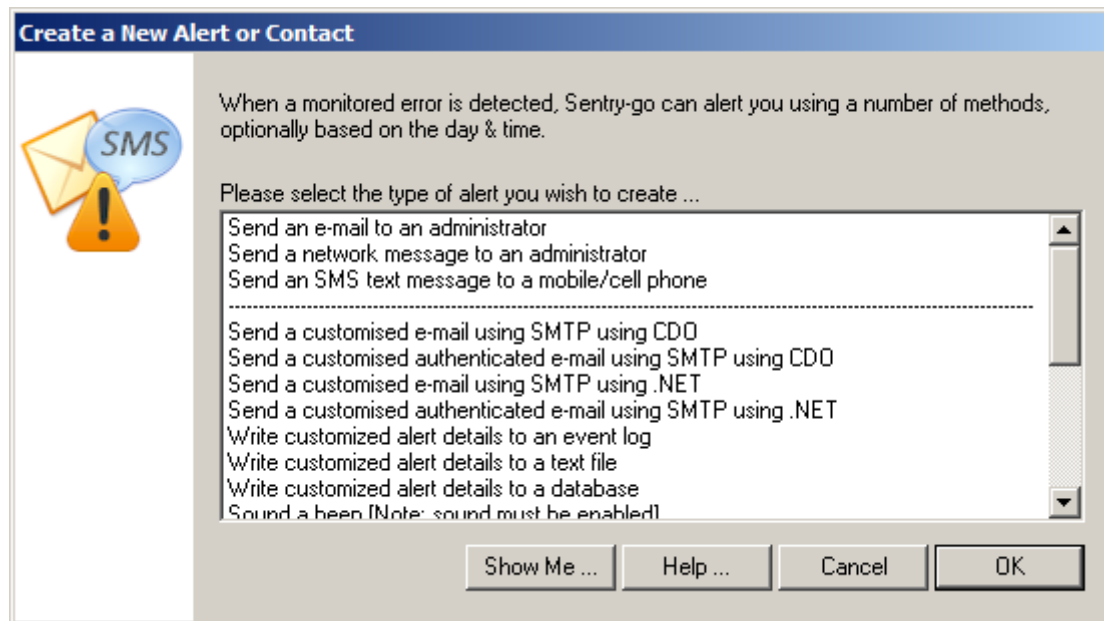
Before you can notify someone or run an alert script, they must first be defined. These are stored on a per monitor basis by configuring the monitor and selecting the “Alerts” option from the button bar ...




You can manage all alert contacts and scripts for the selected monitor from here, as well as add new alerts. To do this, click “Add”.

Creating a new alert contact

When you click "Add", the following window will be displayed, allowing you to choose which type of alert you wish to create. Simply select the option from the list and click OK ...



 Some options may only be available if you are configuring the monitor locally on the server itself.

Some options define the alert directly, while others call a script to perform the action as required. The primary options are described in the following sections.

Alerting via E-mail

E-mails are a very popular and accessible way of notifying the administrator or contact that a failure has occurred. To create an e-mail contact, select the appropriate option from the “Create a New Alert or Contact” list above to display this window ...

Add/Edit Alert

Notify Administrator | Message Text | When to Notify

When an alert is triggered, the monitor will notify you by e-mail using these settings ...

Refer to this contact as :

Send an e-mail to this address :

Send config/system messages to this user

Send a daily summary report to this user

Connect using dial-up before sending e-mail

E-mail Server (SMTP) Name : port :

Send e-mail from :

Using : Standard, non-auth SMTP

SMTP User : Password :

Auto Detect Available Options ...

Notify this user when this alert level(s) is triggered :

Test ... Clear Select All

OK Cancel Help

From here ...

- Enter a friendly name or description for the contact.
- Enter the user's e-mail address. The alert notification will be sent to this address.
 - The address given should be fully qualified with the full domain name and must be accessible (or reachable) from the SMTP server specified below.
- If you wish this user to receive system notifications (errors relating to the configuration or setup of the Sentry-go monitor itself), tick the “Send config/system messages to this user” option.
- If you wish this user to receive a daily summary e-mail, outlining all recent activity that day, tick the “Send a daily summary” option.
 - Alert Summaries are always sent by e-mail shortly after midnight.

- Tick the “Connect using dialup” option if Sentry-go needs to connect to the network by invoking dial-up networking before the message can be sent.

For more information, please see “Sentry-go Dial-up Networking”.

- Enter the name or IP address of the SMTP server used to send e-mails from your organisation. This will typically be the same as the server used by your e-mail client such as Microsoft Outlook. If you are unsure, please contact your network administrator.
- Enter the port number on which the above SMTP listens for requests. Typically SMTP uses port 25.
- Enter the e-mail address of the user who will send the mail. This is typically in the format <Someone>@<YourDomain> as the server may check the originating domain before proceeding.
- Next select the type of SMTP message you want to send.

Sentry-go allows you to send e-mails using a number of methods, depending on how your server/organisation is configured.

If you know which one to use – it will normally be the same as used by your e-mail client, please select it. such as Microsoft Outlook. If not, click “Auto Detect Available Option” to have the server determine which options will work.

- **Standard, non-auth SMTP.**

Select this option if you do not need to logon to your SMTP server in order to send e-mail.

- **Auth, Secure SMTP (Windows 2000/ CDO only).**

Select this option if you wish to send an e-mail using authenticated & secure (SSL) SMTP using the Microsoft CDO library. Typically this is used on older servers such as Windows 2000.



To use this option, Microsoft Collaborative Data Objects (CDO) must be installed on the monitoring server.

- **Auth, Secure SMTP**

Select this option if you wish to send an e-mail using authenticated & secure (SSL) SMTP on newer Windows servers.

- **Auth, Non-Secure SMTP**

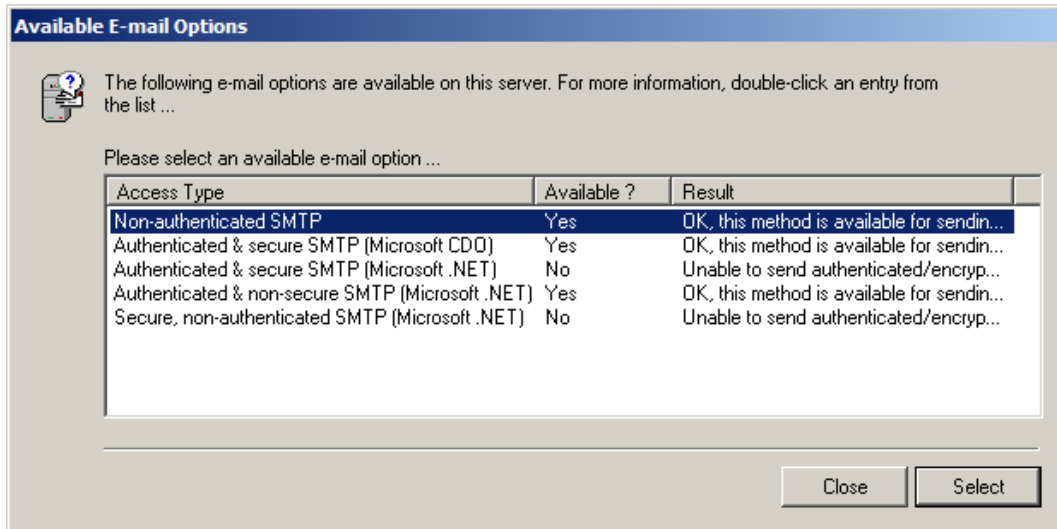
Select this option if you wish to send an e-mail using authenticated but non secure SMTP on newer Windows servers.



Use this option to use when your e-mail (SMTP) server doesn't support secure connections but still requires authentication (user/password logon).


- **Auto Detect Available Options ...**

When you click this button, the Configuration Utility connects to the monitor, sending it the details entered on this window. It then uses these details to determine which e-mail options are available to you – displaying the results in a window similar to this ...



From here you can view the results & see which e-mail options are available to you, based on the settings entered. You can also select the entry you wish to use.

- Enter the user ID that can logon to your SMTP server.
- Enter the password for the above user.
- If you are using alert groups, select the group(s) for which this user should be notified. If an alert is triggered belonging to one of these groups, the user here will be notified.

 For direct alerts, this option is not used.

Alert Text

By default, when the contact is created, a default title & message text, containing details of the server & alert triggered will be defined. To view or override this, select the "Message Text" tab.

See "Specifying message text" for more information.


Alert Schedule

By default, when enabled, the notification will be active regardless of the time of day the alert is triggered. However, you can specify when the notification is to be run and when it isn't by selecting the "When to Notify" tab.

See "Notifying based on schedule" for more information.

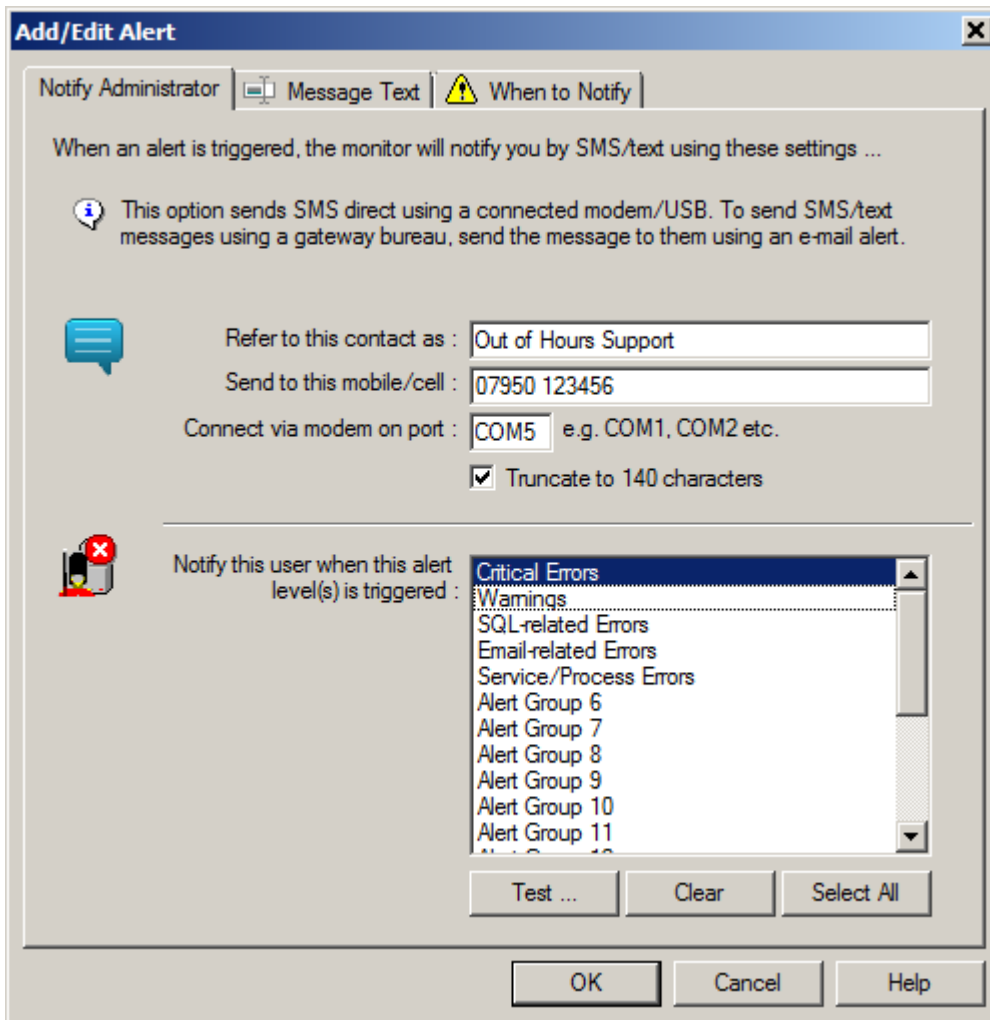
Alerting via SMS/text message

Another popular and more “immediate” method is the SMS or text message to a mobile or cell phone. Sentry-go can notify by SMS either directly using a connected GSM/USB modem, or indirectly via a gateway bureau.

-  To send an SMS using a gateway bureau, you can typically send the details via e-mail. To do this from Sentry-go, simply configure the appropriate alert type – e.g. e-mail.


To configure direct SMS contacts using a connected modem, please follow the steps below.

To create an SMS alert, select the appropriate option from the “Create a New Alert or Contact” list above to display this window ...




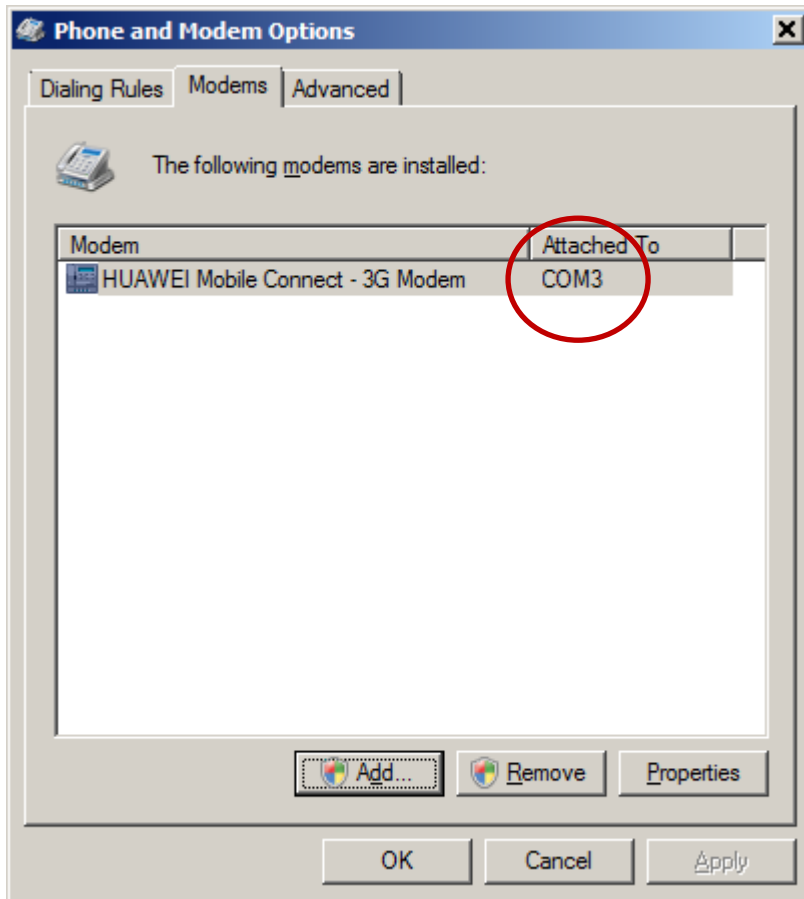
From here ...

- Enter a friendly name or description for the contact.
- Enter the user’s mobile/cell phone number.

-  The number should be in the format typically used within the country. Typically you should not need to include the international dialling code.

- Next, enter the name of the port that the modem is connected to. This will typically be the same for all similar alerts – e.g. COM1, COM2 etc.


 To determine the port number being used, contact your system administrator. Alternatively, access Control Panel/Phone and Modem Options or Windows Device Manager.



- Individual SMS messages are limited to 140 characters, although they can be chained together as required. However, because most SMS messages incur a small charge by the network carrier, you may wish to ensure only a single message is sent per alert.

To do this, tick the “Truncate to 140 characters” option.

- If you are using alert groups, select the group(s) for which this user should be notified. If an alert is triggered belonging to one of these groups, the user here will be notified.

 For direct alerts, this option is not used.

Alert Text

By default, when the contact is created, a default title & message text, containing details of the server & alert triggered will be defined. To view or override this, select the “Message Text” tab.

See “Specifying message text” for more information.

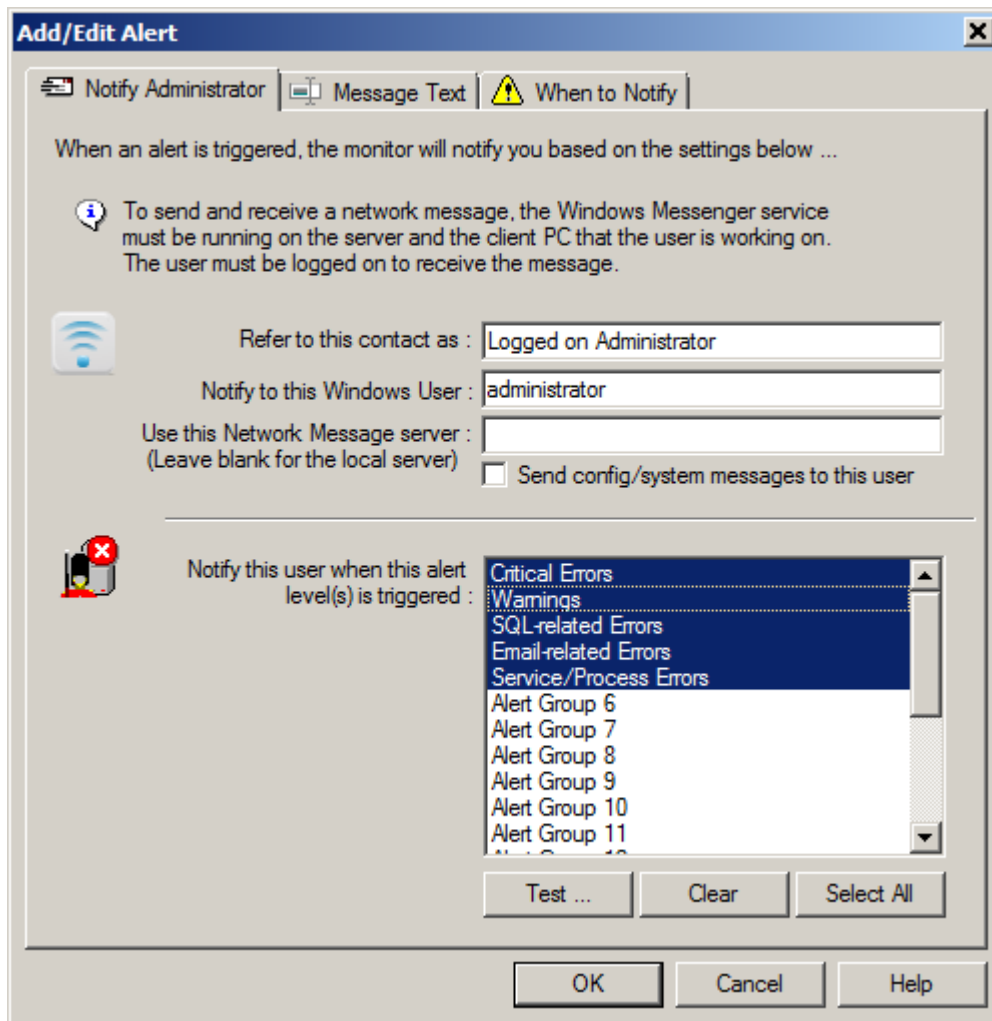
Alert Schedule

By default, when enabled, the notification will be active regardless of the time of day the alert is triggered. However, you can specify when the notification is to be run and when it isn't by selecting the “When to Notify” tab.

See “Notifying based on schedule” for more information.

Alerting via network message


Network messages allow an extremely fast way of notifying an administrator when they are logged on to the domain. To create an SMS alert, select the appropriate option from the “Create a New Alert or Contact” list above to display this window ...



The screenshot shows the 'Add/Edit Alert' dialog box with the 'Message Text' tab selected. The dialog has three tabs: 'Notify Administrator', 'Message Text', and 'When to Notify'. Below the tabs, there is a heading: 'When an alert is triggered, the monitor will notify you based on the settings below ...'. An information icon (i) is followed by the text: 'To send and receive a network message, the Windows Messenger service must be running on the server and the client PC that the user is working on. The user must be logged on to receive the message.' Below this, there is a wireless network icon. The 'Refer to this contact as :' field contains 'Logged on Administrator'. The 'Notify to this Windows User :' field contains 'administrator'. The 'Use this Network Message server :' field is empty, with the note '(Leave blank for the local server)'. There is an unchecked checkbox for 'Send config/system messages to this user'. Below this, there is a list of alert groups to notify the user when triggered. The list includes 'Critical Errors', 'Warnings', 'SQL-related Errors', 'Email-related Errors', 'Service/Process Errors', and 'Alert Group 6' through 'Alert Group 11'. At the bottom of the dialog are buttons for 'Test ...', 'Clear', 'Select All', 'OK', 'Cancel', and 'Help'.

From here ...

- Enter a name or description for the contact.
- Enter the Windows User ID of the user you wish to contact.
- Optionally enter the name or IP address of the SMTP server used to send e-mails from your organisation. By default this field is blank, meaning the local server will be used.
- If you wish this user to receive system notifications (errors relating to the configuration or setup of the Sentrygo monitor itself), tick the “Send config/system messages to this user” option.
- If you are using alert groups, select the group(s) for which this user should be notified. If an alert is triggered belonging to one of these groups, the user here will be notified.

 For direct alerts, this option is not used.

Alert Text

By default, when the contact is created, a default title & message text, containing details of the server & alert triggered will be defined. To view or override this, select the “Message Text” tab.

See “Specifying message text” for more information.

Alert Schedule

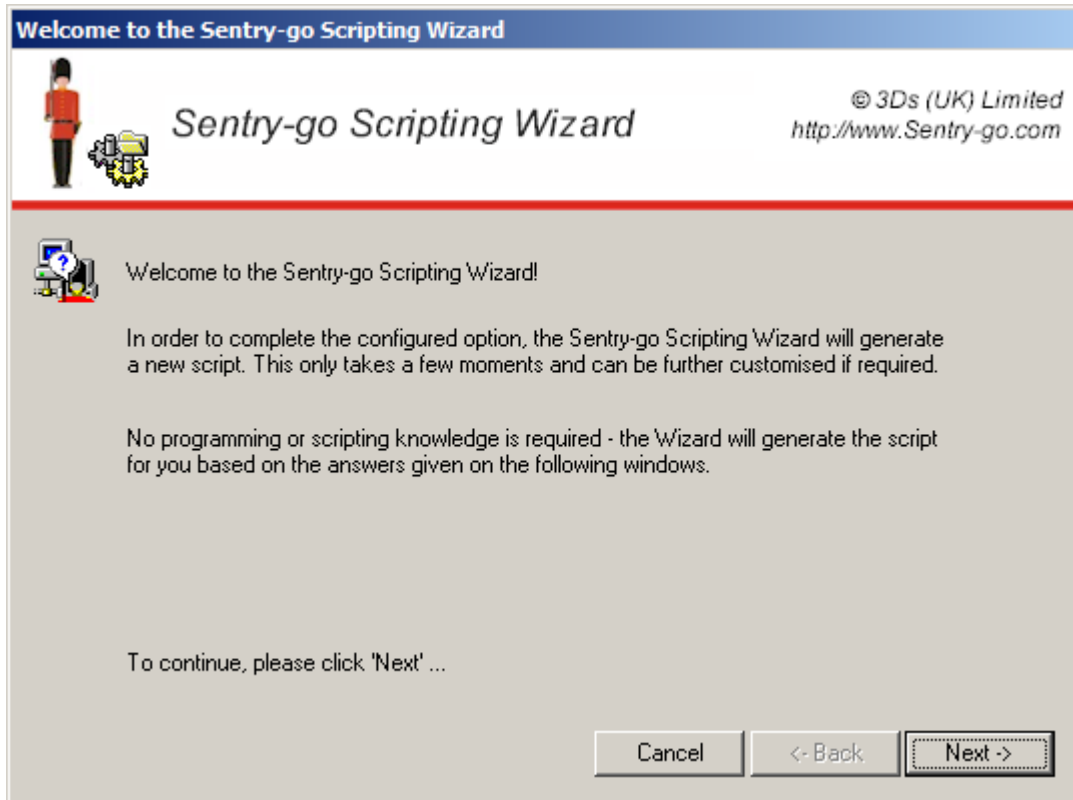
By default, when enabled, the notification will be active regardless of the time of day the alert is triggered. However, you can specify when the notification is to be run and when it isn't by selecting the “When to Notify” tab.

See “Notifying based on schedule” for more information.

Alerting using an “implicit” script

“Implicit” scripts are selectable alerts that actually cause a script to be generated to perform the required functions. The Sentry-go Scripting Wizard is automatically invoked in this case, allowing the file to be generated without the need for coding or script knowledge.

These alerts are created in the same way as before. Simply select the appropriate option from the “Create a New Alert or Contact” list above and if it results in an implicit script, the following window will be displayed ...

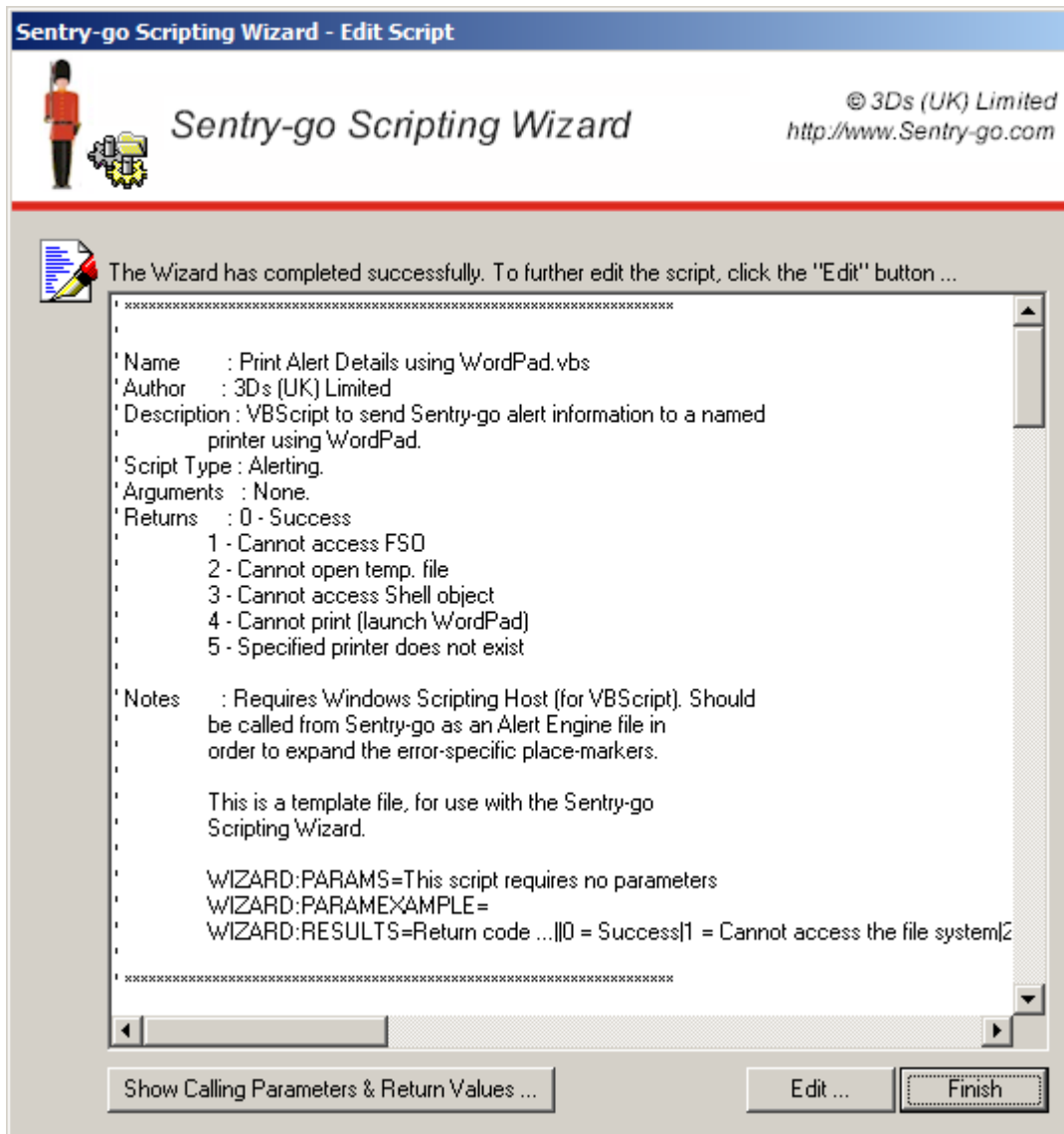


From here ...

- Follow the on-screen prompts, which are dependent on the option selected and therefore the script being generated.

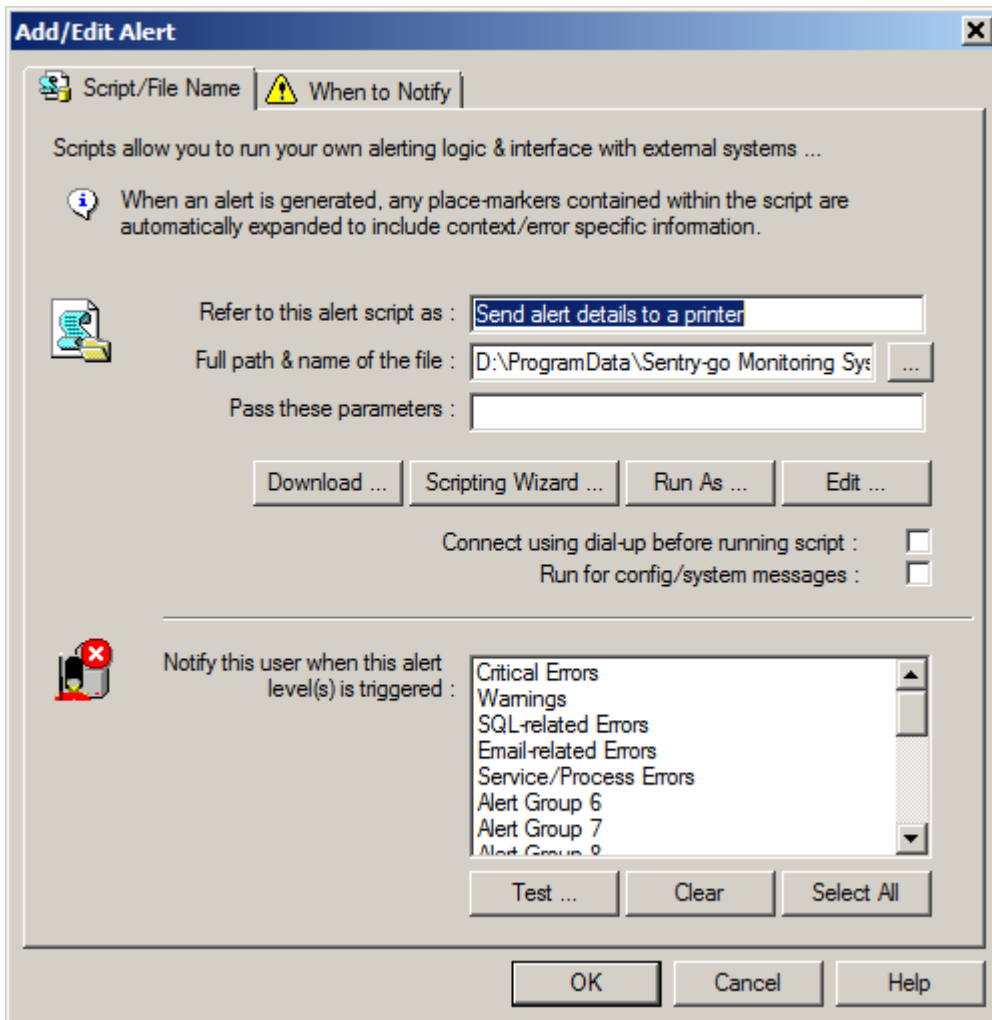
For more information on using the scripting wizard, see “Using the Sentry-go Scripting Wizard”.

- Once complete, the script will be generated & displayed to you. You can review & edit this if required, or further enhance it as required, or leave it “as is”.



- Click “Show Calling Parameters & Return Values” if available to view information on how the script is called etc.
- Finally, click finish to continue.

- Once complete, the generated filename will be pre-filled and the alert type changed to “VBScript”.




- If required, enter any parameters that are required by the file or script, otherwise leave the next field blank.
- By default the file or script will be run as the user running the monitor. To override this, for example, to use a domain account with permissions to access remote resources or specific software referenced by the script, click the “Run As” button and enter the appropriate details.

For more information, see “Running File or Script as Named User”.

- Tick the “Connect using dialup” option if Sentry-go needs to connect to the network by invoking dial-up networking before the message can be sent.

For more information, see “Sentry-go Dial-up Networking”.

- Tick the “Run for config/system messages” option if the defined file or script should be run for system notifications - errors relating to the configuration or setup of Sentry-go itself. For example, if web publishing errors occur, details of the fault will be sent to the user if this option is enabled.
- If you are using alert groups, select the group(s) for which this script should be run. If an alert is triggered belonging to one of these groups, the user here will be notified.

 For direct alerts, this option is not used.

Alert Text

For script-based logic, you can easily set up your own message text, incorporating the appropriate place-markers (such as <\$\$ERROR> and <\$\$SERVER> as required.

See “Sentry-go Place-markers” for more information.

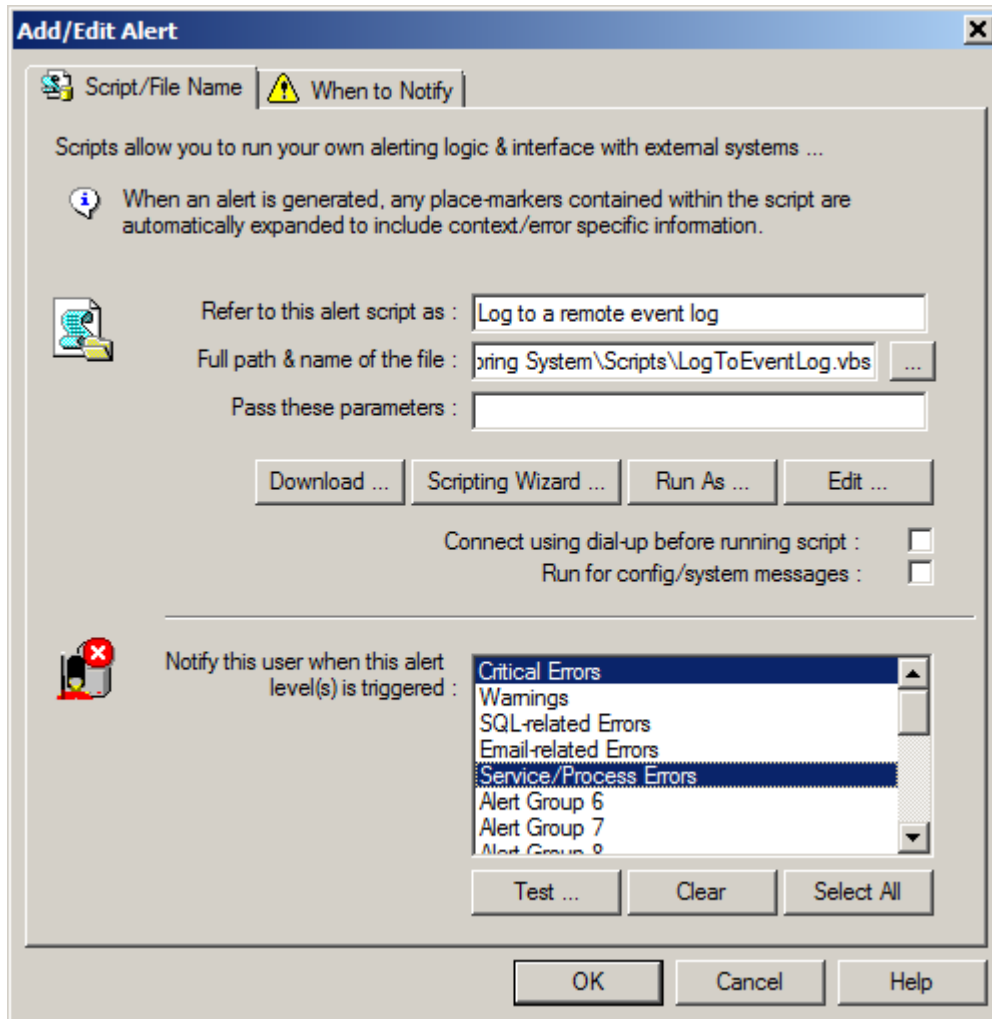
Alert Schedule

By default, when enabled, the notification will be active regardless of the time of day the alert is triggered. However, you can specify when the notification is to be run and when it isn't by selecting the “When to Notify” tab.

See “Notifying based on schedule” for more information.

Alerting using a custom script, command, batch file or 3rd party application

There may also be times when you wish to call a specific script or file – either one you have created or in order to invoke a 3rd party application. Once again, simply select the appropriate option from the “Create a New Alert or Contact” list above to display the following window



From here ...

- Enter a friendly name or description for the job or script.
- Enter the full path & name of the command, file or script to run, depending on the alert type selected ...
 - When editing an existing file, this will be the full path & name to that file on the server being monitored. If you're configuring the local server, you can click the "Edit ..." button to edit the file
 - When defining a new file, simply enter the full path and name of the file, relative to the local server. If you're configuring the local server, you can click the "Edit ..." button to create & then edit the file. For preformatted files, a template will be provided, allowing you to quickly & easily supply your own information.

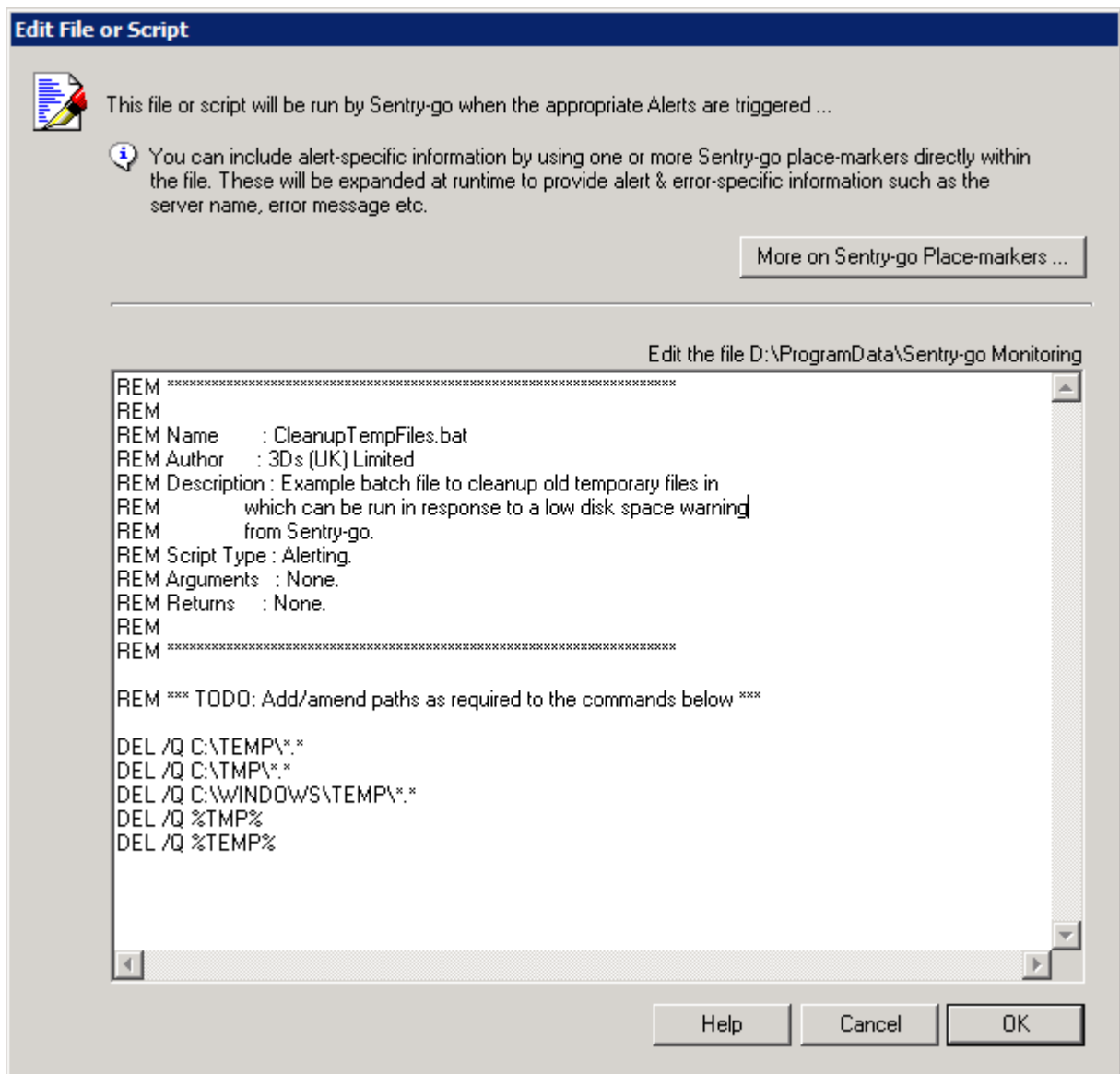
- Optionally enter any parameters that are required by the file or script, otherwise leave the next field blank.
- Click the “Download” button to access the on-line Sentry-go Scripting Library. From here you can download files & scripts as well as templates for use with the Scripting Wizard.

The scripting library is also available on-line at <http://www.Sentry-go.com/sentry-go-scripting-library.aspx>.

- Click the “Scripting Wizard” button to run the Sentry-go Scripting Wizard. This allows you to use predefined templates to generate VBScripts for you.

For more information on using the scripting wizard, see “Using the Sentry-go Scripting Wizard”.

- Click the “Edit” button to edit a local file or script ...



- If no file is found, you will be offered to copy a default template, depending on the type of notification being defined. You can use this as the basis of your own script.

For more information on place-markers, see “Sentry-go Place-markers”. For more information on using the scripting wizard, see “Using the Sentry-go Scripting Wizard”.

- By default the file or script will be run as the user running the monitor. To override this, for example, to use a domain account with permissions to access remote resources or specific software referenced by the script, click the “Run As ...” button and enter the appropriate details.

For more information, see “Running File or Script as Named User”.

- Tick the “Connect using dialup” option if Sentry-go needs to connect to the network by invoking dial-up networking before the message can be sent.

For more information, please see “Sentry-go Dial-up Networking”.

- Tick the “Run for config/system messages” option if the defined file or script should be run for system notifications - errors relating to the configuration or setup of Sentry-go itself. For example, if web publishing errors occur, details of the fault will be sent to the user if this option is enabled.
- If you are using alert groups, select the group(s) for which this script should be run. If an alert is triggered belonging to one of these groups, the user here will be notified.



For direct alerts, this option is not used.

Alert Text

For script-based logic, you can easily set up your own message text, incorporating the appropriate place-markers (such as <\$\$ERROR> and <\$\$SERVER> as required.

See “Sentry-go Place-markers” for more information.

Alert Schedule

By default, when enabled, the notification will be active regardless of the time of day the alert is triggered. However, you can specify when the notification is to be run and when it isn't by selecting the “When to Notify” tab.

See “Notifying based on schedule” for more information.

Example batch file or script

Batch file or scripts are standard text files run through the appropriate interpreter. In this example, a short VBScript is used to export alert information to an in-house system, through an external utility called LogInfo.exe. In particular, it shows how to include the strings "<\$\$ERROR>" and "<\$\$SERVER>" which are then expanded at runtime by the Alert Engine to include the actual error message and server name prior to running the script. Batch files are similar, except that standard Windows commands & external command-line utilities are used in place of script-based commands.

```
'
' Sentry-go Alert Engine Script to log alert information
' via an external LogInfo.exe routine.
'
' See associated documentation for more details on how to
' specify the information to send via this file.
'
' ----- Local declarations -----
Dim strTextToSend

' ----- Set up parameters -----
strTextToSend = "Error - < $$ERROR> on <$$SERVER>"
Set Shell = CreateObject("WScript.Shell")

' ----- Create & execute the target command -----
Shell.Run ""c:\program files\Inhouse\LogInfo.exe"" "" & strTextToSend &
""",,True

' ----- Cleanup -----
Set Shell = Nothing

' ----- End of Script -----
```

Example script for recording to a SysLog file

When the alert file is defined as a SysLog file, the preformatted commands are used to interface with an external SysLog server. The following commands, which are generally used in the format <Command>:<Value> should be included in this type of file ...

Command	Meaning
#	Any commands or lines prefixed with a # are counted as comments by the Alert Engine and ignored. Blank lines are also ignored.
AE-SERVER: <TargetServer>	Required. This command is used to identify the target SysLog server - either by name or IP address.
AE-PORT: <Port No>	Required. This is the port number on which the server is listening for inbound HTTP requests. Unless otherwise stated by your provider, this is normally 514.
AE-SYSLOGSEVERITY: <Lvl>	Optional. Indicates which SysLog severity you wish to log the alert under. If not specified, the default severity level is 1 (alert).
AE-SYSLOGFACILITY: <Lvl>	Optional. Indicates which SysLog facility you wish to log the alert under. If not specified, the default facility is 14 (alert message).
<Alert Text>	The last parameter (with no command prefix) is the alert you wish to log. It can span multiple lines, but will be truncated if the length exceeds the maximum size allowed by the SysLog standard.

Example

```
#
# SysLog Alert File
#
# This file allows you to send alert details to a SysLog server.
# Simply edit the appropriate details below and configure the Alert
# Engine to call this file for the appropriate alert levels. Any
# place markers found (e.g. <$$ERROR>) will automatically be expanded
# by the Alert Engine at runtime.
#
AE-SERVER: MySysLogServer
AE-PORT: 514
AE-SYSLOGSEVERITY: 1
AE-SYSLOGFACILITY: 1

# The following (last) entry is the message we want to log. This
# will be expanded to contain the actual error/alert information
# at runtime.

The error <$$ERROR> occurred on server <$$SERVER> at <$$TIMELOGGED>
```

Example SMS script for gateway bureau, using e-mail

When the alert file is defined as an SMTP file, the preformatted commands are used to interface with an external SMTP server. For example, you can use these to send a custom e-mail or to interface with an external system such as an SMS gateway. The following commands, which are generally used in the format <Command>:<Value> should be included in this type of file ...

Command	Meaning
#	Any commands or lines prefixed with a # are counted as comments by the Alert Engine and ignored. Blank lines are also ignored.
AE-SERVER: <TargetServer>	Required. This command is used to identify the target SMTP (e-mail) server - either by name or IP address.
AE-PORT: <Port No>	Optional. This is the port number on which the SMTP server is listening for inbound requests. Unless otherwise stated by your provider or Administrator, this is normally 25.
AE-SENDFROM: <User>@<YourDomain>	Required. This is the e-mail address of the user sending the mail. In general, this should be in the format <Someone>@<YourDomain> as the server may check the originating domain before proceeding..
AE-SENDTO: <User>@<Domain>, <User>@<Domain>, <User>@<Domain> etc.	Required. This is the e-mail address of one or more users that should receive the mail. Separate multiple entries with a comma.
AE-SUBJECT: <Title>	Required. This is the string that will form the subject for the e-mail. It can contain any valid text or place markers.
<Alert Text>	The last parameter (with no command prefix) is the alert you wish to log. It can span multiple lines and contain one or more place markers.

Example

```
#
# SMTP Alert File
#
# This file allows you to send alert details to an SMTP server.
# Simply edit the appropriate details below and configure the Alert
# Engine to call this file for the appropriate alert levels. Any
# place markers found (e.g. <$$ERROR>) will automatically be expanded
# by the Alert Engine at runtime.
#
AE-SERVER: MySMTPServer
AE-SENDFROM: Sentry-go@Company.com
AE-SENDTO: Support@Company.com, SMS@Provider.com
AE-SUBJECT: Critical Error Detected!

# The following (last) entry is the message we want to log. This
# will be expanded to contain the actual error/alert information
# at runtime.

The error <$$ERROR> occurred on server <$$SERVER> at <$$TIMELOGGED>
```


Example SMS script for gateway bureau, using http (web)

When the alert file is defined as an HTTP file, the preformatted commands are used to interface with an external web (HTTP) server (and optionally on to an external system such as an SMS gateway). The following commands, which are generally used in the format <Command>:<Value> should be included in this type of file ...

Command	Meaning
#	Any commands or lines prefixed with a # are counted as comments by the Alert Engine and ignored. Blank lines are also ignored.
AE-HTTPSERVER: <TargetServer>	Required. Indicates the name or IP address of the target web/HTTP server. This name is dependent on your provider .
AE-PORT: <Port No.>	This is the port number on which the server is listening for inbound HTTP requests. Unless otherwise stated by your provider, this is normally 80.
AE-METHOD: GET	Required. Indicates which HTTP call type the Alert Engine should use. Currently, this must be set to GET - indicating that an HTTP Get request is to be performed. This may be extended in a future version of the Alert Engine.
AE-URL: <URL>?<Params>	Required. This is the URL that is to be called in order to make the GET request. It may contain one or more parameters as required. Parameters must be URL encoded - e.g. %20 in place of spaces, no double quotes etc.
AE-SUCCESSTEXT: <Text>	Optional. If included, it indicates some text that the server will return to indicate that the call was successful - e.g. OK. If the text is not returned (or no text is returned), the command will be considered to have failed. <i>If both AE-ERRORTTEXT and AE-SUCCESSTEXT are included and neither string is found, it is assumed that the command failed.</i>
AE-ERRORTTEXT: <Text>	Optional. If included, it indicates some text that the server will return to indicate that the call failed - e.g. Error. If the text is not returned (or no text is returned), the command will be considered to have worked successfully. <i>If both AE-ERRORTTEXT and AE-SUCCESSTEXT are included and neither string is found, it is assumed that the command failed.</i>

Example

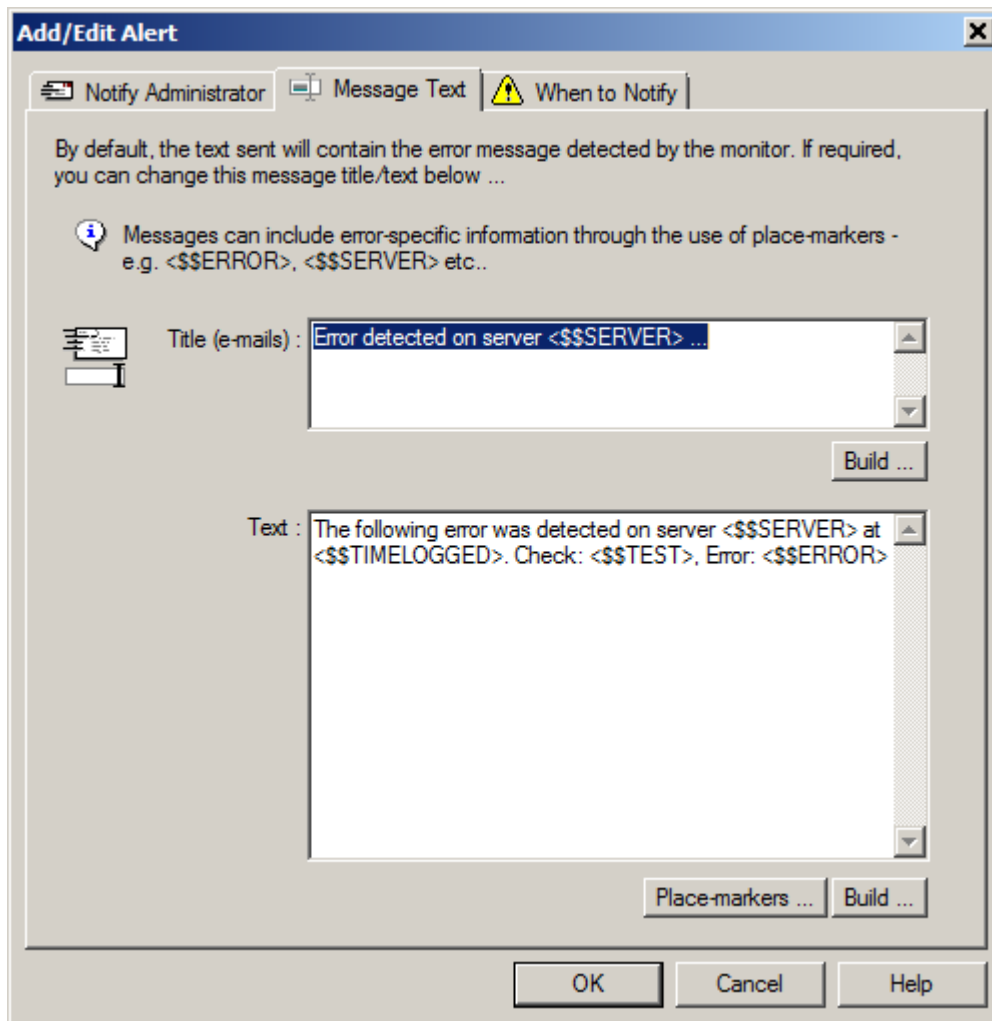
```
#
# HTTP Alert File
#
# This file allows you to send alert details to an HTTP (Web) server.
# Simply edit the appropriate details below and configure the Alert
# Engine to call this file for the appropriate alert levels. Any
# place markers found (e.g. <$$ERROR>) will automatically be expanded
# by the Alert Engine at runtime.
#
AE-HTTPServer: www.YourProvidersSite.com
AE-Port: 80
AE-METHOD: GET

# The following should appear on a single line
AE-URL: http://www.YourProvider.com/TheirPage.htm?
      Param1=Value&Text=<$$ERROR>%20on%20server%20<$$SERVER>

AE-SuccessText: OK
AE-ErrorText: ERR
```

Specifying message text

By default, when an e-mail, SMS or network message contact is created, a default title & message text, containing details of the server & alert triggered will be defined for you. To view or change this, display the select the “Message Text” tab.



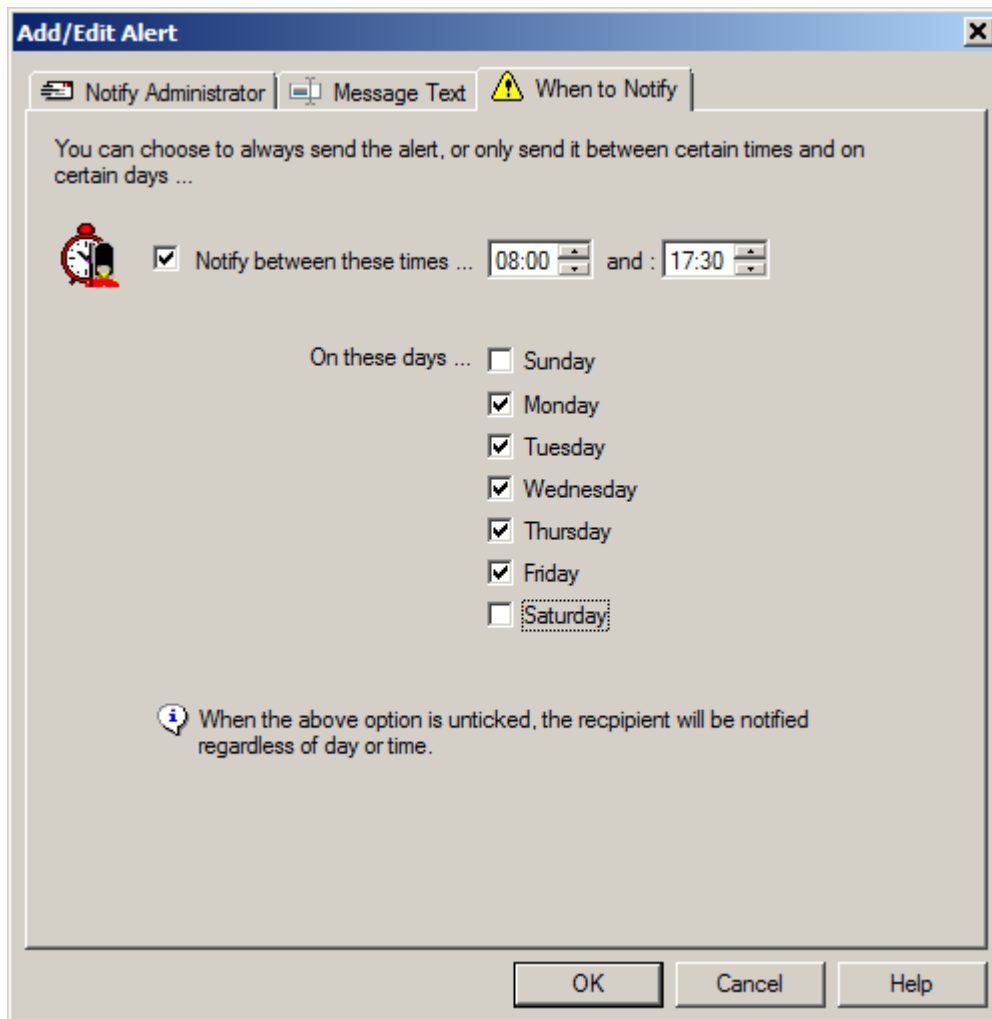
The above screenshot shows the default title & message text. The <\$\$SERVER> and <\$\$ERROR> are examples of special place-markers which are expanded by the monitor to include context-specific information when the alert is triggered.

To help build the message text, click the appropriate “Build ...” button.

For more information on the place-markers and message builder options available, see “Sentry-go Place-markers”.

Notifying based on schedule

By default, when an alert is created, the notification will be active regardless of the time of day the alert is triggered by the monitor. However, there may be times, when certain methods or scripts should only be run during certain hours or on certain days. To specify a specific timetable for a contact or script, display its properties and click the “When to Notify” tab.



The screenshot shows a dialog box titled "Add/Edit Alert" with three tabs: "Notify Administrator", "Message Text", and "When to Notify". The "When to Notify" tab is active. The dialog contains the following elements:

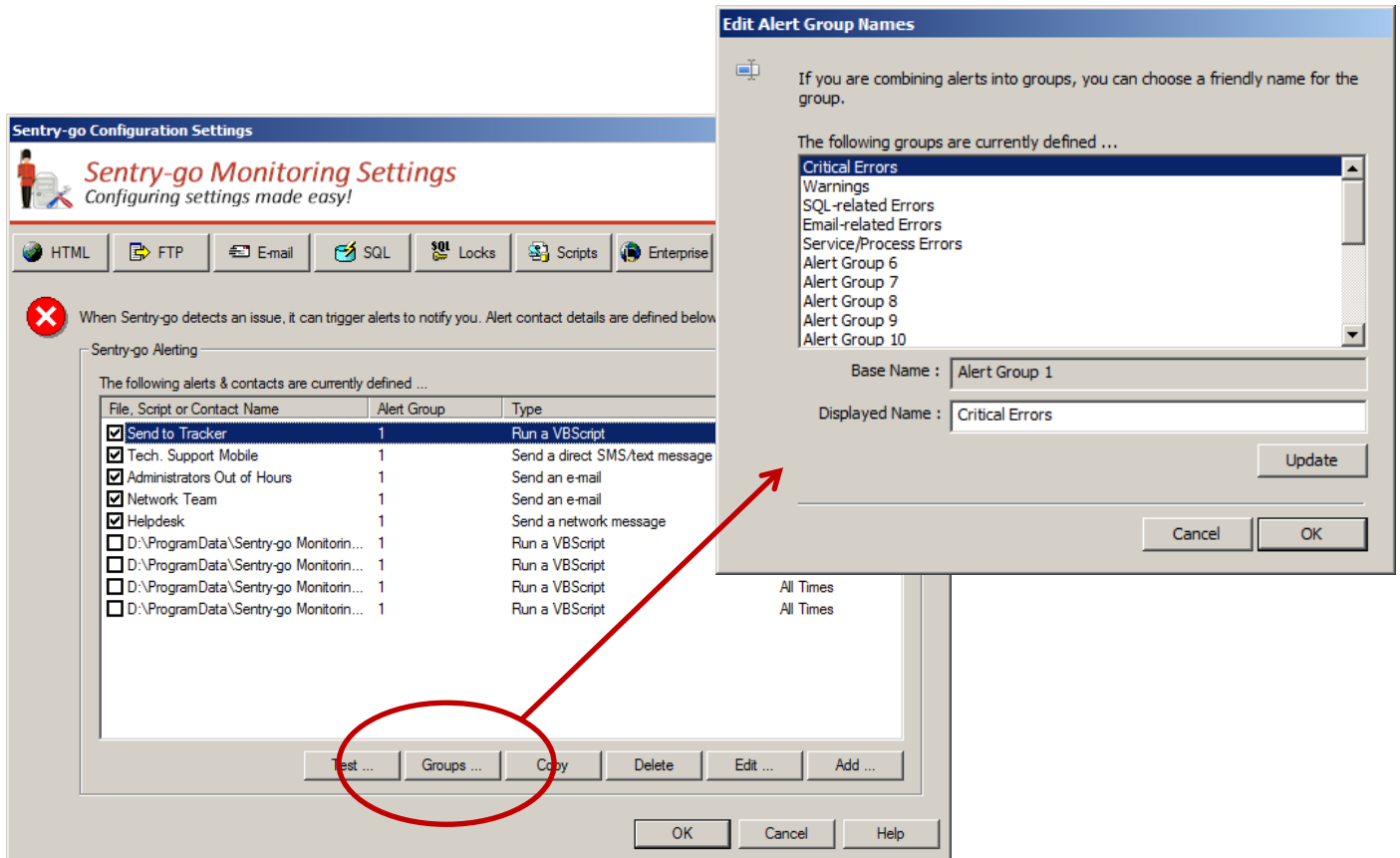
- Text: "You can choose to always send the alert, or only send it between certain times and on certain days ..."
- Checkbox: "Notify between these times ..."
- Time pickers: "08:00" and "17:30" with up/down arrows.
- Text: "On these days ..."
- Day checkboxes:
 - Sunday
 - Monday
 - Tuesday
 - Wednesday
 - Thursday
 - Friday
 - Saturday
- Information icon and text: "When the above option is unticked, the recipient will be notified regardless of day or time."
- Buttons: "OK", "Cancel", and "Help".

This page lets you determine when the contact will be notified or the alert script run.

Configuring alert groups (if alert groups are being used)

Alert groups, if used, are defined centrally within the monitor. Up to 20 groups can be defined and named as appropriate to your needs. Once an alert group is defined, one or more contacts/alert scripts can be allocated to it.

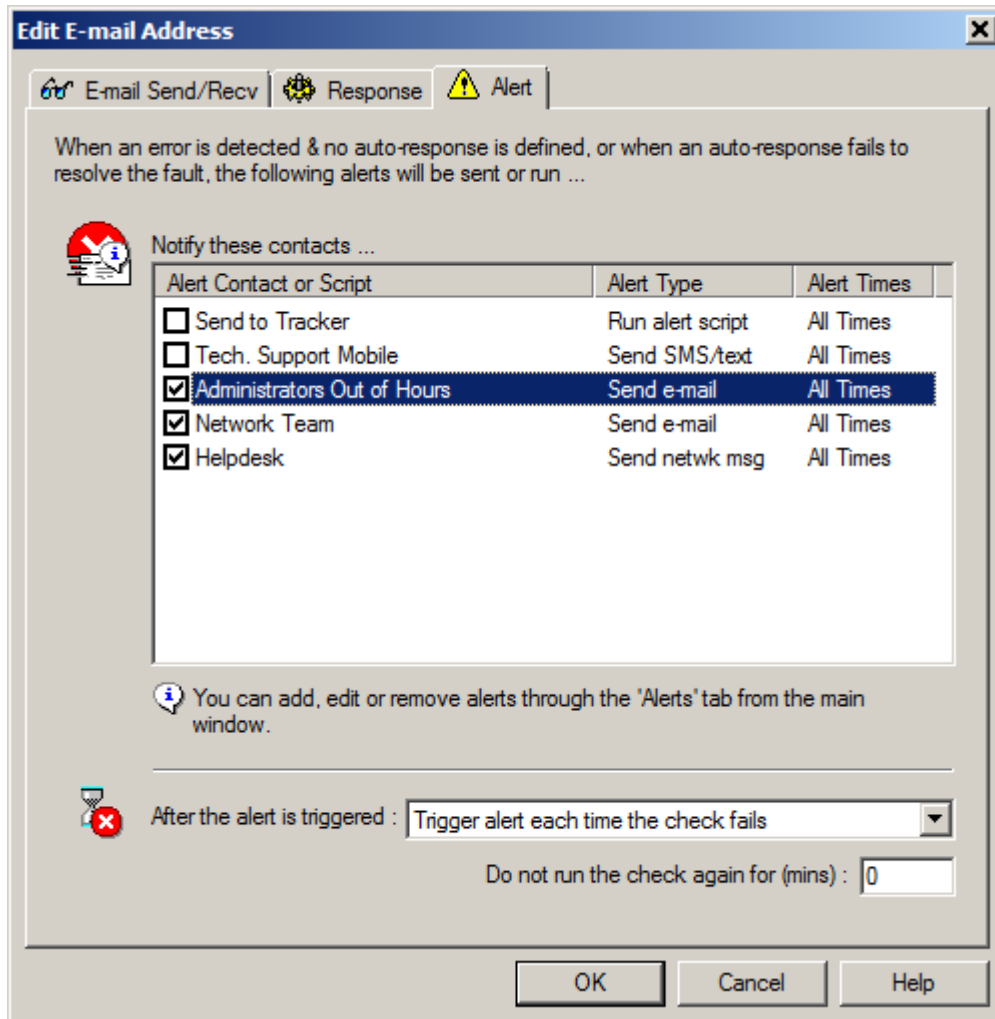
To setup & name the alert groups themselves, configure the monitor and select the “Alert” option from the button bar. From here, click the “Groups” button ...



From here you can list & configure the group names. Internally, the monitor numbers groups from 1 to 20 – the “base name”. However, they can also be given a more friendly name, thus making it easier to see which group should be informed of an error, should an alert be triggered.

Triggering an alert from a check using direct alerts

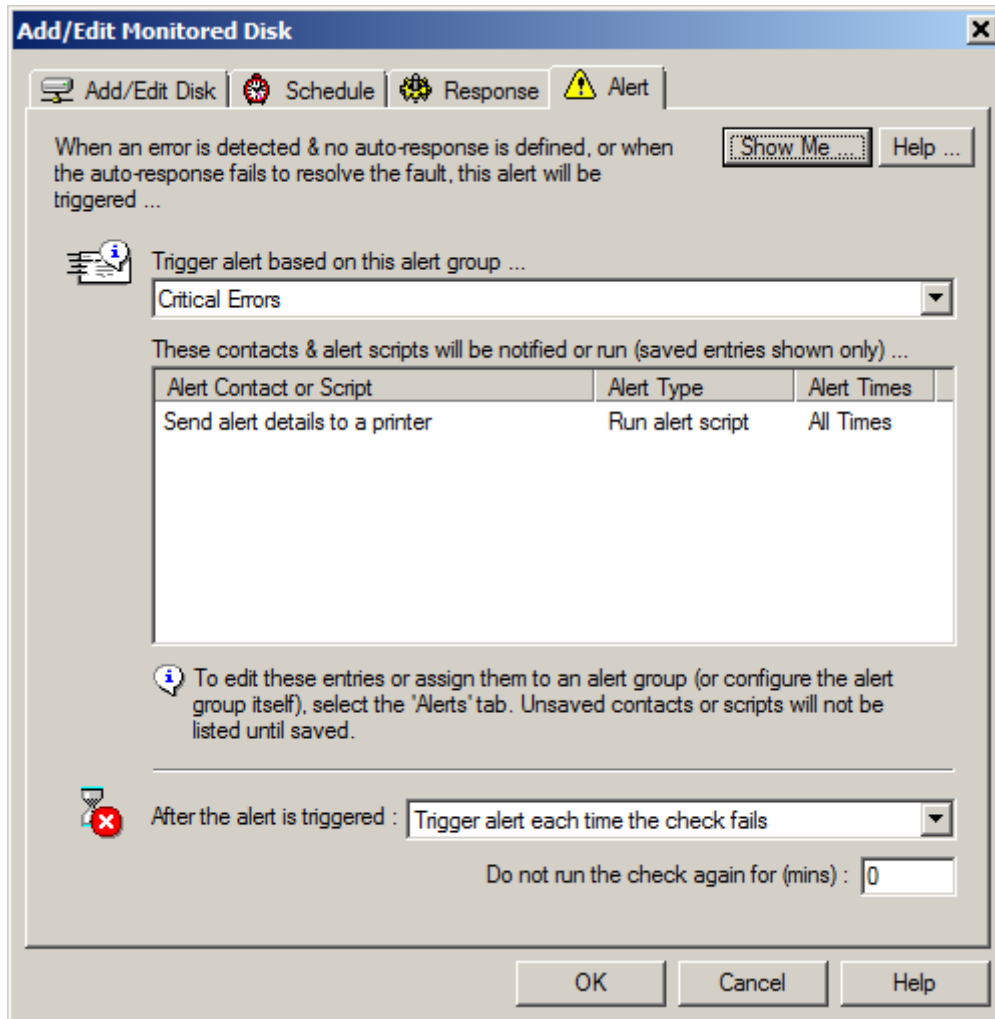
To determine who will be notified or which alert scripts will be run for a check, either click the “alerting” button from the main list, or edit a check, display its properties and click the “Alert” tab ...



This window will list all active contacts shown in the main alert list. To notify a contact or run a script, simply tick the appropriate entry in this list. Tick all that apply.

Triggering an alert from a check using alert groups

To determine who will be notified or which alert scripts will be run for a check, either click the “alerting” button from the main list, or edit a check, display its properties and click the “Alert” tab ...



At the top of this window, you'll see a dropdown list of alert groups. Simply select the group you wish to notify. All members & scripts associated with this group will be notified – and displayed in the list below.

Preventing repeated alerts with ACM

When an alert is triggered, it often indicates that further investigation and possible correction is required. To do this may take some time and lead to an element of delay, during which the alert could well be repeated if the monitoring intervals are regular and short. To prevent this, you can additionally invoke the Alert Control Mechanism or “ACM”. This allows the monitor to approach alerts more intelligently, in a number of ways.

Do not run the check again for (mins)

This option allows you to set a fixed time within which the monitor will not re-run the check following a previous failure. This gives the administrator time to resolve the fault without repeated alerts being triggered.

After the alert is triggered

This option invokes the ACM and lets the monitor determine when to repeat the check following a failure.

- **Trigger an alert each time the check fails**

By default any failure will result in the associated alert being triggered. If a previously alerted fault has not yet been fixed, a subsequent alert will be triggered, repeatedly until resolved.

- **Do not trigger alert again until resolved**

In this mode, the monitor notes the failure and continues monitoring at the prescribed interval. However, it will only trigger an alert again after its run the check successfully at least once. In other words, the failure must have been previously fixed – and noted as being fixed, before alerts are reset.

This automatically gives the administrator time to resolve the fault before alerts are triggered again for the check.

- **Do not trigger until resolved & notify when successful**

This is similar to the last option, with the exception that contacts are additionally notified when the monitor detects that the fault has been resolved.

This option gives you total control; being given time to resolve the fault and ensuring it has in fact been resolved such that the monitored check is now successful.

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>*