FORTRA

Enterprise Console 11.4

User Guide

Copyright Terms and Conditions

202402070153

Table of Contents

Enterprise Console

Introduction

Halcyon Enterprise Console is a highly configurable, real-time focal point for managing cross-platform systems and security alerts centrally.

The Enterprise Console displays system and security related alerts from IBM i, Windows, Linux, AIX and UNIX servers as well as SNMP devices. Once the alerts have been received the user has the ability, via the console, to automate and escalate actions in order to respond.

Color-coded options help identify different servers and/or different types of alert.

Multiple instances of the Enterprise Console can be run simultaneously meaning that each remote location in an organization has visibility of the current operational status.

The Enterprise Console allows users to add comments and provides the ability to centrally manage alerts from all your managed systems.

Any number of users can be connected simultaneously, although each must have a unique user name. Individual user privileges can be set to restrict or enable operators to perform different tasks.

If several users are on duty and one person closes or replies to an alert, their action is broadcast to all other users.

The Enterprise Console is displayed in View mode. To amend the current layout, use Edit Mode.

Components

Enterprise Server

This is a service used to receive alerts from a variety of sources and allows users to manage them centrally via any networked machines which have the Enterprise Console application installed. Any number of incoming connections can be handled simultaneously; the only limitations are imposed by machine hardware capabilities (processor speed, memory, and so on).

Enterprise Server Options

This application is used to specify, edit and change Enterprise Server settings.

Enterprise Server Options is used to:

- Specify user access rights
- Set up rules and actions for incoming alerts
- Set up alerts display information
- Specify Ping and Connection Monitor settings
- Specify Syslog Monitor settings
- License Enterprise Server
- Specify default email / SMS settings
- Specify default helpdesk settings
- View system informational and diagnostic messages
- View and reset SQL Server settings

Enterprise Console

This is the application that connects to the Enterprise Server to manage received alerts which are displayed on any machines which have the Enterprise Console application installed.

Any number of users can be connected, although each must have a unique user name. Individual user privileges can be set to restrict or enable operators to perform different tasks. If several users are on duty and one person closes or replies to an alert, their action is broadcast to all other users.

Device Manager

This application is a stand-alone GUI used for:

- Manual entry of devices
- Device categorization
- Launching default applications
- Providing information regarding the SQL database connection

Instant Alert

Instant Alert is used to:

- Send text messages to mobile phones from the Enterprise Console
- Send email messages from the Enterprise Console
- Send messages to 3rd party help desk applications.
- Set up broadcast groups and call schedules to send messages to the appropriate on-call personnel.

User Names and Passwords

A user name and password is required to access the Enterprise Console. Privileges can be assigned to each user according to the system access and control required by that user.

Default User Name and Password

When the Enterprise Console is first launched the following default user name and password is applied:

- **User Name**: Administrator
- **Password**: Administrator

When a new user is added, a default password (the text used for the user name) is created automatically. When a new user first launches the Enterprise Console the current user name must initially be entered as the password. A message is then displayed advising the password has already expired and a new password must be entered.

Users and Administrators

Users are added, edited and deleted from **Enterprise Server Options** | **Users** page. User log on details (user name and a password) are required by each user or administrator each time they launch the Enterprise Console.

Multiple users and administrators can be added, but name/password combinations must be unique.

User and Administrator Privileges

Administrator privileges allow full control and typically, users can be granted a limited set of privileges, or full privileges specified from the privilege options available.

There are six areas of system privilege that can be granted to a user. If the user is entered as an administrator then access rights to these six areas are granted automatically.

Close

Gives the user the ability to close alerts.

Reply

Gives the user the ability to reply to alerts (where applicable).

Delete

Gives the user the ability to delete alerts.

Comment

Gives the user the ability to add a comment to alerts.

Command

Gives the user the ability to use the Command facility of the Enterprise Console.

Purge

Gives the user the ability to purge alerts.

Adding A User

Enterprise Console ships with a single default Administrator user profile. New users are added from the Enterprise Server Options | Users page.

To add a new user:

1. Click **Add User**.
2. Enter the following **User** details:

   Name: Enter the name for the new user.
   Nickname: If known, and required, enter the user's nickname.
3. Enter the following **Contact** details:

   Email: Enter the user's email address.
   Phone: Enter the user's land line phone number.
   Mobile: Enter the user's mobile phone number.
4. Select the **Privileges** that this user has when using Enterprise Console:

   Administrator: Check this box to give the new user administrator rights (all options)
   Close: Check this box to give this user the ability to close alerts (required if also Closing Inquiry Alerts - see below)
   Reply: Check this box to give this user the ability to reply to alerts
   Delete: Check this box to give this user the ability to delete alerts
   Comment: Check this box to give this user the ability to add comments to alerts

Command: Check this box to give this user the ability to run commands against alerts
Purge: Check this box to give this user the ability to purge alerts from the system

Select the **User Options** available to this user:

Close Inquiry Alerts: Check this box to give this user the ability to close inquiry alerts (user must already have the ability to close alerts). Leave the box empty to prevent the user from being able to perform this operation and warn the user of an invalid action. If they try and close multiple alerts in a single action, some of which are inquiry alerts, the inquiry alerts will not be closed and the user does not receive notification.

3. Click **OK** to accept the details and add the new user to the list of users displayed.

> NOTE: At this stage the password for the new user is the same as the user name, but must be changed when you log on to the Enterprise Console (see Changing Passwords for further details).

Editing User Details

User and administrator details are edited from Enterprise Server Options | Users page.

> NOTE: You cannot change a user name from this option. To change a user name, you must delete the existing profile and add a new user.

To edit user details:

1. Highlight the required user from the list displayed on the **Enterprise Server Options** | **Users** page and click **Edit User**.
2. Edit the required details in the **Edit User** dialog (The fields are the same as when adding a new user).
3. Click **OK** to accept the changes and return to the **Enterprise Server Options** | **Users** page.

Deleting a User

If an employee changes role or leaves the company it is good housekeeping to remove the user profile from the system to prevent any unauthorized access.

Users are deleted from the **Enterprise Server Options** | Users page.

To delete a user:

1. Select and highlight a user from the list displayed on the **Enterprise Server Options** | **Users** page.
2. Click **Delete User**. A message is displayed asking you to confirm the deletion.
3. Click **Yes** to delete the user details and prevent the user from being able to access Enterprise Console.

Changing Passwords

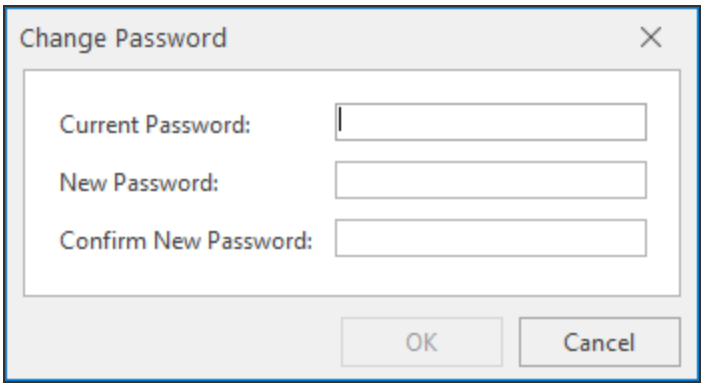
Passwords are changed from within the User Status option of Enterprise Console.

A password must be changed if it has expired, or a new password need to be generated for security reasons.

TIP: You can only change the password, using this option, for the current user that is logged in to the Enterprise Console.

To change a password:

1. From the Enterprise Console menu bar click ADMINISTRATOR **User Status** icon in the top-right corner.
2. From the drop-down menu choices, select **Password**. The **Change Password** dialog is displayed.



3. Type the **Current Password** in the top box, then enter a **New Password** and re-enter to confirm. Both entries must be identical.
4. Click **OK** to accept and save the new password. This is the password that must be entered the next time this user logs on to the launch the Enterprise Console.

Resetting Passwords

Passwords are reset from the **Enterprise Server Options**| Users page.

Resetting a password is a temporary measure, allowing the update of a user's existing password if they've forgotten it.

To reset a password:

1. Launch **Enterprise Server Options**, and select the **Users** option from the list of options in the left pane.
2. Select an existing user and if necessary set a **Password Expiration Interval**. This date is applied to the new password created at the point of the next log-on with this user.
3. Click **Reset Password**. A confirmation message is displayed.
4. Click **Yes** to confirm the reset password command. The reset password is now also the current user name. A confirmation message is displayed to validate the password has been reset against the specified user name.
5. Launch the Enterprise Console and enter the **User Name** and **Password**. At this stage the password is the same as the current user name (see step 4 above).
6. Enter the user name as the password (including spaces if required). A message is displayed advising the current password has expired and you are prompted to create a new one.
7. Click **OK** to display the **Change Password** dialog.
8. Enter the user name as the old password and enter and confirm the new password. The password dialog closes and the user now has access to the Enterprise Console.

Reset User Status

If a user becomes disconnected from the Enterprise Console while they are logged in, for example as the result of a power outage, and try to log in again, the system may assume they are already logged in and prevents access.

Quick Self -Reset

If the user trying to access the Enterprise Console is deemed to be already logged in, a 'User Already Logged In' message is displayed. Click **Yes** to reset this user's login status.

Reset on behalf of another user

1. Select the user name in the **Enterprise Server Options** | Users page and click **Reset Status**.

2. A confirmation message is displayed. Click **Yes** to confirm the status reset or **No** to cancel the request.
3. Click **Apply** to save the changes.

Keep **Enterprise Server Options** open or click **Cancel** to close Enterprise Server Options and return to the Enterprise Console.

Expired Passwords

When a password has expired, a new password must be created. The expiry period for the new password is specified on the **Enterprise Server Options** | Users page. This is a global setting and is applied to all further passwords until changed.

If prompted to change an expired password:

1. Click **OK** when prompted to display the **Change Password** dialog.
2. Enter the current password as the old password.
3. Enter a new password of your choice.
4. Click **OK** to close the dialog and return to the Enterprise Server Options.

Enterprise Console Connection Options

To launch the Enterprise Console select **Windows** | **Start** | **Halcyon** | **Enterprise Console**.

Each time the Enterprise Console is launched, the **Log In** dialog is displayed. The user must then enter a valid user name and associated password as defined in Enterprise Server Options. Passwords are not case sensitive.

Connecting to a different server other than the local machine

If more than one instance of Enterprise Console is installed on your network, a different server can be entered or selected at the point of log-in.

1. From the **Log-In** dialog box, click **Options >>**. The **Server Details** options are displayed. The TCP/IP address of the currently associated server is shown as a default.
2. Enter the **IP address** of the Server on which the required instance of Enterprise Console is installed.
3. Click **OK** to connect.

Connection to servers on a remote network

1. If the server is installed at a remote location protected by a firewall, use the additional **Route** option to specify the **IP address** of the firewall, so that the connection can be made successfully without blocking.
2. Click **OK** to connect.

Porting Requirements

1. Halcyon products use Port 15000 on IBM i to communicate between the device and the Enterprise Server.
2. Add 1 to the port number for each additional environment on the same partition to which the connection is made. For example, HALPROD = Port 15000, HALTEST = Port 15001, HALDR = Port 15002, and so on.

The implications of changing the IBM i port assignment

Changing the communications port on an IBM i that communicates with any other device will also require the same change of port on the devices with which it communicates.

If you have a network of IBM i devices that previously communicated with the Enterprise Server via port 15000 and you change the port of the Enterprise Server to 15005 you must also change the port assignment on all communicating IBM i to 15005 in order for systems messages and replies to be sent and received correctly.

> **NOTE:** Remember that any active firewalls must have the new range of ports opened.

Logging On and Off Enterprise Console

Logging onto the Enterprise Console

1. From Windows **Start** select **Halcyon** | **Enterprise Console**.
2. Enter a valid user name and password to log on to the **Enterprise Console** and click **OK**.

> **NOTE:** If you enter an invalid user name or password a generic login failure message is displayed. Click **OK** to close the dialog and retry.

> **IMPORTANT:** Following a system restart, the **Enterprise Console** may not be available for a short time period as the relevant services need time to start.

Logging off the Enterprise Console

1. From the Enterprise Console menu bar click 

User Status in the top-right corner.
2. From the drop-down menu select **Log Off**.
3. At the **Confirmation** prompt click **Yes** to log off the Enterprise Console and **No** to cancel the request.

Working with Substitution Variables

Substitution variables are used to insert a value that the code can reference. At run time, the actual value replaces a substitution variable. Different variables allow you to determine the text or detail that you wish to insert and at which point.

The commonest use of substitution variables is when formatting the text of alerts sent to the Enterprise Console or Instant Alert to be forwarded as SMS messages or emails.

All substitution variables begin with an ampersand (&) and are usually case-sensitive. When a substitution variable is used, the program searches for an ampersand and if found, compares the following text against a list of valid variables. If a match is made, the existing text is replaced with the substitution variable. Any non-matching text is left in its original condition.

When using substitution variables, any entries that are formed correctly are highlighted in green and those that will result in an error are highlighted in red.

EXAMPLE: In the following use of substitution variables:

'User &NA is not authorized to file &FN in folder &FL'

where:

- &NA equals User Name
- &FN equals File Name
- &FL equals Folder Directory and Name

may produce the following text:

'User John is not authorized to file Payroll.dat in folder C:\Program Files\

Retaining an ampersand in the existing text

If an ampersand is already present in the existing text to be retained when using substitution variables, simply insert a double ampersand to instruct the program that you wish to retain the original entry instead of using a substitution variable.

EXAMPLE: An example of how this works in practice can be seen below:

'Drives C, D &&E are working normally' would result in

'Drives C, D & E are working normally'.

Understanding Substitution Variables

In their most basic form, substitution variables are two character combinations. However, they can be of any length and longer variables are often required when two characters are not enough to differentiate one variable from another.

Generally, when a variable is used in a piece of text it is directly followed a break character such as a space, comma, period and the like.

> EXAMPLE: This is demonstrated in the example below:
>
> 'An error has occurred for Device ***&Name***. Please Investigate.'
>
> where: ***&Name*** equals **Backup**
>
> produces the following text:
>
> 'An error has occurred for Device ***Backup***. Please investigate.'

In the above example, the use of the period tells the program where the substitution variable ends so that it can correctly insert the replacement text.

Substitution variables can also be placed directly next to each other as shown in the next example which also demonstrates how substitution variables can be used in file naming conventions:

> EXAMPLE: 'HECArchive_***&DD&MM&YYYY***.eca'
>
> where:
> - &DD equals Day
> - &MM equals Month
> - &YYYY equals Year

may produce something similar to:

'HECArchive_***18June2009***.eca

Using Substitution Variables within text

In the previous sections, we explored entering substitution variables as standalone items, but there may be occasions when you need to use a substitution variable that is immediately followed by more text.

EXAMPLE: The following example uses variables called '&Type' which returns a value of 'Run', and '&Name', which returns a value of 'Backup'.

'***&Typetime*** Error Logged for System ***&Name***'

Entered in this format, the following is returned:

'***&Typetime*** Error Logged for System ***Backup***'

By using this format, entering the variable '&Type' immediately followed by the word 'time', results in an error as the program is looking for the substitution variable '&Typetime', which doesn't exist.

In order for the program to differentiate between where the substitution variable ends and the text begins, a pipe character followed by a semi-colon '|;' (without quotes) must be inserted between the end of the variable and the start of the text.

EXAMPLE: Therefore, by using the previous example:

'***&Type|;***time Error Logged for System ***&Name***' now results in:

'***Runtime*** Error Logged for System ***Backup***'

The '|;' signifies the end of a variable and that any text that immediately follows the semi-colon (and up to the next ampersand or break character) should be inserted as entered. The pipe and semi-colon characters are also used when adding parameters to substitution variables.

Adding Parameters to Substitution Variables

Parameters can be added to substitution variables to further enhance or manipulate the values that are substituted in the text.

Parameters are added in the same way as when inserting substitution variables within text, in that a pipe character '|' (without quotes) is added to the end of the variable. Further parameters, each separated by '|', finishing with '|;' can then be added when the full substitution variable with the required parameters has been entered. This combination tells the program when to start and end processing of the substitution variable with parameters.

Examples

In the following examples, the substitution variable '&UN' is used to return the text of 'Administrator'.

> EXAMPLE: If the basic form of the substitution variable was used:
>
> 'User &UN has logged on' would return:
>
> 'User Administrator has logged on'

However, by using parameters the user name can be displayed in upper case. To do this, add the 'u' parameter. (a full list of parameters can be found in Substitution Variable Parameters). This would affect the previous example as follows:

> EXAMPLE: 'User &UN|u|; has logged on' returning:
>
> 'User ADMINISTRATOR has logged on'

To add multiple parameters and change the appearance of the substitution variable even further, specify, for example:

> EXAMPLE: 'User &UN|u|+5|; has logged on'.
>
> This substitution variable entry would now return:
>
> 'User ADMIN has logged on'

This is because the variable now has the parameters of firstly converting the user name to upper case and then returning just the first five characters of the user name.

> NOTE: Substitution variables can return either string or numeric values. While applying each parameter, the software checks to see if the variable result is numeric. If it is, then only numeric parameters can be applied from that point onwards. To override this behavior and treat the numeric result as a string, the 's' parameter can be used.

String Substitution Variable Parameters

The following are examples of String Substitution Variable Parameters.

Parameter	Description	Example Value	Variable	Result
f	Trims any spaces from the beginning and end of the variable result	S=' Error Occurred '	&S|t|;	'Error Occurred'
tl	Trims any spaces from the beginning of the variable result	S=' Example text'	&S|tl|;	'Example text'

tr	Trims any spaces from the end of the variable result	S='Example text '	&S|tr|;	'Example text'
l	Converts the variable result to lower case	S='Example Text'	&S|l|;	'example text'
u	Converts the variable result to upper case	S='Example Text'	&S|u|;	'EXAMPLE TEXT'
p	Converts the variable result to proper case. i.e. the first letter of each word is a capital followed by lower case characters	S='EXAMPLE text'	&S|p|;	'Example Text'
P	The same as the 'p' parameter but preserves any existing capital letters	S='EXAMPLE text'	&S|P|;	'EXAMPLE text'
n-	Removes the first *n* characters from the variable result	S='Example text'	&S|-3|;	'mple text'
-n	Removes the last *n* characters from the variable result	S='Example text'	&S|-3|;	'Example t'
n+	Returns the first *n* characters from the variable result	S='Example text'	&S|4+|;	'Exam'
+n	Returns the last *n* characters from the variable result	S='Example text'	&S|=4|;	'text'
's'-	Removes all characters from *s* to the end of the variable result	S='Example text'	&S|'ple'-|;	' text'
-'s'	Removes all characters from *s* to the end of the variable result	S='Example text'	&S|-'ple'|;	'Exam'
's'+	Returns all characters up to and including *s* from the beginning of the variable result	S='Example text'	&S|'ple'+|;	'Example'

+'s'	Returns all characters from *s* to the end of the variable result	S=Example text'	&S|+'test'|;	'ple text'
s	Instructs the software that the variable result should be treated as a string	N=1784.23	&N|s|-4|;	'178'

Numeric Substitution Variable Parameters

The following are examples of Numeric Substitution Variable Parameters:

Parameter	Description	Example Value	Variable	Result
f	Returns the fractional part of a floating-point number	N+1784.23	&N|f|;	0.23
I	Returns the integer part of a floating-point number	N=1784.23	&N|i|;	1784
p*n*	Formats the variable to n decimal places from 0-9	N=1784.238175	&N|p2|;	1784.24
'kb' 'mb' 'gb' 'tb' 'pb' and 'eb' also supported	Converts a number representing bytes into the respective storage unit. The result is the decimal representation of the byte value (i.e. divided by 1000)	N=10273460156234	&N|kb|; &N|mb|; &N |gb|; &N|tb|;	102734601562.34 102734601.56234 102734.60156234 102.73460156234

'kib' 'mib' 'gib' 'tib' 'pib' and 'eib' also supported	Converts a number representing bytes into the respective storage unit. The result is the binary representation of the byte value (i.e. divided by 1024)	N=10273460156234	&N|kib|; &N|mib|; &N |gib|; &N|tib|;	10032675933.822 9797535.0916233 9567.9053629133 9.3436575809701
+n ***+&v***	Adds the number n to the variable result, or adds the value of variable &v to the result	N1=356 N2=78	&N1|+45|; &N1|+&N2|;	401 434
-n ***-&v***	Subtracts the number n to the variable result, or subtracts the value &V from the result	N1=356 N2=78	&N1|-45|; &N1|-&N2|;	311 278
*n ****&v***	Multiplies the number n to the variable result, or multiplies the value &V from the result	N1=356 N2=78	&N1|*45|; &N1|*&N2|;	16020 27768
/n ***/&v***	Divides the number n to the variable result, or multiplies the value &V from the result	N1=356 N2=78	&N1|/45|; &N1|/&N2|;	7.9111111 4.5641025

Device Manager

Overview

Device Manager is a standalone program that manages and configures network devices so that they are then available to other Halcyon programs.

> **NOTE:** In order to be visible in, and available for selection by other Halcyon programs, a device must exist within Device Manager.

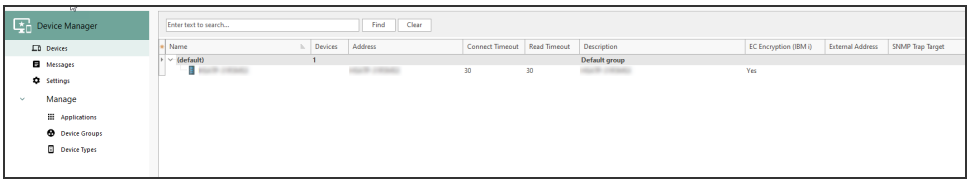
Recorded device information can be restricted to just **Name**, **Description** and **IP Address**, or can be fully comprehensive, incorporating time zones, support information and SNMP capability if available.

Defined devices can then be split into groups by, for example, type, department or location or whatever best suits an organizational structure.

Select Windows **Start** | **Halcyon** | **Device Manager** to open Device Manager.

The Device Manager display

By default when opened, the Device Manager main window displays a list of defined devices. This panel displays summary information for any devices that have already been defined.



Defined Devices panel

The following information is shown in the Devices panel.

Name

Displays the name of the device as it was defined in Device Manager.

Devices (at Group Level only)

Displays the number of devices currently defined in the group).

Address

Displays the IP Address, URL or Host name of the device as it is currently defined in Device Manager.

Connection Timeout

Displays the timeout period (in seconds) after which a request to connect to this device is considered unsuccessful.

Read Timeout

Displays the timeout period (in seconds) after which a request to read information from this device is considered unsuccessful.

Description

Displays the description of each device (and each group) defined within Device Manager.

EC Encryption (IBM i)

For IBM i type devices only, this setting indicates whether data sent from the device to the Enterprise Console is encrypted.

External Address

If the device is located behind a firewall, and an external IP address via which any connection can be made to ensure that alerts are transmitted to the Enterprise Console has been defined, the external IP address is displayed in this column.

SNMP Trap Target

Identifies if the device is specified as an SNMP Trap Target.

> TIP: Use the vertical scroll bar to view any additional devices that are not visible on the default display.

Re-arranging the information shown in this display

Information is listed in each panel in table columns. The contents of each column can be can be arranged in ascending/descending order by clicking on the column title to toggle the view.

Column positions can also be rearranged by single left-clicking on a column and keeping the mouse button depressed, dragging the column horizontally to a new position in the panel. Release the mouse-button to confirm the new column position.

Finding Device Entries

If you have many devices configured within Device Manager you can use the Search facility to pinpoint the device(s) that you want.

Begin typing the alphanumeric characters of the device(s) that you want to find in the defined list. Click **Find** to move to the located device in the list (providing that a match is made). Click **Clear** to remove the search criteria from the field.

Messages

The Messages panel is used to display warning and error messages regarding failed connections or porting issues with any of the devices listed in the Defined Devices panel.

Additionally, if Device Manager Settings for Informational and/or Diagnostic messages has been enabled, these messages are also displayed within this panel.

The Messages panel displays the following information:

Message type

Displays an icon to indicate the type of message that was generated.

	Complete
	Diagnostic
	Information
	Connected
	Disconnected
	Heartbeat
	Send
	Receive
	Check
	Warning
	Secure
	Locked
	Error
	Prohibited
	Critical
	Log

Date/Time

Displays the date and time at which the message was generated.

From

Displays the origin of the message.

Message

Displays the actual message text.

Clear Messages

Messages can be cleared by either highlighting the messages to be removed and using the  **Clear Message** option from the toolbar ribbon. Alternatively, right-click on an individual message in the Messages panel and select **Clear** from the pop-up menu.

Re-arranging the information shown in this display

Information is listed in each panel in table columns. The contents of each column can be can be arranged in ascending/descending order by clicking on the column title to toggle the view.

Column positions can also be rearranged by single left-clicking on a column and keeping the mouse button depressed, dragging the column horizontally to a new position in the panel. Release the mouse-button to confirm the new column position.

Devices

Devices are manually added to Device Manager so that they are then available for selection, monitoring, and sending of notifications within other Halcyon applications.

Devices must belong to a group. If they are not manually assigned a specific group, they are automatically assigned to the Default group that is shipped with the software.

As standard, devices can be any of the following types:

- AIX Server
- Bridge
- Fax
- Hub
- IBM i
- Laptop
- Linux Server
- Mail Server
- Modem
- PDA
- Printer
- Proxy Server
- Router
- Scanner
- Server
- Switch
- Unix Server
- Unknown
- Windows Server
- Windows Server 2003 Standard
- Workstation

See Adding a Device Type for instructions on how to add further device types to this default list.

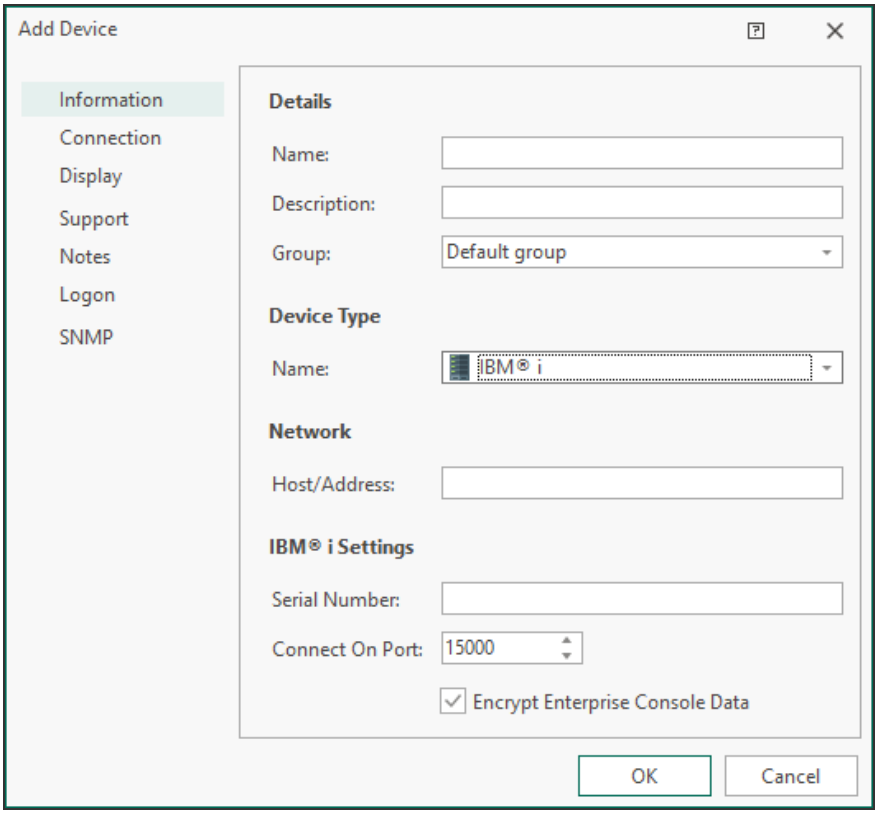
Adding a Device

A device must be added to Device Manager before it can be made available to other Halcyon programs.

To add a device to Device Manager:

1. Open **Device Manager**.
2. From the side navigation panel, select **Devices**.
3. Click **Add** from the toolbar ribbon.

   The **Add Device** dialog is displayed.



There are seven separate pages into which device information can be entered:

IMPORTANT: Completion of the parameters on the **Information** page is mandatory. Entering details into the parameters on the remaining pages is optional.

Information page

The following parameters must be completed on the Information page as they identify the device within the network.

Details section

Name

The device name **MUST** be the same as the actual system name.

Description

Enter an accurate description by which the device can be identified.

Group

Device Groups are used to be segregate groups of say, similar devices, or all devices belonging to a specific department. The Device Group (if used) can be specified using a selection from the drop-down menu.

Device Type section

Device Type

From the drop-down choice menu, select the device type. The following device types are shipped with the product and available for selection:

- AIX Server
- Bridge
- Fax
- Hub
- IBM i
- Laptop
- Linux Server
- Mail Server
- Modem
- PDA
- Printer
- Proxy Server

- Router
- Scanner
- Server
- Switch
- Unix Server
- Unknown
- Windows Server
- Windows Server 2003 Standard
- Workstation

> NOTE: Bespoke devices can be added to this list by using the **Device Types** option from the Device Manager menu ribbon. See Adding a Device Type for more information.

Network section

Network Host/Address

Enter the IP address of the device as it is registered in the network. A fully qualified domain name (FQDN) can be entered as an alternative.

IBMi Settings section (For IBM i Devices only)

Serial Number

Enter the serial number of the IBM i Device. Ask your system administrator if you are not sure where to locate this.

Connect On Port

The entry in this field specifies the port number on the IBM i to which Enterprise Console connects. This value must match the Port Value in the *SYSTEM Location of the IBM i device.

This value can be found as the top entry in **Configuration Menu** > **Work with Remote Locations** from the Halcyon menu on the IBM i device.

Encrypt Enterprise Console Data

This setting determines that any data sent between this device and the Enterprise Console is encrypted. This is enabled by default for any new IBM i device that is added.

> **NOTE:** Within the IBM i configuration, the Enterprise Console device will be identified as a *PC Remote Location which defaults data encoding to *ENCRYPT for any manually created or auto-config *PC Remote Location.

Connection page

The Connection page is used to enter details of alternative methods of connecting to the device and also specifies connection and read timeout parameters.

Alternative IP Addresses section

Alternative IP Address

Alternative IP Addresses are used to account for devices with multi-IP address capability or those that have further IP Addresses linked to the main IP Address. Click **Add** to add one or multiple IP addresses to this device.

External Interface section

External Interface

If this device is located behind a firewall, enter an external IP address via which any connection can be made to ensure that alerts are transmitted to the EEnterprise Console. See Device Groups - Connection Page for more information.

Timeout Settings (Seconds) section

Connection Timeout

The Device Manager abandons its connection attempt after the time period (in seconds) specified in this field. The default setting is 30 seconds.

Read Timeout

The entry in this field sets the read timeout limit, (the time waiting to read data), between the Device Manager and the remote device. The default setting is 30 seconds.

Display Page

The Display page controls the appearance of the device within Halcyon programs and sets geographical and time zone defaults.

Appearance section

Color

Specify the default color of the device when displayed in the Device Manager.

Geographical section

Location

If required, specify the physical geographical location of the network device.

Time Zone

If required, enter the time differential to take account of the geographical location of the device. For example, with the host device based in the UK, devices in Paris, France, would have a time differential of +1.00 to GMT.

The settings for this field are derived from the Windows time zone defaults, as found in Windows **Start** | **Control Panel** | **Date and Time**.

When an alert is received from a device located in a different time zone, the time is extracted from the incoming alert and an adjustment is made via the setting in this field on the receiving Enterprise Console device prior to being displayed.

The **Use Current** setting for this field automatically sets the time zone to the local setting derived from the device to which the alert is sent. This setting is useful for devices such as printers and those that send SNMP Traps.

> WARNING: Ensure that the time settings on the remote device are correct prior to activating this feature otherwise timing inaccuracies of alert data can occur.

> WARNING: Any changes to the Time Zone settings in this field override any pre-existing settings on devices running Server Manager.

Support Page

The parameters on this page are used to enter the details of any support information. None of the fields on this page are mandatory.

Contact section

Name

If required (or known), enter the name of associated personnel responsible for this device.

Company

If applicable, enter the name of the associated company/division where the device is installed.

Associated Application section

Name

Select an application which is then associated with a device (for example wireless configuration software). The entry in this field is then used if the Launch Associated Application from an alert received from this device is actioned from the Enterprise Console.

Test Application

Click **Test Application** to test launch the selected application associated with the device.

Notes Page

Use this page to enter any free-text notes about the device. These notes can be used as a substitution variable when sending an alert from this device.

Logon page

The Logon page is used to supply a user name and associated password that can be used to log-on to this device, should a log-on be required.

Logon Details section

User Name

Enter a user name that can be used to access this device.

Password

Enter the password associated with the specified user name for this device.

SNMP page

These settings are used to define any SNMP capabilities of the device.

SNMP Options section

Device is a Trap Target

Check to indicate if the current device is a trap target, and therefore can receive trap messages. SNMPv3 is supported.

Trap Port

Enter the port number used for the trapping of messages.

Once the required device information has been entered, click **OK** to add the device to Device Manager.

Editing a Device

The details of any device listed in the **Defined Devices** panel can be amended at any time.

> WARNING: Editing certain fields, such as Time Zone for example, may cause unexpected results in other settings within Enterprise ConsoleNetwork Server Suite.

To edit device details:

1. Open **Device Manager**.
2. From the side navigation panel, select **Devices**.
3. From within the **Defined Devices** panel, single-click on the device to be edited. The device is now highlighted.
4. From the toolbar ribbon, click  **Edit**.
5. Edit the current settings as required. The fields are the same as used when Adding a Device.

Copying a Device

Devices can be copied directly from the Defined Devices panel allowing instant duplicates to be created.

The copied device can then be edited to change one or more parameters to make it unique. This facility is useful if there are many similar devices that need adding but may only differ by, for example, IP Address.

To copy a device:

1. Open **Device Manager**.
2. From within the **Defined Devices** panel, single-click on a device so that it is highlighted.
3. From the Device Manager toolbar ribbon, click **Copy**.
4. From the same toolbar, click **Paste**.

An instant copy of the selected device is now displayed in the **Defined Devices** panel, identified by **Copy** after the device name. Both the copied and original device are displayed in red text in the **Address** column to draw attention that edits and renaming conventions need to be applied.

TIP: Use **Select All** to select all defined devices for copying.

Deleting a Device

Deleting a device permanently removes it from view within Device Manager and its availability across all Halcyon applications that use Device Manager.

To delete a device:

1. Open **Device Manager**.
2. From the side navigation panel, select **Devices**.
3. From within the **Defined Devices** panel, single-click on the device to be removed. The device is now highlighted.
4. From the toolbar ribbon, click **Delete**.
5. When prompted, click **Yes** to confirm the deletion or **No** to cancel.

Device Groups

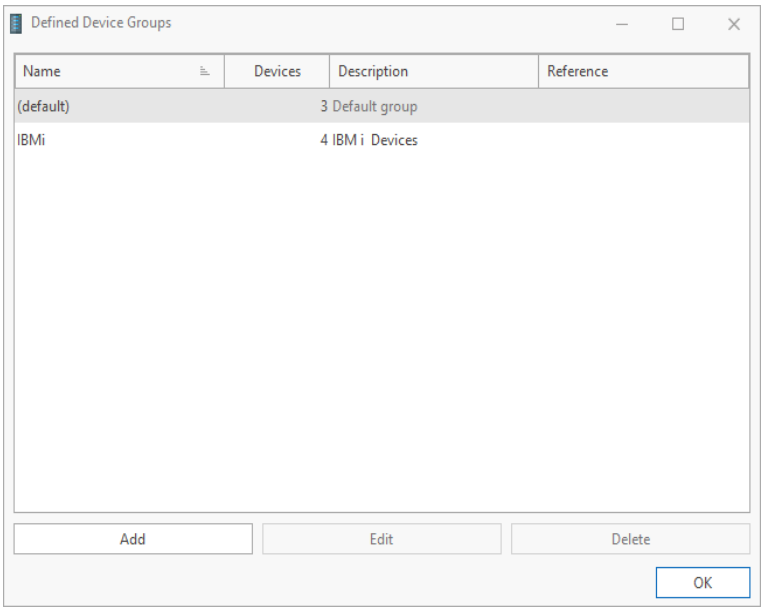
Once defined, devices can optionally be segregated into groups, for example, of similar devices, all devices belonging to a specific department, by location, or by whatever method required.

> **NOTE:** If you choose not to define any groups, all devices are grouped together in the standard Default group that is shipped with the product.

Devices can be displayed by Group in the Devices panel of other Halcyon applications.

From the side navigation panel, select **Manage** > **Device Groups** to display a list of the current **Defined Device Groups**.

From the toolbar ribbon, click **Manage Device Groups** to open the Defined Device Groups dialog.



From this dialog it is possible to add new or edit and delete existing device groups from Device Manager.

Adding a Device Group

To add a Device Group to Device Manager:

1. Open **Device Manager**.
2. From the toolbar ribbon, click **Manage Device Groups**.
3. Click **Add** to open the **Add Device Group** dialog.

There are three pages into which device group information can be entered.

Information page

The Information page is used to enter basic, identification labels for the device group.

Information section

Name

Enter a unique name by which to identify the device group.

Description

Enter text that accurately describes the device group.

Additional section

Reference

If required, enter a reference, such as for example, Department Account Number or Asset Number, for the device group.

Connection Page

The following parameter is available on the Connection page:

Route section

Route

The route field defines a series of IP addresses that are then used in sequence order to connect to all the devices included in this group.

> **NOTE:** This field can include external IP addresses if required.

Use of the Route function allows Enterprise Console alerts to be passed between firewalls.

1. Click **Add** to open the **Add Route Entry** dialog into which a new **IP Address** can be entered.
2. Click **OK** to add the new connection route to the list.

Notes Page

The Notes page can be used to enter any free-text notes relating to this device group.

Once the required information has been entered, click **OK** to add the new device group.

Editing a Device Group

The details of any device group can be edited, other than the Default device group.

To edit Device Group details:

1. Open **Device Manager**
2. From the toolbar ribbon, click **Manage Device Groups**.
3. From the device groups listed in the **Defined Device Groups** dialog, single-click on the one to be edited. The device group is now highlighted.
4. Click **Edit** to open the **Edit Device Group** dialog. Parameters that can be edited on this display are the same as those used when Adding a Device Group.

When editing is complete, click **OK** to save the changes or **Cancel** to leave the original settings in tact.

Deleting a Device Group

Any device group can be deleted, other than the default device group.

> WARNING: Deleting a device group does not delete the devices contained within the group. They are moved to the default device group.

To delete a Device Group:

1. Open **Device Manager**.
2. From the toolbar ribbon, click **Manage Device Groups**.
3. From the device groups listed in the **Defined Device Groups** dialog, single-click on the group to be deleted.
4. Click **Delete**.
5. At the prompt click **Yes** to delete the device group or **No** to cancel the request.

Device Types

Device types are a way of categorizing devices that have similar characteristics.

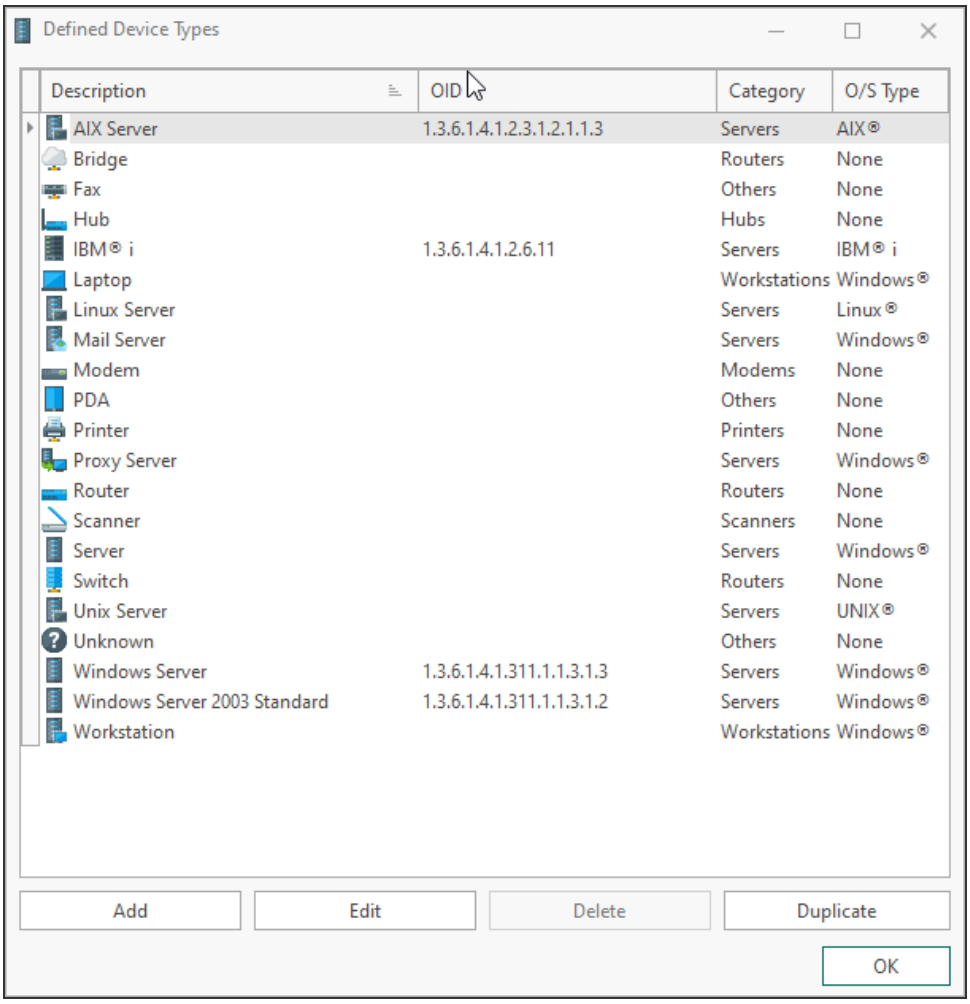
The full list of shipped device types is shown below:

- AIX Server
- Bridge
- Fax
- Hub
- Laptop
- Linux Server
- Mail Server
- Modem
- PDA
- Power/System i
- Printer
- Proxy Server
- Router
- Scanner
- Server
- Switch
- Unix Server
- Unknown
- Windows Server
- Windows Server 2003 Standard
- Workstation

Any devices that are not currently available from the supplied device type list can be added using the Add Device Types option.

From the side-navigation panel, click **Manage >** **Device Types** to display the current list of device types.

To work with device types, open **Device Manager** and from the **Toolbar** ribbon click **Manage Device Types**.



This display shows the **Device type icon**, associated **Description** and if one has been defined, the **Object ID** for use with SNMP Monitoring. The **Category** and **O/S Type** for each device type are also displayed.

From this dialog it is possible to add new and edit, delete and duplicate existing device types.

> **NOTE:** It is not possible to delete a default device type that was shipped with the software.

Adding a Device Type

To add a Device Type to Device Manager:

1. Open **Device Manager**.
2. From the toolbar ribbon, click **Manage Device Types** to open the **Defined Device Types** dialog.
3. Click **Add** to open the **Add User-Defined Device Types** dialog.

The following parameters are available on the **Add User-Defined Device Type** dialog:

Description

Enter a meaningful description used to identify the new device type.

Object ID

If the device is SNMP trap enabled, enter the unique object identity number for this type of device.

Category

If required, select a pre-defined category with which the device type is then associated. The following categories are available:

- Others
- Workstations
- Servers
- Hubs
- Routers
- Bridges
- Modems
- Printers
- Scanners

O/S Type

From the drop-down menu, select the type of Operating System that the device uses. The choices are:

- None
- AIX
- i5/OS
- Linux
- UNIX
- Windows

Icon

From the drop-down choice menu, select an icon by which the device type is then identified.

Default Associated Application

From the drop-down choice menu, select an application with which the device type is associated by default. This can be overridden when adding a new device. Select from:

- None
- Device Web Page
- pcAnywhere
- Remote Desktop Connection
- VNC

> **NOTE:** Additional applications are available in this parameter once they have been added using the Add Application options.

4. Click **OK** to add the new Device Type.

Editing a Device Type

The details of any user-defined device type can be edited.

> **NOTE:** Only the icon and the default associated application parameters can be edited for default device types.

To edit a Device Type:

1. Open **Device Manager**.
2. From the toolbar ribbon, click **Manage Device Types** to open the **Defined Device Types** dialog.
3. From the **Defined Device Types** dialog, single-click on the device type to be edited. The device type is now highlighted.
4. Click **Edit** to open the **Edit Pre** (or) **User Defined Device Type** dialog. Parameters that can be edited on this display are the same as those used when Adding a Device Type (Unless the device type being edited is a default device type).
5. When editing is complete, click **OK** to save changes or **Cancel** to leave the original settings.

Deleting a Device Type

Any user-defined device type can be deleted but not a default device type (one that was shipped with the product).

To delete a user-defined device type:

1. Open **Device Manager**.
2. From the toolbar ribbon, click **Manage Device Types** to open the **Defined Device Types** dialog.
3. From the **Defined Device Types** dialog, single-click on the user-defined device type to be deleted. The device type is now highlighted.
4. Click **Delete** (this is only enabled for applicable device types).
5. At the prompt click **Yes** to delete the Device Type or **No** to cancel the request.

Duplicating a Device Type

Duplicating a device type allows the rapid creation of device types with similar attributes which can then be edited at a later time.

To duplicate a Device Type:

1. Open **Device Manager**.
2. From the toolbar ribbon, click **Manage Device Types** to open the **Defined Device Types** dialog.
3. From the device types listed in the **Defined Device Types** dialog, single-click on the one to be duplicated. The device type is now highlighted.
4. Click **Duplicate**. The selected device type is instantly duplicated and displayed in the list of device types, identifiable by **Copy** after the device type name.

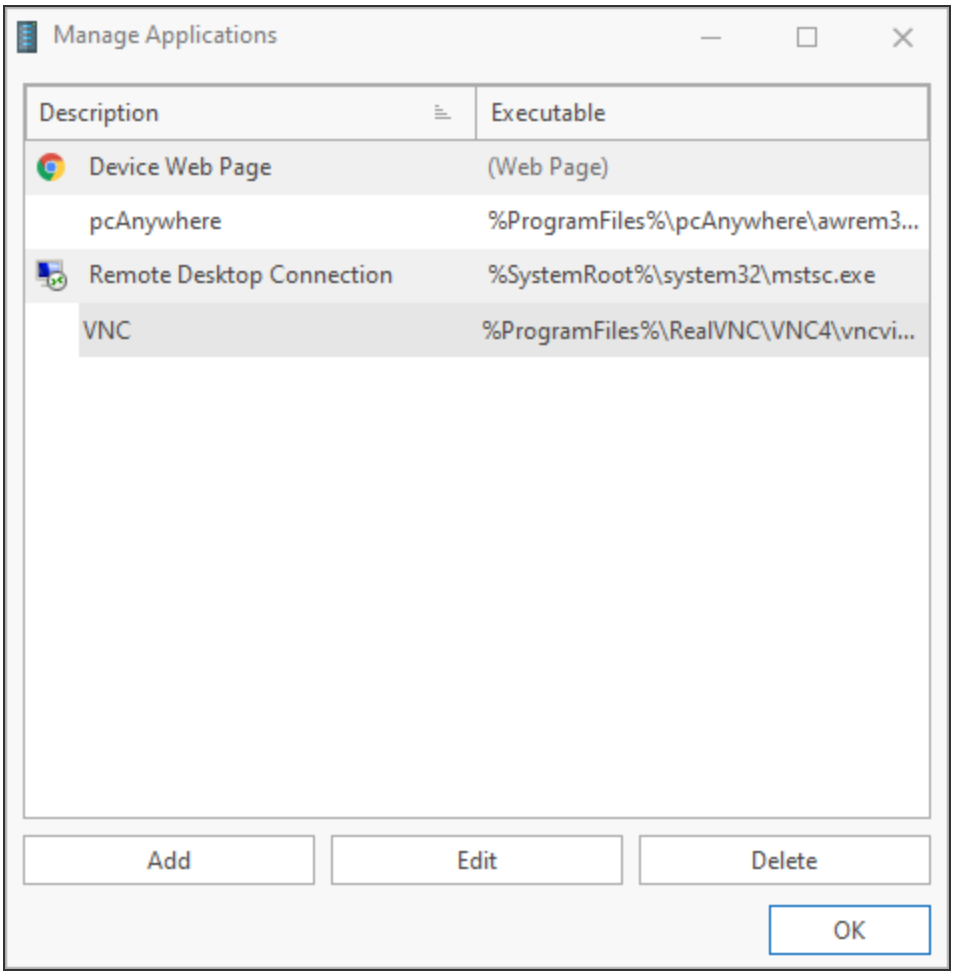
The device type can now be edited as required.

Applications

Applications are programs that can be launched directly from an alert on the Enterprise Console when received from any device associated with the selected device type.

Such programs are typically Remote Access or Web Page Interfaces from which diagnostic and configuration settings can be maintained.

Applications associated with device types are defined and managed from the **Manage Applications** dialog.



This dialog allows the addition of new applications and the editing or deletion existing applications.

To display applications select **Manage** > **Applications** from the side navigation panel,

To work with applications, from the toolbar ribbon click **Manage Applications** .

Adding a new Application

If an application is not currently listed, it can be added using the following procedure.

To add a new application:

1. Open **Device Manager**.
2. From the toolbar ribbon, click  to open the **Manage Applications** dialog.
3. Click **Add** to open the **Add Application** dialog.

The following parameters are available on the **Add Application** dialog.

Application section

Description

Enter a textual description of the application by which it will then be identified within Device Manager and Enterprise Console.

Application Is A Web Page

Click to define the new application as a web page.

Executable

Enter the directory path in which the application executable is stored. If required, use  **Browse** to navigate to a specific directory path.

> NOTE: This field is not required if the **Application Is A Web Page** parameter is enabled.

Parameters

Enter any parameters required to launch the application upon opening (listed Substitution and Environmental Variables may be used).

Example

Displays an example of how the entry in the **Parameter** field will read when using a mixture of free-text, substitution and environmental variables.

Substitution and Environmental variables

Displays a selection of valid substitution and environmental variables that can be used in the construction of the instruction in the **Parameter** field.

4. Click **OK** to add the application.

Editing an Application

The details of any existing application can be edited.

To edit an application:

1. Open **Device Manager**.
2. From the toolbar ribbon, click  to open the **Manage Applications** dialog.
3. From the **Manage Applications** dialog, single-click on the application to be edited.
4. Click **Edit** to open the **Edit Application** dialog. Parameters that can be edited on this display are the same as those used when Adding a new Application.
5. When editing is complete, click **OK** to save changes or **Cancel** to leave the original settings.

Deleting an Application

An application can be deleted if it is no longer required.

To delete an application:

1. Open **Device Manager**.
2. From the toolbar ribbon, click  to open the **Manage Applications** dialog.
3. From the **Manage Applications** dialog, single-click on the application to be deleted.
4. Click **Delete**.
5. At the prompt click **Yes** to delete the application or **No** to cancel the request.

IBM i Client Access Applications

A client access application can be created for when access to an IBM i device is directly required from within the Enterprise Console.

> **NOTE:** The IBM emulator software must be running on the same device as that on which Device Manager is installed.

A separate .WS file must be created for each IBM i device to be added.

TIP: It is recommended that each of these are named as the system name.ws to ensure connection to the correct device.

To create an IBM i Client Access Application

1. Open **Device Manager**.
2. From the toolbar ribbon, click  to open the **Manage Applications** dialog.
3. From the **Manage Applications** dialog click **Add** to open the **Add Application** dialog.
4. In the **Description** parameter, enter **Client Access 'System Name'**, for example 'Client Access Dev123'.
5. In the **Executable** parameter, either type the path of where the required emulator .ws file is stored or use  **Browse** to search for and automatically enter the file path.

NOTE: If the **Browse** option is used, change the search parameters to look for '**All Files**' and not just '**Program**' files.

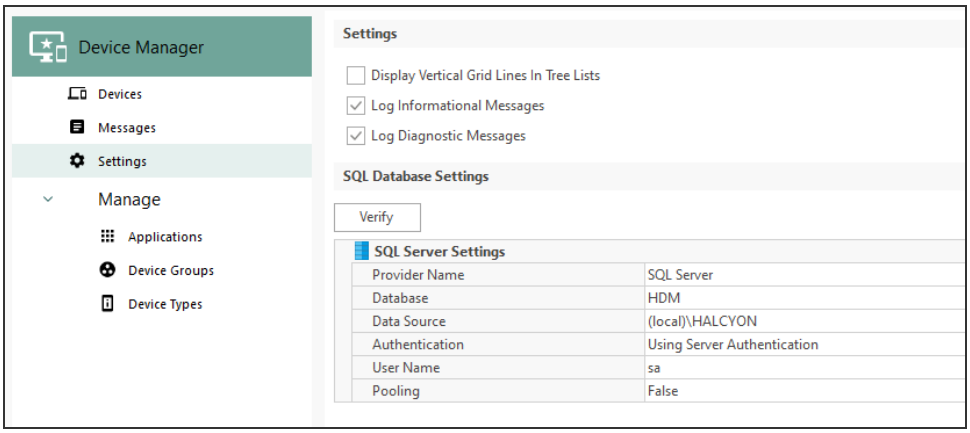
6. Click **OK** to confirm and add the client access application.

Device Manager Settings

Device Manager Settings are used to set display view options, specify logging and view the current database settings.

From the **Device Manager** side navigation panel, select **Settings** to open the Device Manager Settings display.

The display view options, current logging and SQL Server Settings are shown in a quick view format.



Display Vertical Grid Lines In Tree Lists

Click this option to display the information within each Device Manager view within extended column grid lines.

Logging options

Logging of messages allows for the provision of housekeeping and fault-finding analysis. The information recorded may also be useful to the technical support team should an issue arise that requires further investigation. The default name for the saved Log file information is **DevManager.hlf**, which is saved in **C:\ProgramData\Halcyon\Device Manager\Logs** unless the default settings were changed at the point of installation. if logged, messages are also displayed in the Messages panel of the Device Manager display.

Log Informational Messages

Click to log all messages relating to the operation of Device Manager.

Log Diagnostic Messages

Click to log all Device Manager diagnostic messages.

SQL Database Settings

The SQL Database Settings panel allows the view, but not the ability to amend, the details of the database to which Device Manager is connected.

Provider Name

Displays the name of the type of database that this installation is currently using.

Database

Displays the name of the database being used by this installation of Device Manager.

Data Source

Displays the name and location of the database source.

Authentication

Displays the method of authentication being used between Device Manager and the database.

User

Displays the name of the user that is currently accessing the database.

Pooling

Indicates whether or not the pooling of database connections is used so that the connections can be reused when future requests to the database are required.

Minimum Pool Size

Displays the minimum number of database connections that can be used concurrently.

Maximum Pool Size

Displays the maximum number of database connections that can be used concurrently.

Verifying the Connection

Click **Verify** to ensure that a connection is made to the database with the current settings. Please contact Technical Support if the connection is not verified.

Once the contents have been viewed, click **OK** to close this dialog.

> **NOTE:** The settings on this dialog are for informational purposes only. No amendments can be made from this display.

Importing and Exporting Devices

If you are transferring this instance of Device Manager to another PC, devices can be exported and imported.

This process saves the device configuration to a file, which can then be transferred to an external source such as a network drive or memory stick. The file can then be imported onto the new machine at a later time and/or date. This saves time and effort in re-defining the devices a second time on a different machine.

Exporting Devices

To export the current device configuration:

1. Open **Device Manager**.
2. From the header bar click **Export Devices**.

   TIP: This option is also available by clicking in the title bar and selecting **Export Devices** from the drop-down menu.

3. Click **Export Device** from the toolbar. The **Select Export File** dialog is displayed.
4. Use the standard Windows dialog to navigate to the directory to where the file will be stored. The file name defaults to:
   Devices-yyyy-dd-mm-hhmmss-msc.dsf.

NOTE: The .DSF extension represents Device Settings File.

5. Click **Save** to save the exported devices file.

Importing Devices

To import the current device configuration:

1. Open **Device Manager**.
2. From the header bar click **Import Devices**.

   TIP: This option is also available by clicking in the title bar and selecting **Import Devices** from the drop-down menu.

3. When prompted to confirm the import of devices, click **Yes** to continue. The **Select Import File** dialog is displayed.
4. Navigate to the path to where the exported .dsf file was saved and make sure the file is selected.
5. Click **Open** to import the devices with the default settings, otherwise enter a new file path and/or file name prior to importing.

SNMP Page

The SNMP page of Device Manager is used to define and list SNMPv3 Users that can then be used within Network Server SuiteEnterprise Console to Send Trap Actions when rule criteria has, or hasn't been met.

From the bottom of the Device Manager side-navigation panel, click  to open the SNMPv3 Users display.

The main display lists users that have been defined for sending and receiving SNMPv3 traps.

Options on the toolbar allow you to add, edit and delete SNMPv3 users.

When you have completed your tasks on the SNMP page, click  to return to the Devices menu options.

Adding an SNMPv3 User

1. Open **Device Manager**.
2. From the side-navigation panel, click  to open the SNMPv3 Users display..
3. From the toolbar ribbon, click  **Add SNMPv3 User**. The Add SNMPv3 User dialog is displayed.
4. In the **User Name** field, enter the name of the user that you want to define for the sending and receiving of SNMPv3 Traps.
5. In the **SNMPv3 Authentication** field, select the method of authentication to be used for the sending and receiving of SNMPv3 Traps for this user.
    - **MD5**: Authenticates by using an encoded MD5 checksum that is included in the transmitted packet.
    - **SHA**: A 160-bit hash function which resembles the earlier MD5 algorithm.
    - **SHA-256**: The SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash.

- **SHA-512**: The SHA-256 algorithm generates an almost-unique, fixed size 512-bit (64-byte) hash.
- **None**: No authentication is used

6. In the associated **Password** field, enter the password required for the chosen method of authentication (unless the authentication method is none).

> NOTE: The password must be a minimum of 8 characters. For MD5 Authentication it **must** be 16 octets long and for SHA authentication it must be 20 octets long.

7. In the **SNMPv3 Privacy** field, select the required SNMPv3 privacy protocol for this user.
   - **DES**: Data Encryption Standard (DES) Cipher Block Chaining (CBC) mode. Uses 16-byte key (56-bit DES key, 8-byte DES initialization vector) known by sender and receiver
   - **3DES**: Triple Data Encryption Standard (Triple DES)
   - **AES192**: Advanced Encryption Standard (192 bit key)
   - **AES256**: Advanced Encryption Standard (256 bit key)
   - **None**: No SNMPv3 privacy protocol is used.
8. Click **OK** to add the new SNMPv3 user.

Editing an SNMPv3 User

1. Open **Device Manager**.
2. From the side-navigation panel, click  to open the SNMPv3 Users display..
3. Single-click on the SNMPv3 User that you want to edit.
4. From the toolbar ribbon, click **Edit SNMPv3 User**. The Add SNMPv3 User dialog is displayed.
5. Use the instructions in Adding an SNMPv3 User to amend any of the details for the selected user.
6. Once the amendments are complete, click **OK** to add the new SNMPv3 user.

Deleting an SNMPv3 User

1. Open **Device Manager**.
2. From the side-navigation panel, click  to open the SNMPv3 Users display.
3. Single-click on the SNMPv3 User that you want to delete.
4. From the toolbar ribbon, click **Delete SNMPv3 User**.
5. At the prompt, click **Yes** to delete the SNMPv3 User or No to cancel the request.

Enterprise Console

Overview

View messages and alerts generated by IBM i, AIX, Linux and Windows servers on a centralized graphical PC console to give a dashboard view of your entire enterprise.

The hub of Halcyon’s systems management is the Enterprise Console. The Enterprise Console is supplied free of charge with all of Halcyon's major IBM i and Windows suites.

Replies can be given to messages and alerts closed from the central console while color-coded options help identify different servers and/or different types of alerts. Comprehensive filters can escalate actions, change severity and forward alerts.

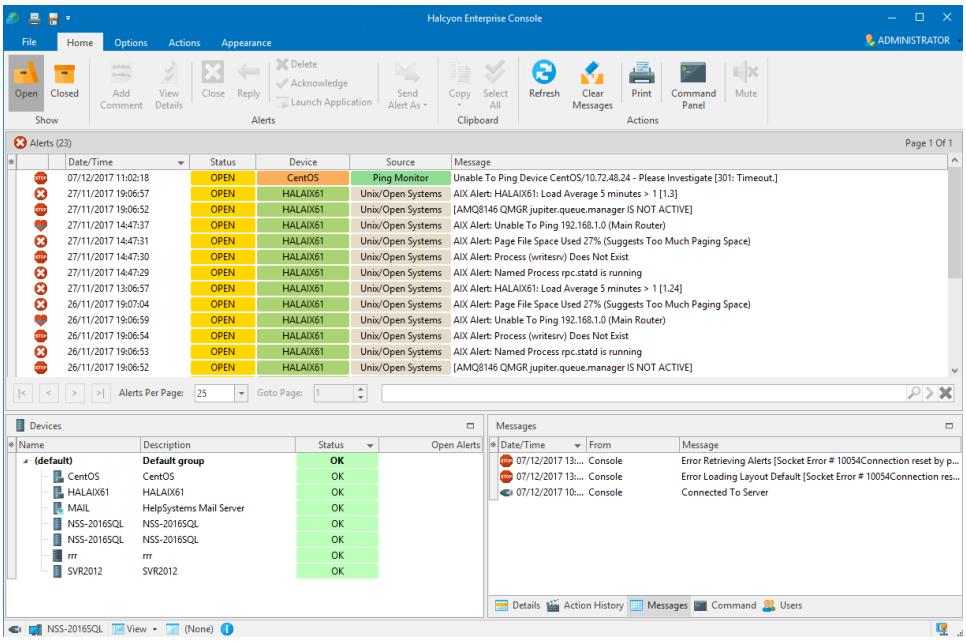
Enterprise Console is best used for monitoring and controlling multiple servers from a single location.

Use the Enterprise Console to:

- Provide color-coded monitoring for easy identification of different servers and types of alert.
- Set rules to monitor for specific actions happening or more importantly NOT happening.
- Deliver notifications by SMS or Email.
- Integrate with existing help desk applications.
- Provide a full audit trail of alerts.

The Enterprise Console Display

Alert details, device identities, device details, action histories and associated alert messages are displayed, by default, in panels contained within the main Enterprise Console window.



Each panel within the display can be repositioned within the window or floated on the desktop and re-sized as required. See Changing Layouts for more information.

User privileges also affect which functions are available from the layout (privileges are set in the **Enterprise Server Options** | **Users** | **Add-Edit User** dialog).

Default Panels of the Enterprise Console

The default panels of the Enterprise Console are split into:

- Alerts (Information and Inquiry)
- Devices
- Details/Action History/Messages/Command/Users

WARNING: On upgrade from a previous version, the Enterprise Console will revert to the default layout, regardless of how the panels were previously setup. A warning of this change is provided during the upgrade process.

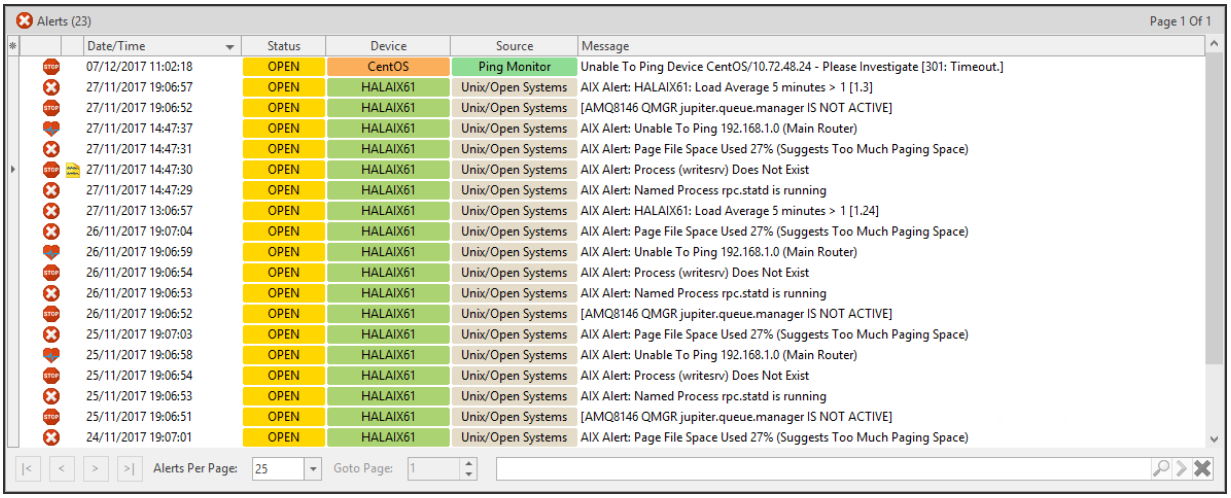
Alert panels

In its default format, these panels display alerts that have been directed to the panels from a Send Console Alert rule action. The default alert panels are called Inquiry and Information.

If required, the name of these panels can be changed in order to make it more meaningful. See Editing Panels for more information.

Information in this panel is displayed across the following columns.

TIP: To display or hide columns from this panel, left-click in the header of the far left-column of this panel to display a drop-down menu of available columns that can be displayed or hidden from view in this panel.



Date/Time	Status	Device	Source	Message
07/12/2017 11:02:18	OPEN	CentOS	Ping Monitor	Unable To Ping Device CentOS/10.72.48.24 - Please Investigate [301: Timeout.]
27/11/2017 19:06:57	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: HALAIX61: Load Average 5 minutes > 1 [1.3]
27/11/2017 19:06:52	OPEN	HALAIX61	Unix/Open Systems	[AMQ8146 QMGR jupiter.queue.manager IS NOT ACTIVE]
27/11/2017 14:47:37	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Unable To Ping 192.168.1.0 (Main Router)
27/11/2017 14:47:31	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Page File Space Used 27% (Suggests Too Much Paging Space)
27/11/2017 14:47:30	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Process (writesrv) Does Not Exist
27/11/2017 14:47:29	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Named Process rpc.statd is running
27/11/2017 13:06:57	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: HALAIX61: Load Average 5 minutes > 1 [1.24]
26/11/2017 19:07:04	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Page File Space Used 27% (Suggests Too Much Paging Space)
26/11/2017 19:06:59	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Unable To Ping 192.168.1.0 (Main Router)
26/11/2017 19:06:54	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Process (writesrv) Does Not Exist
26/11/2017 19:06:53	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Named Process rpc.statd is running
26/11/2017 19:06:52	OPEN	HALAIX61	Unix/Open Systems	[AMQ8146 QMGR jupiter.queue.manager IS NOT ACTIVE]
25/11/2017 19:07:03	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Page File Space Used 27% (Suggests Too Much Paging Space)
25/11/2017 19:06:58	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Unable To Ping 192.168.1.0 (Main Router)
25/11/2017 19:06:54	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Process (writesrv) Does Not Exist
25/11/2017 19:06:53	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Named Process rpc.statd is running
25/11/2017 19:06:51	OPEN	HALAIX61	Unix/Open Systems	[AMQ8146 QMGR jupiter.queue.manager IS NOT ACTIVE]
24/11/2017 19:07:01	OPEN	HALAIX61	Unix/Open Systems	AIX Alert: Page File Space Used 27% (Suggests Too Much Paging Space)

Alerts

The number of alerts within this panel, that are currently held in the database, is shown in brackets in the header of this panel.

Selection Identifier

The first column is used as a secondary indicator of which alert has been selected. In addition to the alert being highlighted, a '**>**' mark is inserted in this column against the selected alert.

Alert Type Identifier

The second column is used to display the alert type icon associated with the alert. See Alert Settings for a full list of possible icons that may be displayed in this column.

Comment Identifier

The third column is used to display  **Comments** to indicate any alert that has a comment raised against it.

Date/Time

Displays the date and time at which the alert was received by the Enterprise Server. See Time Zone for information regarding alerts received from remote devices in different time zones.

Status

Displays the current status of the alert. This can be one of:

- Open
- Closed
- Acknowledged
- Console
- Error

> **NOTE:** The  symbol against an alert in this column signifies that the alert is an Inquiry alert. See Replying to Inquiry Alerts for more information.

Device

Displays the name of the device from which the alert was received.

Address

Displays either the device host name or IP Address dependent on how the device was defined within Device Manager. This column is hidden by default.

Description

Used to identify any device that was used to forward the alert to the Enterprise Console. See Alerts received via forwarding systems for more information. This column is hidden by default.

Source

Displays the name of the Halcyon monitor, source system or third party application that generated the alert. The following Halcyon products do not generate alerts and therefore do not interface with Enterprise Console:

- Message Communicator
- Performance Analyzer
- Spooled File Manager
- Disk Space Manager
- Authority Swapper
- Document Management System
- Record & Playback
- Exit Point Manager
- Password Reset Manager

See Source Types for more information.

Message

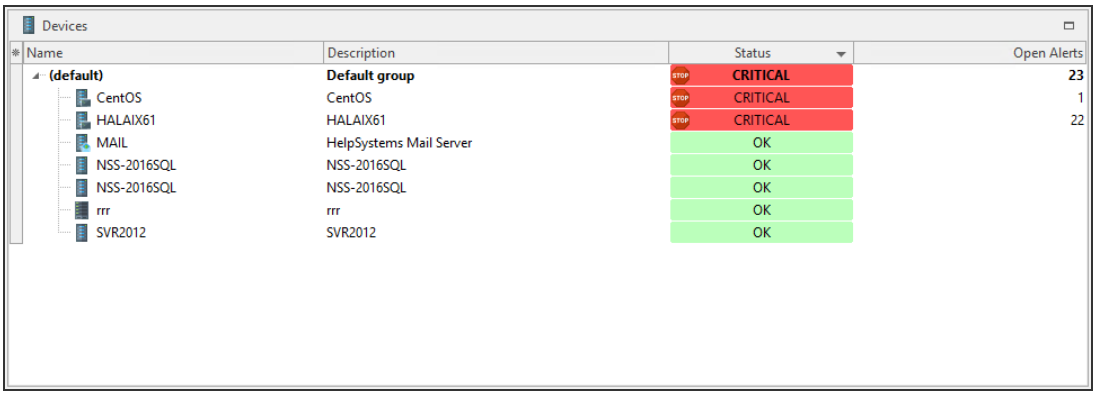
Displays the alert text as defined in the rule criteria that generated the alert. See Rule tab - Alert Message for more information.

Devices Panel

The Devices panel shows all the current devices that have been defined using the Device Manager.

By default, the devices are displayed in descending order by Status (i.e. those needing urgent attention are shown at the top of the list).

It is possible to change the sequence by clicking on any of the other column headings. For example, to change the sequence to display by alphabetical device name, click the **Name** column heading.



The following columns are available in the Devices panel. Left-click ✱ in the header of the far left-column of this panel to display a drop-down menu of available columns that can be displayed or hidden from view in this panel.

Default Columns

The default columns displayed in this panel are:

Selection Identifier

The first column is used as a secondary indicator of which device has been selected. In addition to the device being highlighted, a '**>**' mark is inserted in this column against the selected device.

Name

Displays the name of the Device Group and subsequent device within that group. Click on the arrow beside the group name to expand or hide the devices contained within the group.

Description

Displays the description attributed to each group and device listed.

Status

Shows the current status of the device. By default, devices are listed in descending order of severity depending on the number and type of alerts currently registered against the device.

Open Alerts

Displays the number of open alerts currently registered against this device.

Additional Columns

Additional columns that can be displayed in this panel are:

Devices

Displays, at Group level, the number of devices contained within the group.

Address

Displays the Host name or IP Address of each displayed device.

Object ID

Displays the Object ID attribute if the device has been defined as having SNMP Trap capability.

Connect Timeout

Displays the connection timeout period for each device.

Read Timeout

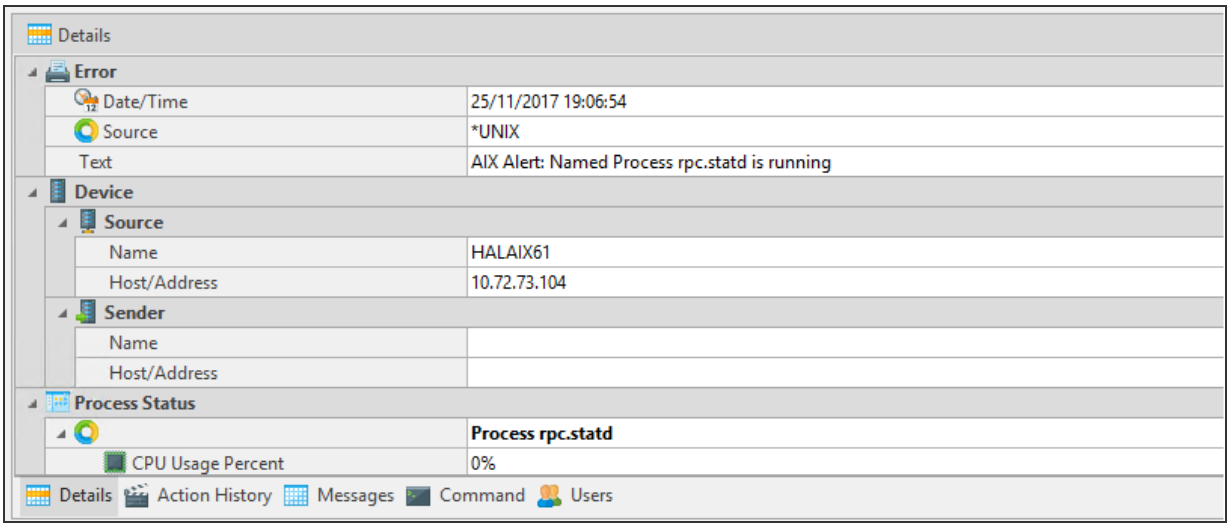
Displays the read timeout period for each device.

Alert Pct

Displays the alerts registered against groups and individual devices as a percentage figure of all open alerts.

Details/Action History/Message/Command/Users Panel

There are five different options that can be displayed within this panel. Each is accessible by clicking the relevant menu tab at the bottom of the panel.



Details Panel

This panel has a dual purpose and can be used to display the details of any device selected from the Devices panel or the details of an alert selected from any alert panel.

When displaying device details:

For IBM i devices, this panel shows details of the following (information from other devices vary by device and operating platform):

Device

As taken from the field properties in Device Manager.

Device Information

Includes serial number, model, feature code, processor group, processors, etc.

Environment

Name and details of the Halcyon environment.

IPL Settings

Details of last IPL and other IPL settings.

Cache Battery Information

Provides details if the IBM i is equipped with cache battery.

Installed Products

Displays details of all Halcyon products installed.

When displaying alert details:

When displaying alert detail, this panel commonly shows:

Alert Type

The Alert Type assigned to the alert, such as Error, Critical, etc. Sub-panels in this section show:

- **Date/Time**: Displays the date and time at which the alert was generated
- **Source Type**: Displays the source type that generated the alert
- **Message**: Displays the alert text

Device

Sub-panels in this section show:

- **Source**: Displays the Device name and Host name/IP Address of the Source device and which raised the alert.
- **Sender**: If the alert was routed via another device this displays the Device name and Host name/IP Address of the device which sent the alert to the Enterprise Console

Comments

This section displays any user comments that have been applied to the alert.

Status

If applicable, this section displays a snapshot of the process status at which time the alert was raised. This contents and title of this section are dependent on the process on which the rule was based.

Rule Details

Full details of the rule criteria that raised the alert.

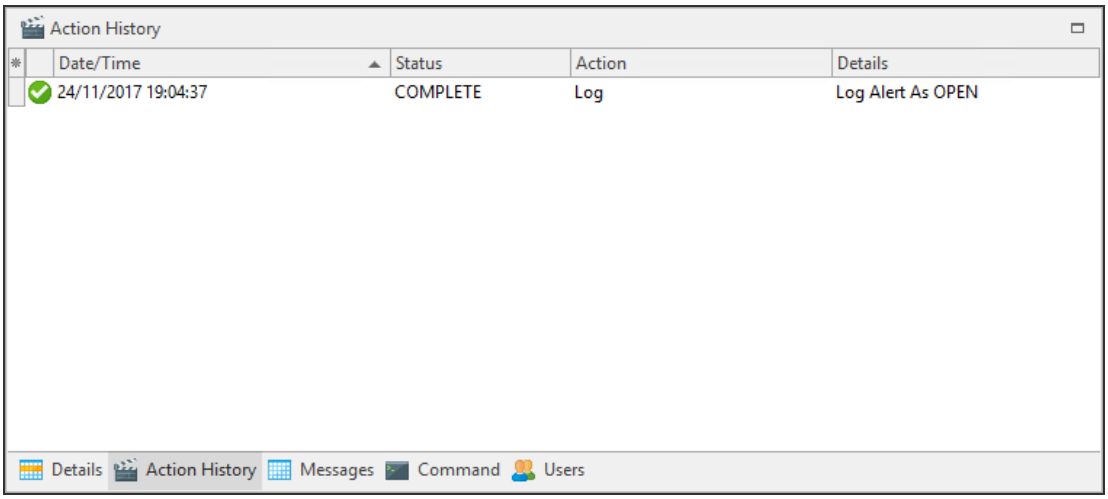
Console

Sequence number and name details of the rule that raised this alert to the Enterprise Console

Dependent on the panel size and orientation, use the vertical scroll bar to view further details not visible in the initial display.

Action History panel

The Action History panel shows what actions have been processed against the alert since it was first logged on the Enterprise Console.



Selection Identifier

The first column is used as a secondary indicator of which action has been selected. In addition to the action being highlighted, a '>' mark is inserted in this column against the selected action.

Success Identifier

Displays an icon to indicate the success of the action.

Date/Time

Displays the date and time at which the action was processed.

Status

Displays the current status of the action.

Action

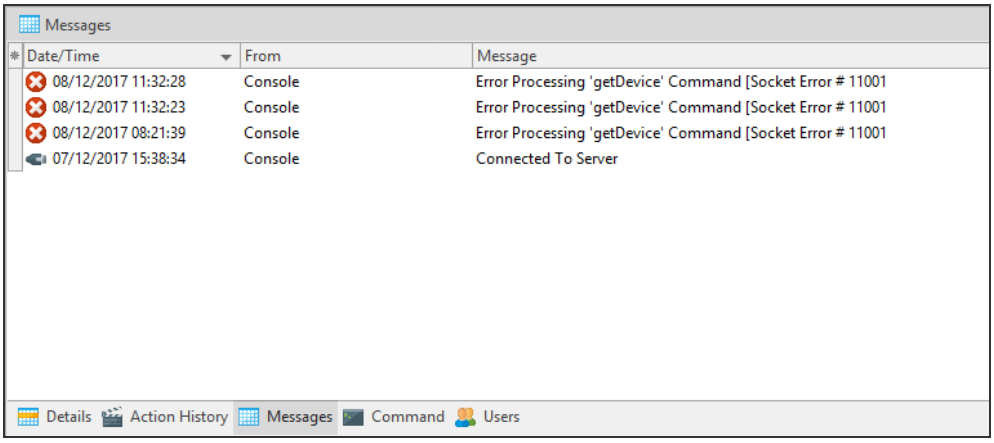
Displays the type of action that was performed.

Details

Displays a full description of the action that was performed.

Messages Panel

The Messages panel shows details of any system messages that may have been generated as a result of Enterprise Console activity. The messages within this panel are consistent, regardless of the alert or device that has been selected in any other panel.



Selection Identifier

The first column is used as a secondary indicator of which action has been selected. In addition to the action being highlighted, a '>' mark is inserted in this column against the selected action.

Date/Time

Displays the date and time at which the message was generated.

From

Displays the name of the device from which the message was received.

Message

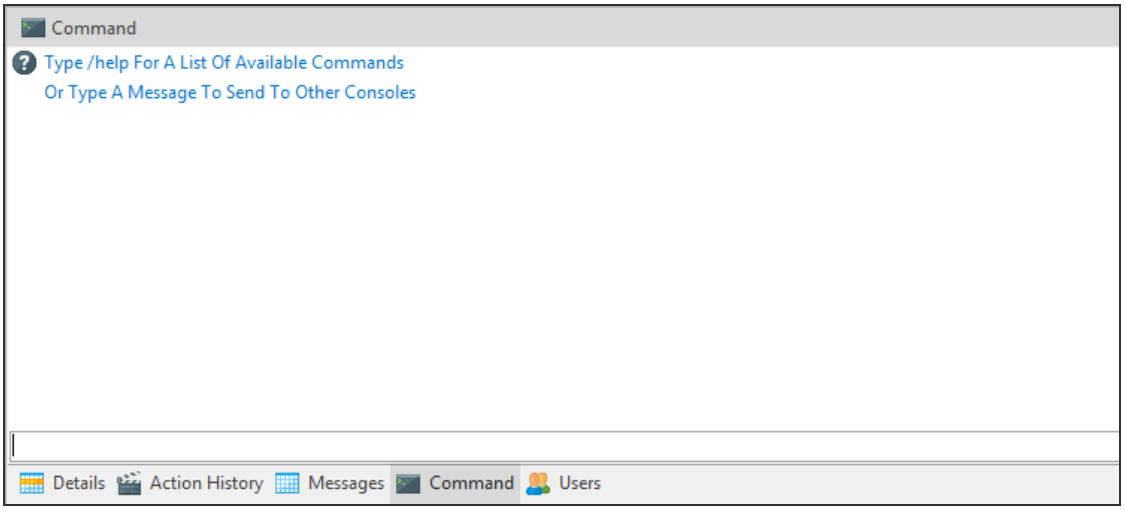
Displays full text of the message.

Clear Messages

Right-click on any message from within the **Messages panel** and click **Clear Messages** to remove **ALL** the messages from this panel.

Command Panel

The Command panel is used to send system messages to other users.



In the text box, at the bottom of this panel type **/help** to see a list of commands that can be sent. Alternatively, type a message that can be sent to one or more of the other console users listed in the right pane of this panel.

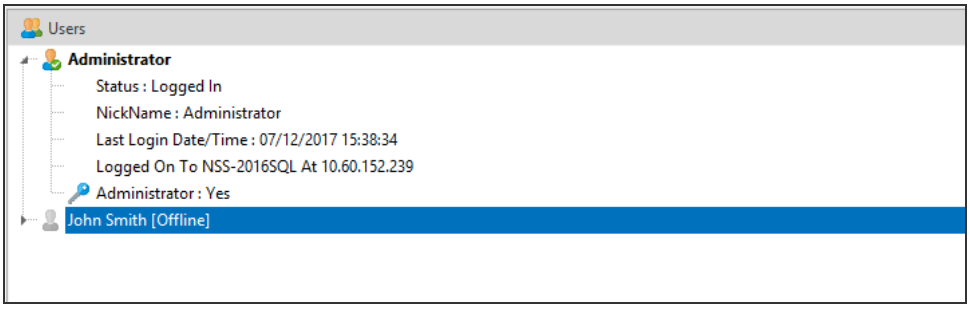
The following commands can be entered (commands are not case-sensitive):

- **/AWAY**: without message
- **/AWAY AT LUNCH**: with a message, for example; 'At Lunch'
- **/CLS**: clears the command screen
- **/DATE**: returns the Enterprise Server date
- **/HELP**: displays a list of available commands
- **/LICENSE**: displays licensing information
- **/MSG**: sends a message
- **/TIME**: returns the Enterprise Server time
- **/VERSION**: Returns the Enterprise Console version
- **/PING**: pings a server
- **/NICK**: sets the user's nickname
- **/MSGTO**: sends a message to a specific user (can use either the user name or nickname)
- **/WHOIS**: returns user info for a specified user. Can use either the user name or the nickname.

TIP: The Command Panel can also be accessed by clicking **Command Panel** in the **Enterprise Console** | **Home** menu ribbon.

Users Panel

The Users panel displays the details of all users that have been defined for use with this Enterprise Console.



Expand the view of any user to view the following information:

- Status
- Nickname
- Last Login Date/Time
- Logged On to
- Administrator Status

User Status

Availability of users across the network is remotely monitored and messages can be exchanged between all connected users.

The availability status of users can be set individually by each user. Click 

User in the top-right of the Enterprise Console menu ribbon and select one of the available options:

- I am Available
- I am Away
- I am on a Break
- I am at Lunch
- I am away from my Desk
- Do not Disturb (messages may be hidden when this option is selected)

Although the status is updated and distributed automatically, this function requires a manual change to be made by each user in order to be accurate.

> TIP: This option can also be used to change the user password and by a user to log off from the Enterprise Console

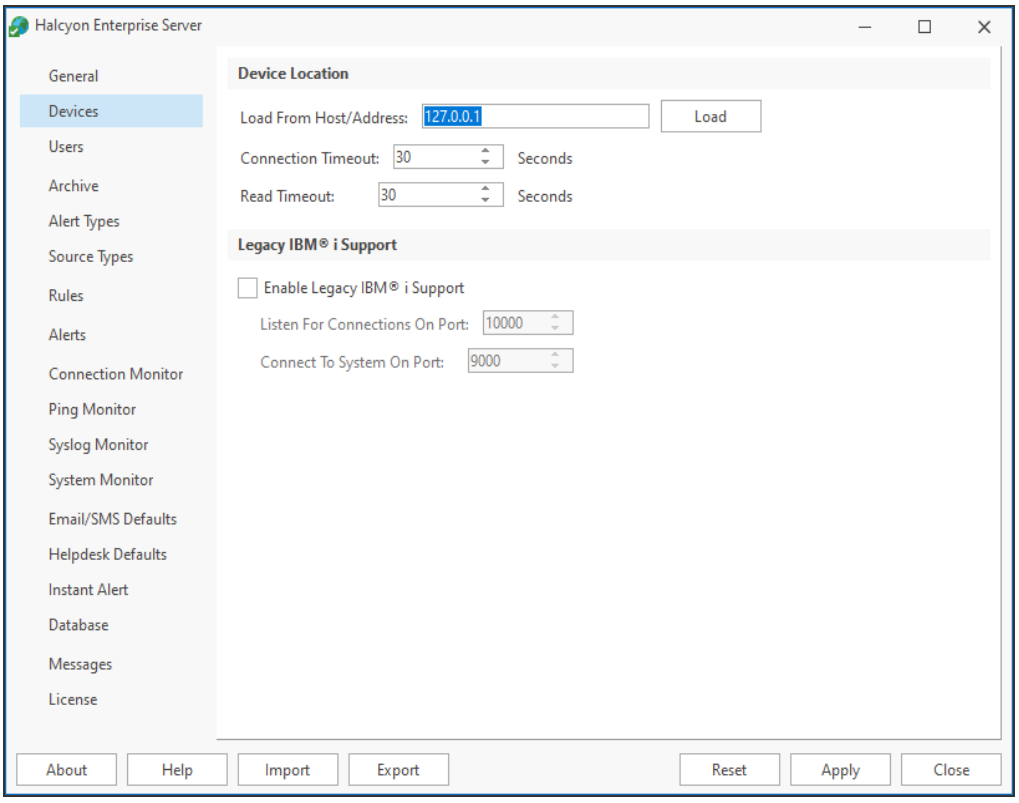
Enterprise Server Options

Enterprise Server Options is a standalone application used to specify, edit and change Enterprise Server settings; for example, message logging, user access rights, rules, alerts, Ping and Connection Monitor settings.

Enterprise Server Options is accessed via Windows **Start** | **All Programs** | **Halcyon** | **EC Server Options**.

TIP: Enterprise Server Options can also be accessed from within Enterprise Console using | **Server Options**.

Settings are entered via page tabs displayed in the left-hand navigation panel of the main panel.



[General settings]

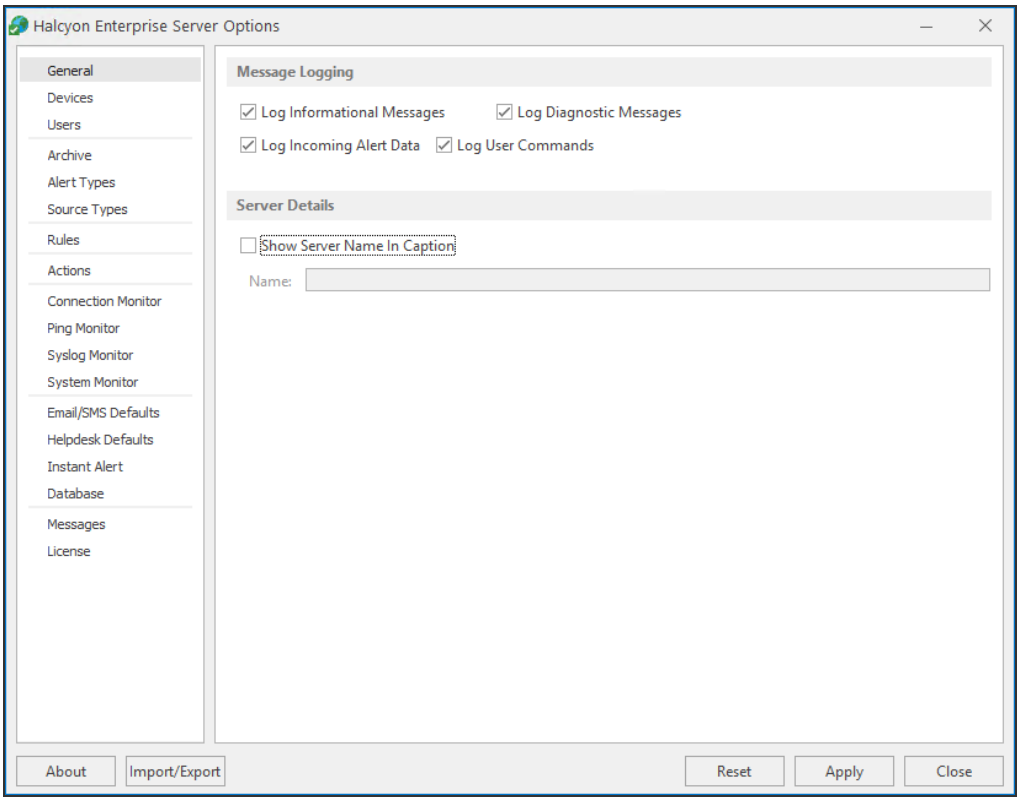
[Device settings]

[Users settings]

[Archive settings]

> **NOTE:** Enterprise Server Options are not available when the Enterprise Console is viewed from a client device.

Enterprise Server Options- General settings



Message Logging Settings section

> **NOTE:** All Enterprise Server Options log files are saved with an extension of .hlf in the folder: %ProgramData%\Halcyon\Enterprise Server Options\Logs

This section is used to determine the messages and commands that are logged.

Log Informational Messages

Check this option to log all messages relating to the operation of the Enterprise Server.

Log User Commands

Check this option to log all commands entered by users in the Enterprise Console Command Panel.

Log Diagnostic Messages

Check this option to log all system diagnostic messages.

Log Incoming Alert Data

Check this option to log all alert messages that have an action of Send Enterprise Console assigned.

Server Details Settings section

This section is used to define the server name that is displayed in the title bar of the Enterprise Console.

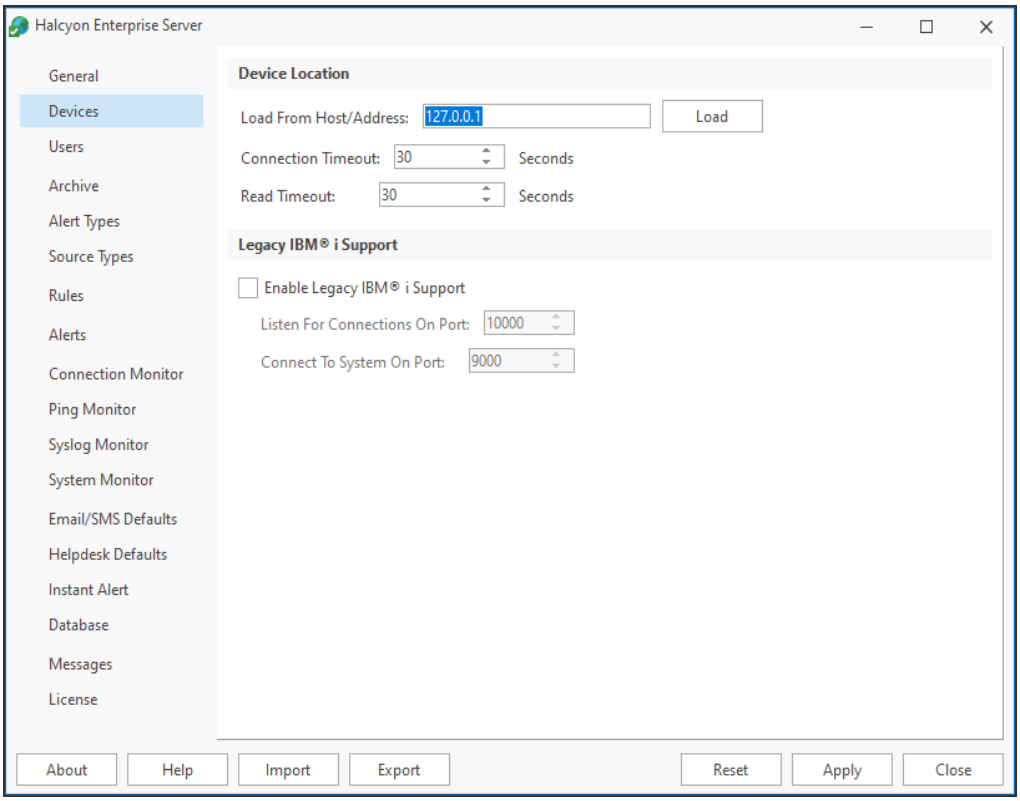
Show Server Name In Caption

Check this option to enable the input of a specific server name.

Name

Type a name that then appears in the **Enterprise Console Window Title Bar**. For example, entering Demonstration Server would result in the following:

Enterprise Server Options - Device Settings



Device Location Settings section

These options are used to define the server on which Device Manager is installed and the connection and read timeout periods.

Load From Host/Address

Type a Host Name or TCP/IP address of the server from which devices can be loaded for use in the Enterprise Console. The default is the local host address: 127.0.0.1.

> **NOTE:** This server must have the Device Manager component installed.

Click **Load** to confirm the entered address and reload any new devices.

Connection Timeout

When the Enterprise Server needs to communicate with a remote device (one of the devices to which it has sent an alert) it abandons its connection attempt after the interval specified here. The default setting is 30 seconds.

The Enterprise Server tries to connect to remote systems when it needs to close an alert, reply to an alert, gather system information or load devices.

Read Timeout

The entry in this field sets the read timeout limit (the time needed to read information) between the Enterprise Console and the remote device. The default setting is 30 seconds.

Legacy IBM Power/System i Support section

For IBM i connections (only visible in specially licensed versions) it is possible to state the port on which to listen for IBM i connections and the port on which outgoing connections to the IBM i device are made.

> TIP: This section only applies to IBM i devices running Halcyon Legacy software.

> **NOTE:** Porting requirements for IBM i devices can be found in the Logon page available when adding a device using Device Manager.

Enable Legacy IBM i Support

Click to enable Legacy IBM i support on this device and enable the Listen For Connection On Port and Connect To System On Port options.

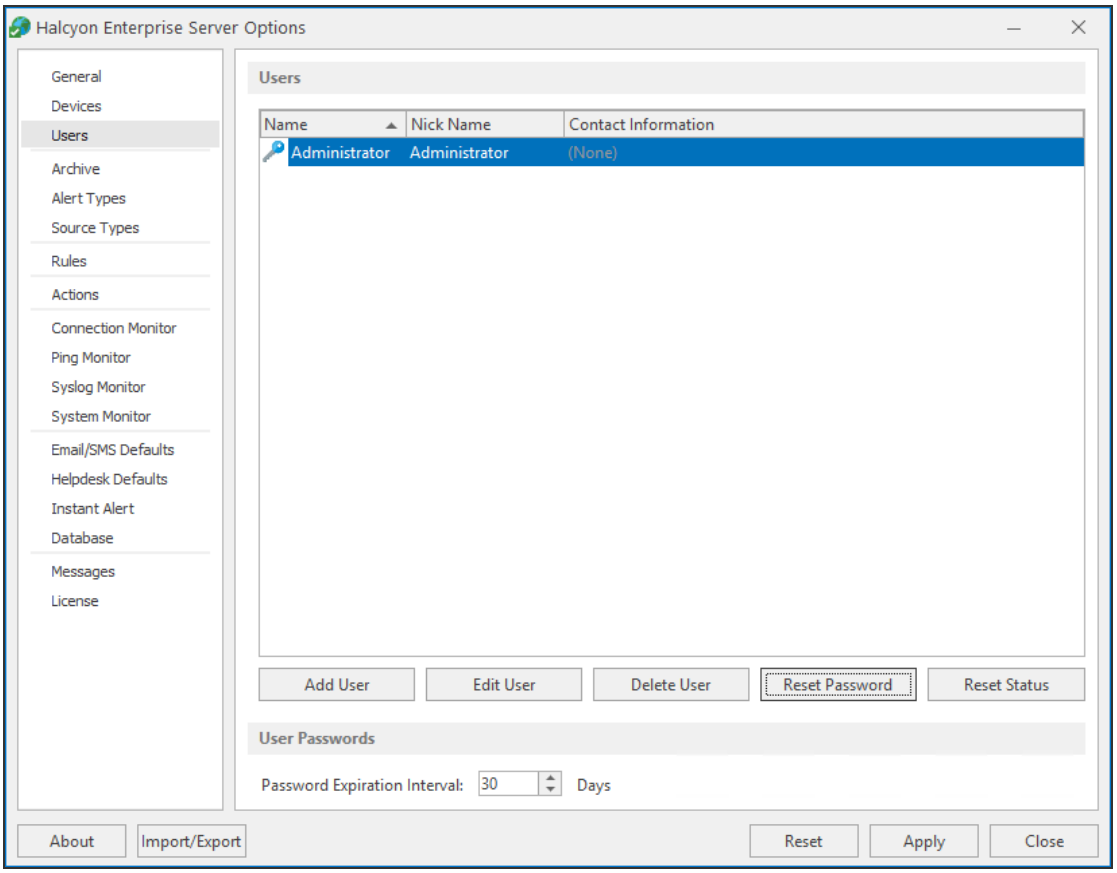
Listen for Connections on Port

Specify the port number on which incoming IBM i alerts are received. The default setting is 10000.

Connect To iSeries On Port

Specify the port number on which outgoing connections to IBM i devices are made. The default setting is 9000.

Enterprise Server Options - Users settings



The Users page of Enterprise Server Options page allows the adding, editing and deletion of users plus the resetting of passwords.

Users section

This displays the list of all the users that have currently been defined for this installation of Enterprise Console.

Users can be added, edited and deleted from this section.

User Passwords section

Password Expiration Interval

This field is used to set the number of days between when user passwords need to be changed. The default setting is 30 days.

> **NOTE:** This setting applies to all users and is not configurable on a user-by-user basis.

Adding A User

Enterprise Console ships with a single default Administrator user profile. New users are added from the Enterprise Server Options | Users page.

To add a new user:

1. Click **Add User**.
2. Enter the following **User** details:

   Name: Enter the name for the new user.
   Nickname: If known, and required, enter the user's nickname.
3. Enter the following **Contact** details:

   Email: Enter the user's email address.
   Phone: Enter the user's land line phone number.
   Mobile: Enter the user's mobile phone number.
4. Select the **Privileges** that this user has when using Enterprise Console:

   Administrator: Check this box to give the new user administrator rights (all options)
   Close: Check this box to give this user the ability to close alerts (required if also Closing Inquiry Alerts - see below)
   Reply: Check this box to give this user the ability to reply to alerts
   Delete: Check this box to give this user the ability to delete alerts
   Comment: Check this box to give this user the ability to add comments to alerts
   Command: Check this box to give this user the ability to run commands against alerts
   Purge: Check this box to give this user the ability to purge alerts from the system

Select the **User Options** available to this user:

Close Inquiry Alerts: Check this box to give this user the ability to close inquiry alerts (user must already have the ability to close alerts). Leave the box empty to prevent the user from being able to perform this operation and warn the user of an invalid action. If they try and close multiple alerts in a single action, some of which are inquiry alerts, the inquiry alerts will not be closed and the user does not receive notification.

3. Click **OK** to accept the details and add the new user to the list of users displayed.

> **NOTE:** At this stage the password for the new user is the same as the user name, but must be changed when you log on to the Enterprise Console (see Changing Passwords for further details).

Editing User Details

User and administrator details are edited from Enterprise Server Options | Users page.

> **NOTE:** You cannot change a user name from this option. To change a user name, you must delete the existing profile and add a new user.

To edit user details:

1. Highlight the required user from the list displayed on the **Enterprise Server Options** | **Users** page and click **Edit User**.
2. Edit the required details in the **Edit User** dialog (The fields are the same as when adding a new user).
3. Click **OK** to accept the changes and return to the **Enterprise Server Options** | **Users** page.

Deleting a User

If an employee changes role or leaves the company it is good housekeeping to remove the user profile from the system to prevent any unauthorized access.

Users are deleted from the **Enterprise Server Options** | Users page.

To delete a user:

1. Select and highlight a user from the list displayed on the **Enterprise Server Options** | **Users** page.
2. Click **Delete User**. A message is displayed asking you to confirm the deletion.
3. Click **Yes** to delete the user details and prevent the user from being able to access Enterprise Console.

Resetting Passwords

Passwords are reset from the **Enterprise Server Options**| Users page.

Resetting a password is a temporary measure, allowing the update of a user's existing password if they've forgotten it.

To reset a password:

1. Launch **Enterprise Server Options**, and select the **Users** option from the list of options in the left pane.

2. Select an existing user and if necessary set a **Password Expiration Interval**. This date is applied to the new password created at the point of the next log-on with this user.
3. Click **Reset Password**. A confirmation message is displayed.
4. Click **Yes** to confirm the reset password command. The reset password is now also the current user name. A confirmation message is displayed to validate the password has been reset against the specified user name.
5. Launch the Enterprise Console and enter the **User Name** and **Password**. At this stage the password is the same as the current user name (see step 4 above).
6. Enter the user name as the password (including spaces if required). A message is displayed advising the current password has expired and you are prompted to create a new one.
7. Click **OK** to display the **Change Password** dialog.
8. Enter the user name as the old password and enter and confirm the new password. The password dialog closes and the user now has access to the Enterprise Console.

Reset User Status

If a user becomes disconnected from the Enterprise Console while they are logged in, for example as the result of a power outage, and try to log in again, the system may assume they are already logged in and prevents access.

Quick Self -Reset

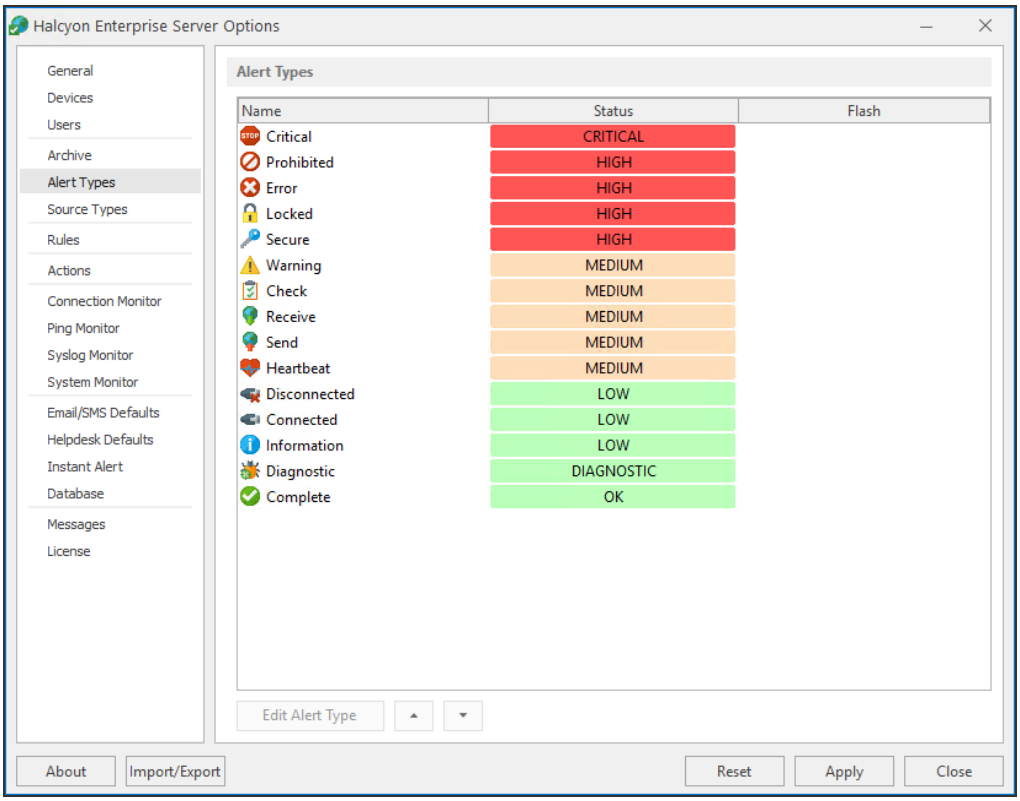
If the user trying to access the Enterprise Console is deemed to be already logged in, a 'User Already Logged In' message is displayed. Click **Yes** to reset this user's login status.

Reset on behalf of another user

1. Select the user name in the **Enterprise Server Options** | Users page and click **Reset Status**.
2. A confirmation message is displayed. Click **Yes** to confirm the status reset or **No** to cancel the request.
3. Click **Apply** to save the changes.

Keep **Enterprise Server Options** open or click **Cancel** to close Enterprise Server Options and return to the Enterprise Console.

Enterprise Server Options - Alert Type Settings



Alert Types section

The Alert Types settings are used in the Enterprise Console Devices panel to indicate the current status of any device.

Device Status (color/description/icon/flashing) is set to the alert type that has the highest priority of alerts raised for that device.

For example, a device that has ten alerts with a low status, five at medium status, two at high status and one at critical status is shown as being in Critical status in the devices panel of the Enterprise Console, as this is the highest priority.

Editing Alert Types

To edit an alert type:

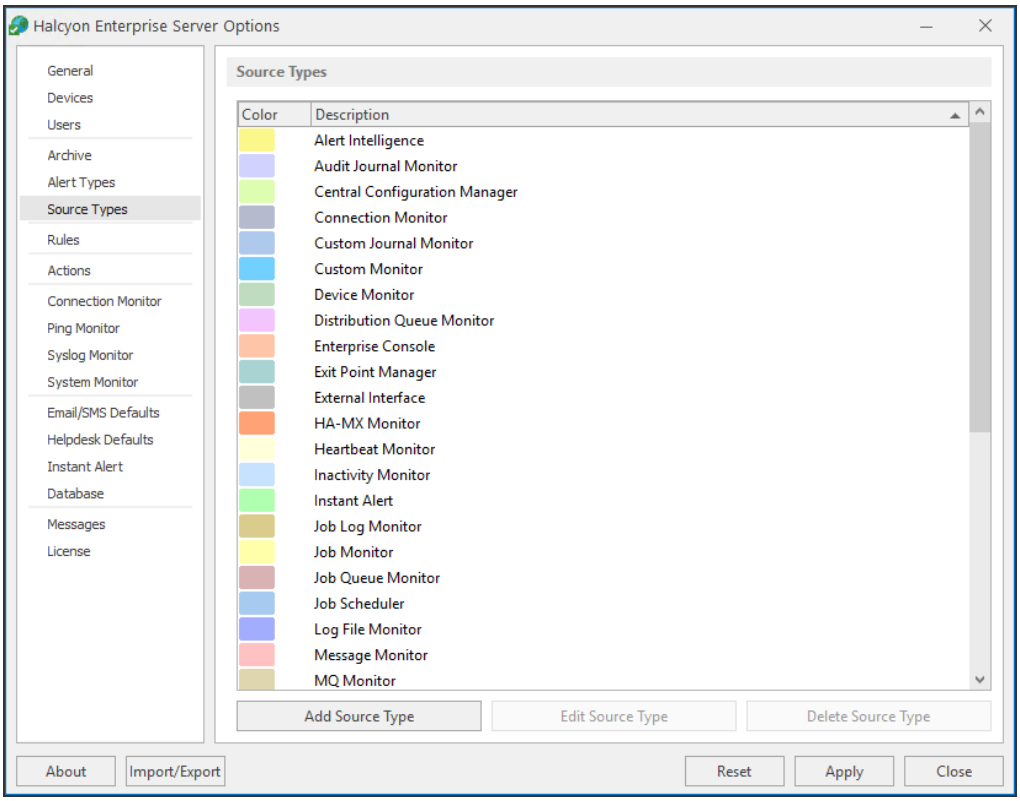
> **NOTE:** It is not possible to change either the Alert Type name or Alert Type icon.

1. Select the alert type from those listed so that it is highlighted.
2. Click **Edit Alert Type**. The Edit Alert Type [alert type name] dialog is displayed.
3. Change the Alert Type **Status Color** and/or over type the existing Alert Type **Status Text** entry.
4. Check **Flash** to have the **Alert Type** flash on and off repeatedly in the Enterprise Console display. See Enterprise Console Options - Flash Background.
5. Click **OK** to confirm and save.

Re-prioritizing alert types

The re-prioritizing of alert types can be achieved by single-clicking on an alert type from the list and using the **Move Up** and **Move Down** arrows to re-position it in the priority list.

Enterprise Server Options - Source Type settings



Source Types section

Source Types indicate the element of the network enterprise from which the alert was sent.

Options on the Source Types page allow you add, edit and delete Source Types.

The following Halcyon Source Types are included by default:

- Alert Intelligence*
- Audit Journal Monitor*
- Central Configuration Manager
- Connection Monitor
- Custom Journal Monitor*
- Custom Monitor*
- Device Monitor*
- Distribution Queue Monitor*
- Enterprise Console

- Exit Point Manager*
- External Interface
- HA-MX Monitor*
- Heartbeat Monitor**
- Inactivity Monitor*
- Instant Alert
- Job Log Monitor*
- Job Monitor*
- Job Queue Monitor*
- Job Scheduler*
- Message Monitor*
- MQ Monitor*
- Object Monitor*
- Output Queue Monitor*
- Performance Monitor*
- Ping Monitor
- Pool Monitor*
- Restricted Tasks Monitor*
- Server Manager
- Syslog Monitor
- System Monitor
- Task Supervisor*
- TCP/IP Monitor*
- Trap Receiver
- Unix/Open Systems
- Unknown
- User Profile Monitor*

Key:

* indicates a Halcyon IBM i source

** indicates a Halcyon IBM i Legacy source

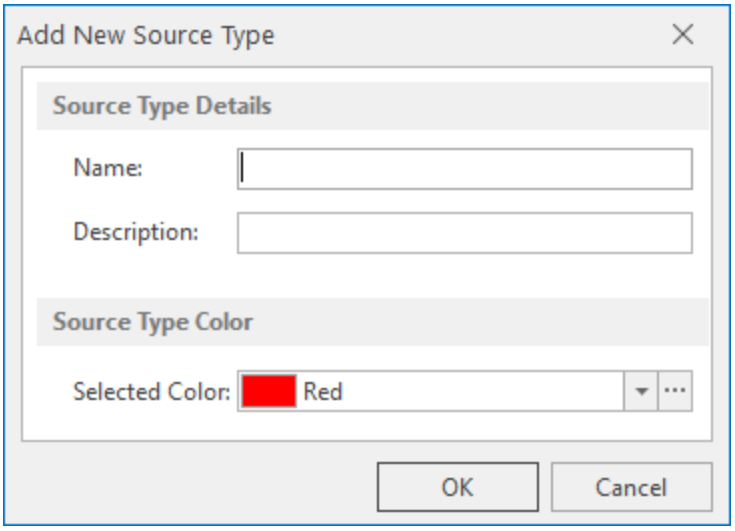
Working with Source Types

Adding a Source Type

Add a Source Type to create a new definition for a third party or in-house application from which you want to send alerts into the Enterprise Console.

To add a new source type:

1. Click **Add Source Type**. The **Add New Source Type** dialog is displayed.



2. Type the **Name** of the new Source Type.
3. Type a **Description** that accurately reflects the new Source Type.
4. From the drop-down menu list select a color by which the Source Type is displayed in the Enterprise Console. Click ... to open the **Color Editor** to access a greater range of colors.
5. Click **OK** to confirm and save the new Source Type.

Editing Source Types

Editing Source Types uses the same parameters as when adding Source Types (see the instructions above).

> **NOTE:** It is only possible to change the Description and Color settings of a Source Type.

Deleting Source Types

Use the **Delete Source Type** option to permanently remove a user-defined Source Type from the system.

1. Select the required user-defined Source Type and click **Delete Source Type**.
2. When prompted, click **Yes** to confirm the delete action.

> **NOTE:** It is not possible to delete a pre-defined Source Type.

Enterprise Server Options - Rules

Rules are the means by which the devices on a network are monitored to ensure compliance with operating procedures.

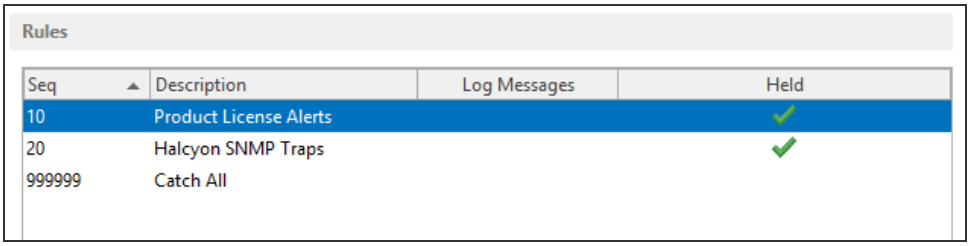
Rules monitor for messages or events across the network and specify what action to take should any specific message or event occur.

In order to be valid a rule must have a description, defined criteria and at least one action applied in the event that the criteria is met.

Options on the Rules page allow the adding, editing, deletion and holding/releasing of rules.

Details of rule settings are available to view in the alert details panel of the Enterprise Console, for any alert generated by the respective rule.

Summary details of currently defined rules and rule sequence numbers are displayed in a four-column table.



Sequence (Seq)

The sequence number of the rule. This number defines the order in which rules are examined when a new alert is received.

Description

The user-defined, textual description of the rule.

Log Messages

A ‘Yes’ in this column indicates which rule messages are logged. When rule messages are not logged, the cell is left empty.

Held

This column indicates which rules are Held by displaying a ✔ tick mark. When rules are not held (released), the corresponding cell is left empty.

Default Rules

There are three default rules that are shipped with the software.

- **Product License Alerts**: An alert is generated if any message from the Enterprise Console is found to contain 'license' in the text. This is to forewarn administrators of any impending license expiry. This rule is held by default.
- **Halcyon SNMP Traps**: An alert is generated if any message from the Trap Receiver is received. This rule is held by default.
- **Catch All**: This rule is provided as a method of catching any message generated from any source. This rule is created with the highest possible sequence number. This means that any rules created above this one are run first, but in case any event or scenario has not been captured in the preceding rules, this acts as a 'catch-all' to ensure no event is missed. This rule is released by default.

Sorting columns

Column order can be rearranged by left-clicking on a column heading and keeping the mouse button depressed, dragging the column to the new position and releasing the button. Information in each column can be sorted in ascending or descending order by clicking on each column title to change the sequence.

Holding/Releasing Rules

The **Hold/Release Rule** button allows selected rules in the Rules panel to be held, preventing them from generating alerts or to be released from the held status.

Held rules are not checked against any new matching criteria found by the system and remain held until released (even if the application is restarted).

To hold a rule:

1. From the **Rules** panel, select a rule that is currently not in a held status. Multiple selections can be included on one action but all rules must be currently active.
2. Click **Hold Rule**.

The rule is now held as indicated by the ☑ tick mark in the **Held** column of the **Rules** panel. No alerts are generated from this rule while it remains in Held status.

To release a rule:

1. From the **Rules** panel, select a rule that is currently in held status as indicated by the ☑ tick mark in the **Held** column. Multiple selections can be included on one action, but all rules must be in held status.
2. Click **Release Rule**.

The rule is now released and alerts will be generated for any instances where the rule criteria are met.

Copying Rules

Copying a rule is a quick way of creating a new rule with many required attributes already in place, meaning only one or two adjustments are needed to create a unique rule.

To copy a rule:

1. From the **Rules** panel, select the rule to be copied with a single-click so that it is highlighted.
2. Right-click on the rule and select **Copy Rule** from the pop-up menu. The **Add New Rule** dialog is displayed
3. Click **OK** to produce an exact copy of the existing rule (labeled as 'Copy of...' in the Rules section of the Rule page)

Deleting Rules

Deleting a rule removes it from the system so that it can no longer generate alerts.

To delete a rule:

1. From the **Rules** panel, select the rule to be deleted. Multiple selections can be included in one action.
2. Click **Delete**.
3. When prompted, confirm the Delete action.

The rule is now deleted and removed from the system.

Adding and Editing Rules

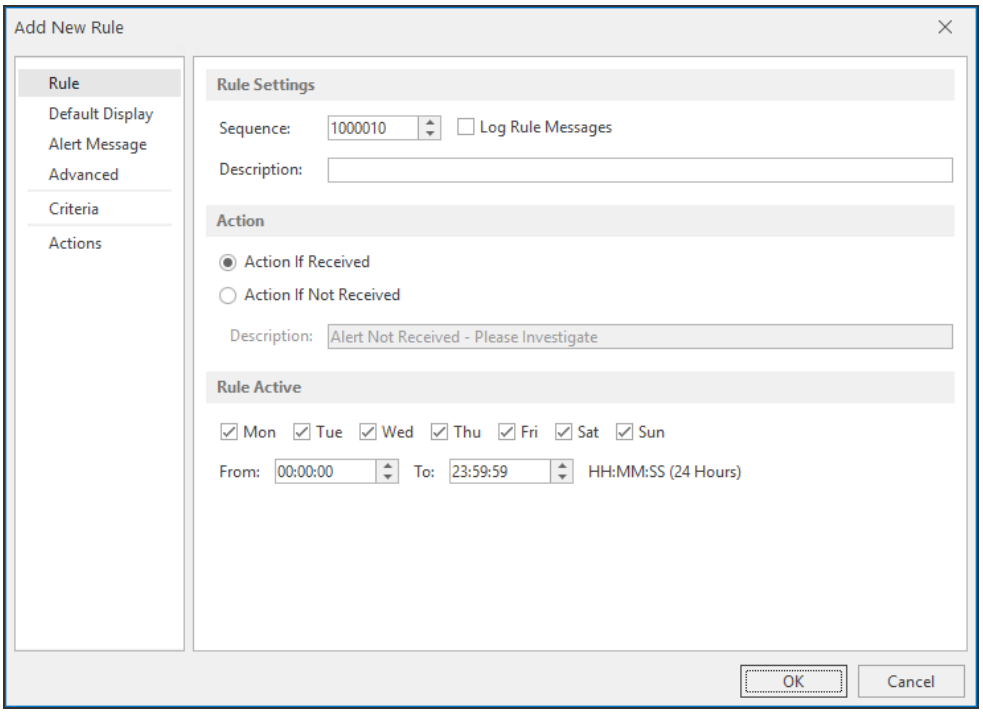
Adding or Editing Rules provides access to a series of dialogs and options used to capture any important events that do (or do not) occur. The dialogs are the same regardless of whether you are adding or editing a rule.

> **NOTE:** In the following text '**Add**' is interchangeable with '**Edit**'.

> TIP: This section assists with the first four tabs used when adding a rule. See also Adding rule criteria and Rule actions for assistance when using these two pages.

To Add a Rule:

1. From the Enterprise Server Options Rules page, click **Add Rule**. The **Add New Rule** dialog is displayed.



There are six pages available:

> **NOTE:** Only the first four pages are covered here. See the Criteria and Actions pages for the last two pages used when adding rules.

Rule Tab - Rule

The settings in this panel are used to determine sequence, action processing and activity of the rule.

Rule Settings section

Sequence

The setting in this field defines the order in which rules are examined. Enter a unique sequence number to specify the sequence position of the rule. Identical sequence numbers are automatically prevented from entry.

Log Rule Messages

Check this box if to identify whether rule is performing as expected. By selecting this option, diagnostic messages are written to the Message Log File . Note that both the **Save to Log File** and **Log Diagnostic Messages** options must be selected).

> **NOTE:** All log files are saved with an extension of .hlf. to %Program Data%\Halcyon\Enterprise Server Options\Logs

Description

Type a descriptive text for the new rule. This could be a summary of what the rule's intended use, for example; Warnings Received - Weekends Only.

Action settings section

The fields in this section define what happens if an alert is or is not received.

Action if Alert Received

If this option is selected, action is taken if an alert generated by this rule is received within the Rule Active time range specified below.

Action if Alert Not Received

If this option is selected, action is taken if an alert generated by this rule is not received within the Rule Active time range specified. This option is recommended for time critical jobs.

Error Text

Enter the text of the message that is generated for a rule that has the **Action If Alert Not Received** option enabled.

Rule Active settings

Mon-Sun

Specifies on which days the rule is active. Click on a day to select or deselect as required. The default setting is active every day.

From - To

Specifies a time range between which the monitor should scan for events matching this rule sequence. Hours can span over midnight, for example, 22.00 - 03.00 hours.

Rule Tab - Default Display

These settings configure the default panel, alert type, background and font colors for alerts that have been processed against this rule for display purposes in the Enterprise Console.

Alert Display Settings section

The fields in this section define the level at which the alert is raised. By default, alerts generated by rules are raised at **Information - Low** level.

Override Alert Type

Check this box to enable the display of an alternative alert type when an alert is triggered by the rule.

Once enabled, use the drop-down menu to select an alternative alert type.

Background Color section

This section allows you to determine the background color of any alert messages raised by this rule. Only one option is allowed.

Default Background Color

This setting keeps the default background color of the alert as defined in the Enterprise Console | Appearance | Alert Status Colors option.

Device Background Color

This setting keeps the default background color of the device as defined in **Device Manager** | **Add Device** | **Display** | Color option.

Selected Color

Specify a color as the background color of any alert messages raised by this rule.

> **NOTE:** Click ... to browse for a color that is not available in the color list.

Flash Background Color

Select this option to flash the background color of the alert raised by this rule when it is displayed in the Enterprise Console.

Font Color section

The fields in this section determine the font color of any alert messages raised by this rule. Only one option is allowed.

Default Font Color

This setting retains the default font color of black.

Selected Font Color

Specify a color as the font color used in any alert messages raised by this rule.

> **NOTE:** Click ... to browse for a color that is not available in the color list.

Rule tab – Alert Message

The Alert Message page is used to provide alternative text details for alerts, providing greater clarity and meaning to the alert when received.

> **NOTE:** The actual alert information remains the same so that any matching rule information is captured prior to the text being changed.

Alert Message settings

Message

Enter free text and/or use the Alert, Device and Details variables (as displayed) to generate alternative text once matching rule criteria has been proven.

An example of the current alert message text convention is displayed in the **Example** field.

Within Enterprise Console, substitution variables are listed as hyperlinks. Click on the blue text of a substitution variable to select and insert in the **Message** field at the current cursor position.

> **TIP:** When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

Using Pipes with Alert Text

Alert text can be reformatted by using pipes to change the number of decimal places reported, remove white space and so on.

For example, to change the text of an alert reporting a numerical value of 1784.238175 so that it only reports two decimal places, use the parameter &N|p2|; resulting in the alert text changing to 1784.24.

> **NOTE:** For a full list of available parameters see Substitution Variable String Parameters. and Substitution Variable Numeric Parameters.

Rules Tab - Advanced

The Advanced settings define the method of counting alerts from this rule and the processing settings applied.

Rule Count Method settings

Alert Count Method

This specifies the method by which alerts raised by this rule are counted.

- **Rule** The standard rule counter is incremented each time an alert is processed against this rule regardless of the alert's source or text.
- **Source** A distinct source counter is incremented each time an alert is processed against this rule depending on the alert's source.
- **Text** A distinct text counter is incremented depending on the alert's message text.

EXAMPLE: **Alert Count Examples**
Assume the following actions have been defined:

Seq	Action	Perform Action For	Action Type
10	Action 1	1 Alert	Change Display Settings
20	Action 2	1 Alert	Send Email
30	Action 3	1 Alert	Send SNMP Trap

Assume the following alerts have been received:

Time	Alert Message Text	Alert Source
10:00	Test Alert 1	Server Manager
10:05	Test Alert 2	Message Monitor
10:10	Test Alert 2	Message Monitor

If the **Alert Count Method** is **Rule** then:

- Action 1 will be performed against the alert '10:00 Test Alert 1' (Rule Counter=1)
- Action 2 will be performed against the alert '10:05 Test Alert 2' (Rule Counter=2)
- Action 3 will be performed against the alert '10:10 Test Alert 1' (Rule Counter=3)

If the **Alert Count Method** is **Source** then:

- Action 1 will be performed against the alert '10:00 Test Alert 1' (Server Manager Counter=1)
- Action 1 will be performed against the alert '10:05 Test Alert 2' (Message Monitor Counter=1)
- Action 2 will be performed against the alert '10:10 Test Alert 1' (Message Monitor Counter=2)

If the **Alert Count Method** is **Text** then:

- Action 1 will be performed against the alert '10:00 Test Alert 1' (Test Alert 1 Counter=1)
- Action 1 will be performed against the alert '10:05 Test Alert 2' (Test Alert 2 Counter=1)
- Action 2 will be performed against the alert '10:10 Test Alert 1' (Test Alert 1 Counter=2)

Rule Processing settings

These settings suspend the rule according to the options defined below. It is good practice to use these options to prevent multiple alerts of the same message being delivered:

Automatically Suspend Rule

Check to enable the Rule Suspension options.

Until Triggered X Times

Specify how many times the rule is triggered before it is activated. The count can also be within a time frame.

Within x Minutes

Adds a time limit to the Until Triggered x Times option.

For x Minutes When Triggered x Times

Defines how many minutes the rule is suspended for after it has been triggered a (user) specified number of times.

Reset Counters on Startup

Check this option to reset these counters on a restart of Enterprise Console. if left blank, the counters continue to accrue from their last position when the Enterprise Console was closed.

Reporting settings

> **NOTE:** This option is only visible if a license has been included for Reporting in this instance of Enterprise Console. Please contact halcyon.sales.admin@fortra.com for assistance should you require access to the reporting function.

Capture Reporting Data

Check this option to enable the capture of reporting data from this rule. Any activity generated by this rule will then be written to the database from where it can be accessed by Advanced Reporting Suite to be included in one of the many available reporting templates.

> **NOTE:** A separate license is required for Advanced Reporting Suite in order to access this data.

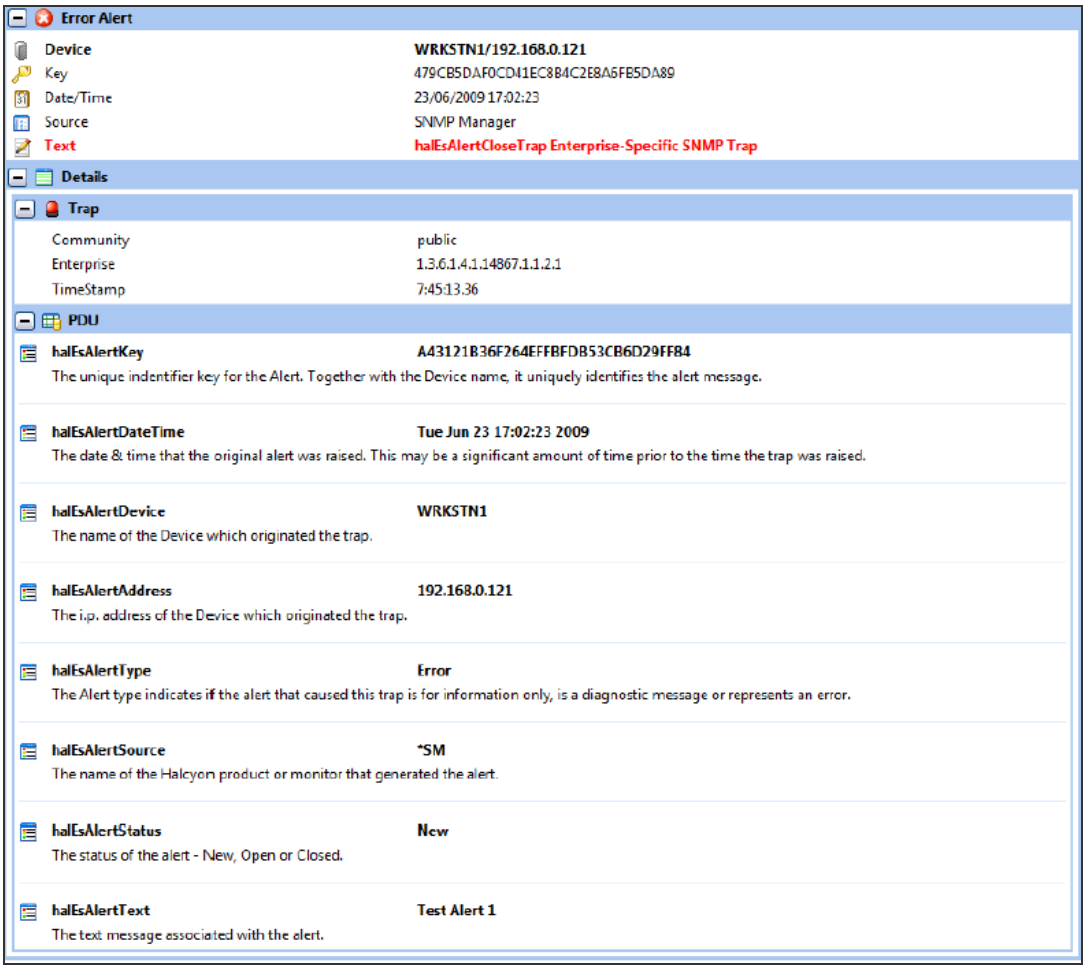
The Criteria and Actions pages are covered in their own sections.

Using Substitution Variables with Alert Detail information

For alerts that generate detail information (such as SNMP Traps), use the **&DetailsName** variable to replace any entry in the left hand column of the details section of the Alert Detail (as viewed by double-clicking the alert within Enterprise Console) with the corresponding entry in the right hand column.

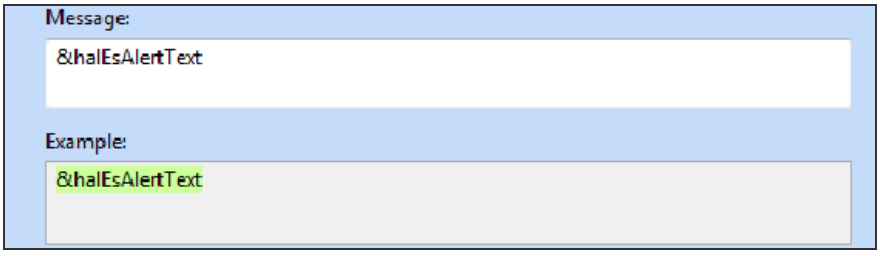
This feature is particularly useful when used for SNMP trap alerts as the Enterprise Console has no automatic way of recognizing which object in the trap payload actually represents the error message.

For example, in the SNMP Trap example below:

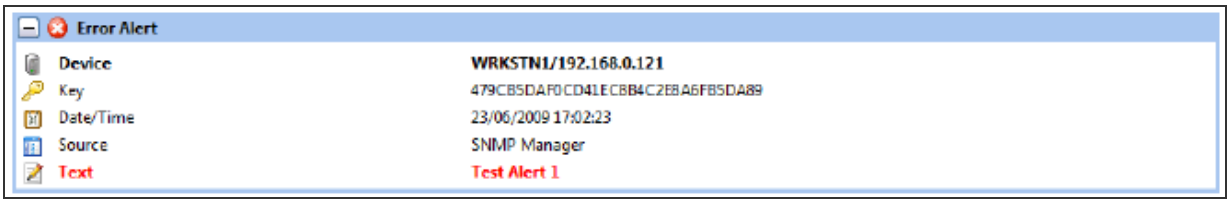


The trap payload is shown in the details section headed PDU. The payload contains a list of objects (left-hand side) and a corresponding value (right-hand side).

Any one of these PDU values can be used in the alert text by using the object name as a substitution variable. For the purpose of this example, the PDU value ‘halEsAlertText’ is used:



When the trap is received, software scans the payload looking for an object with the same name as the variable. If found, it inserts the corresponding value into the alert text (in this case; ‘Test Alert 1’).

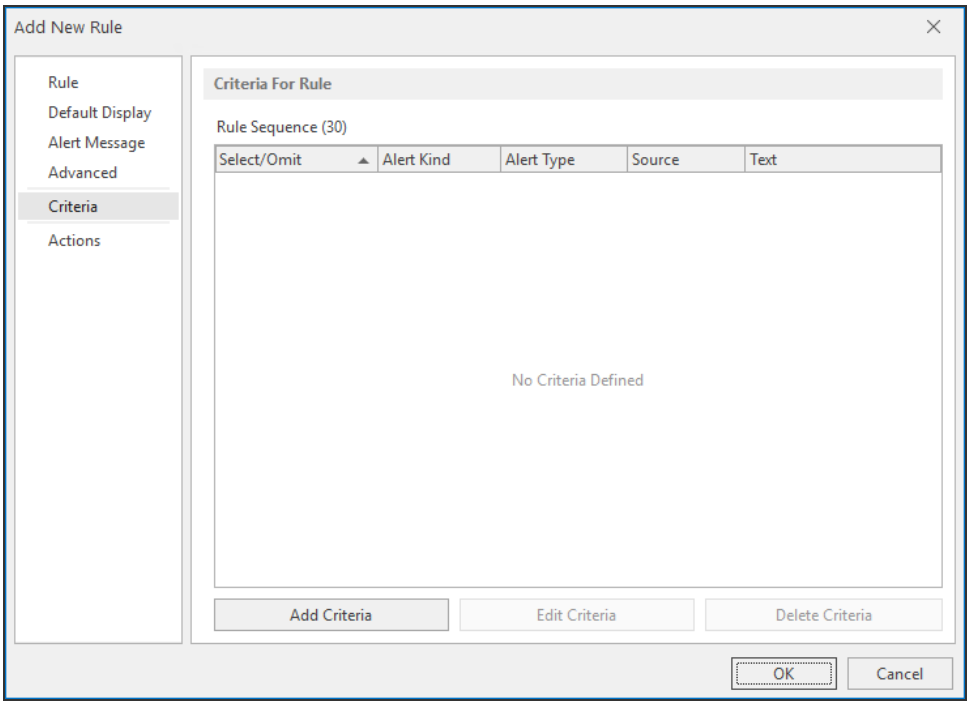


NOTE: If this option is used with common or frequently occurring message text, be sure to specify other criteria to ensure that the alert message generated is correct for the actual alert received.

Adding and Editing Rule Criteria

Options on the **Add New Rule/Edit Rule Criteria** page define rule selection criteria. These are the qualifications that the rule must meet if an alert is to be raised.

Summary details of rule criteria are displayed in a five-column table:



Select/Omit

Displays whether the criteria is selected or omitted from the rule.

Alert Kind

Displays the kind of alert that is raised by the rule criteria.

Alert Type

Displays the type of alert raised by the rule criteria.

Source

Displays the source device that is being monitored by the rule criteria.

Text

Displays the text used in the event that the rule criteria generates an alert.

Sorting columns

Column order can be rearranged by left-clicking on a column heading and keeping the mouse button depressed, dragging the column to the new position and releasing the button. Information in each column can be sorted in ascending or descending order by clicking on each column title to change the sequence.

Adding Criteria

Rule criteria is added in the **Add New Criteria** dialog and edited in the **Edit Criteria** dialog. These dialogs are displayed by clicking **Add Criteria** or **Edit Criteria** (edit is enabled for any selected items displayed in the table). Options on both dialogs are identical.

Click **Add Criteria** to create a new selection criterion for the rule. Multiple criteria can be specified for a single rule.

Criteria tab - Criteria

Criteria Details section

Criteria Type

Choose whether to select or omit this rule from action processing.

- **Select**: Check this option to include this rule for action processing.
- **Omit**: Check this option to exclude this rule from action processing. Events matching similar criteria in other rules may still be selected for processing.

Alert Kind

Choose the kind of alert that is raised for this rule.

- **Inquiry**: These are alerts that usually require some form of action to be taken on the part of the user.
- **Information**: These are alerts that are raised and provide information to the user
- **Both**: Both kinds of alert are raised. This is the default setting.

Alert Type

Define the alert type level for this rule based on selected conditional parameters (equals, less than, greater than, etc.). Priority is taken from the Alert Type table on the - Alert Settings page.

EXAMPLE: (assuming default alert type priority has been kept):

Parameter	Alert Type	Result
=	Any Type	All Alert Types are selected
>	Error	All alert types with a higher priority of error are selected
=	Critical	Only critical alerts are selected

Source Type

Define the source type based on conditional parameters (equal to, not equal to).

EXAMPLE:

Parameter	Source Type	Result
=	Any Type	All Source Types are selected
<>	Ping Monitor	All Source Types except Ping Monitor are selected
=	Ping Monitor	Only the Ping Monitor Source Type is selected

Alert Text

Enter the alert text based on conditional parameters (equals, less than, greater than, etc.). Wildcard characters can be used when defining the 'Alert Text'. This option is selected via the drop-down list.

Search Text From Position ... For ... Characters

Allows the fine tuning of the search for specific alert text by specifying a starting position from which to search and for a specified number of characters.

Alert Details section

The Alert Details section is used to set textual information for alerts raised by the rule criteria.

Details Text

Define the details text. This can be generic or free text and can also use specific textual values that vary depending on the type of alert rule that is being defined. Wildcard characters can be used when defining this text.

> **NOTE:** See the following for more information regarding alert detail for specific alerts:
>
> - Setting Alert Detail Criteria for IBM i Alerts
> - Setting Alert Detail Criteria for Server Manager Alerts
> - Setting Alert Detail Criteria for SNMP Trap Alerts
> - Setting Alert Detail Criteria for Syslog Messages

Details Value

Define the details value based on conditional parameters (equals, less than, greater than, etc.) when used in combination with entry in the **Details Text** field. Wildcard characters can be used when defining the details value.

Wildcard Characters settings

The wildcard characters area is used to define characters which are then used as substitutes for search spans or single characters.

Use ... As A Substitute For Zero or more Characters

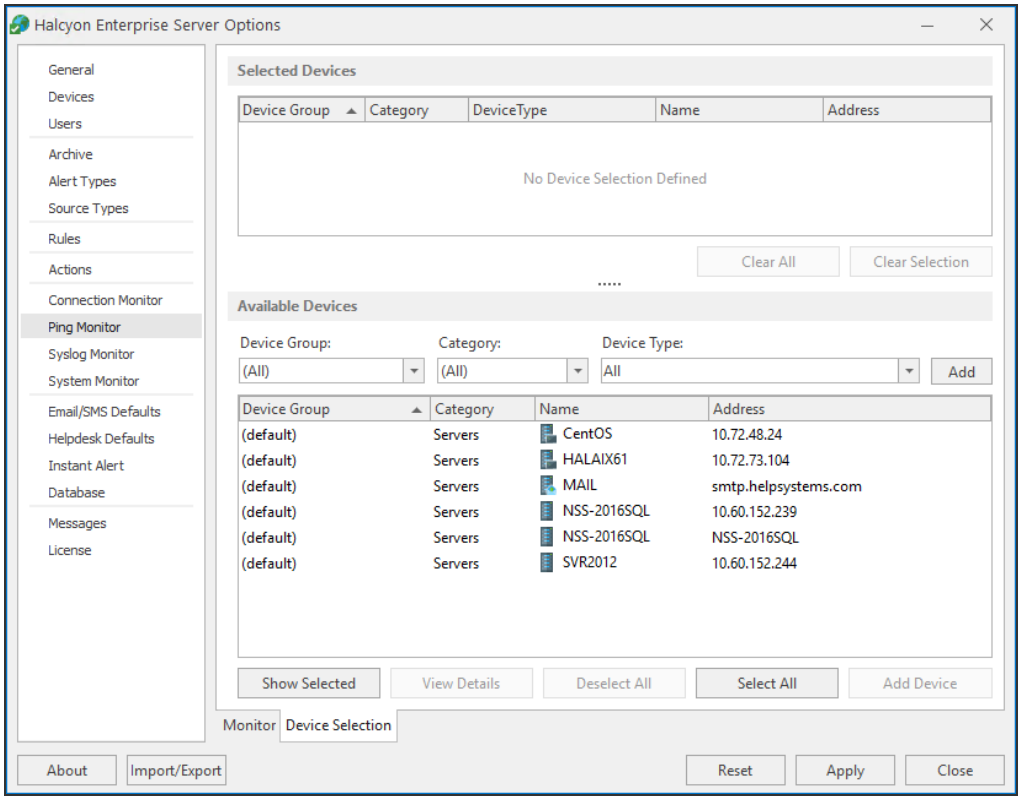
Enter the character to use as a substitute for this search span. '*' is defined as the default search span character.

Use ... As A Substitute For A Single Character

Enter the character to use as a substitute for a single character. '?' is defined as the default single wildcard character.

Device Selection tab

The **Device Selection** tab is used to select the Devices to which the monitor connects and raises alerts if the success percentage figure is not attained.



Selected Devices section

This section shows the devices that are currently selected for use with the monitor. When this tab is opened for the first time, this section is empty.

Information is listed in five columns:

- **Device Group**: Displays the name of the Device Group to which the device belongs.
- **Category**: Displays the category in which the device is defined.
- **Device Type**: Displays the Device Type of the device.
- **Name**: Displays the name of the device.
- **Address**: Displays the IP Address or Host name of the device.

Clear All

Click **Clear All** to remove all of the currently selected devices from selection.

Clear Selection

Highlight a device in the **Selected Devices** section and click **Clear Selection** to remove this device from selection. Multiple devices may be selected in one action.

Sorting columns

Column order can be rearranged by left-clicking on a column heading and keeping the mouse button depressed, dragging the column to the new position and releasing the button. Information in each column can be sorted in ascending or descending order by clicking on each column title to change the sequence.

Available Devices section

This section lists all of the devices that have been defined in Device Manager.

Filter options

These options allow the filtering of available devices on the network in order to restrict the list of available devices to just those that meet the filter criteria.

The categories comprise:

- **Device Group**: Device groups are collections of similar devices, such as all those that belong to a specific department. Device groups are set up and maintained in Device Manager
- **Category**: Devices, such as servers that can be divided into specific types. Items listed here are by default. No other items can be added to this list.

- **Device Type**: Device types, such as proxy servers are listed on this drop down and comprise a mix of default items and any other items identified on the network, which are automatically added to this list.

Add Device

To load a device into the **Selected Devices** section of this page, select the required device in the **Available Devices** section and click **Add Device** to move it into the **Selected Devices** section.

Show/Hide Selected

Click to show in the **Available Devices** section, only those devices not already listed in the **Selected Devices** table. This avoids duplicating device information in both tables. Click again to show all available devices, including those that have already been selected.

View Details

This button is used to open the **View Device** dialog, which displays the attributes of a selected device. No amendments can be made on this display. If changes are required, use Edit Device in Device Manager.

Deselect All

Click to deselect all of the currently selected devices in the **Available Devices** section.

Select All

Click to select all of the devices listed in the **Available Devices** section.

Click **OK** to apply the criteria to this rule.

Setting Alert Detail Criteria for IBM i Alerts

When setting alert detail criteria for alerts originating from IBM i devices, specific string and integer values can be set.

String Values

The following string values are valid when entering textual details for alerts originating from IBM i devices:

- Message ID
- Message Queue
- Message File
- Program
- System
- User
- Number

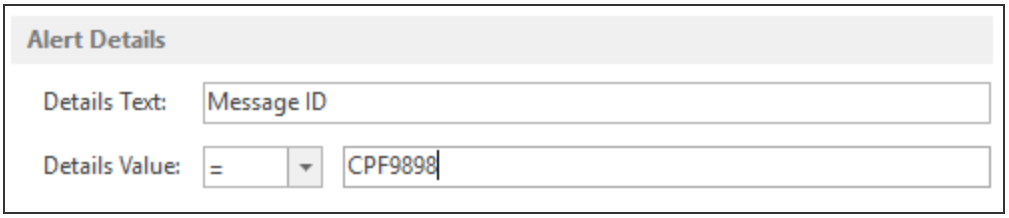
With string values, only operators '=' and '<>' are used. Other operators can be used, but note that unexpected results may be generated.

Textual Details Value

Entries should match the entry in the Details Text field together with the selected operator.

EXAMPLE: To specify alert detail criteria for a specific message ID, you may enter something similar to:

- **Details Text**: Message ID
- **Details Value**: = CPF9898



An alert is generated for any IBM i Message ID of CPF9898, that also passes other specified criteria.

Integer Values

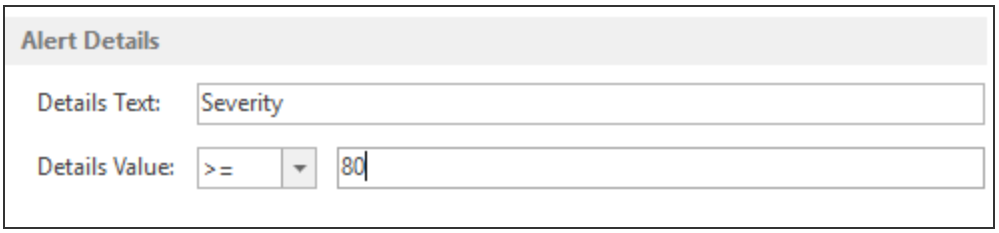
The following integer values are valid when entering Details Text for alerts originating from IBM i devices:

- Severity
- Rule Sequence
- Selection Sequence

All operators can be applied to integer values.

EXAMPLE: An example of specifying alert detail criteria, with an integer value, for an IBM i alert may be similar to:

- **Details Text**: Severity
- **Details Value**: >= 80



An alert is generated for any IBM i message with a severity of greater than or equal to 80, that also passes other specified criteria.

Setting Alert Detail Criteria For Server Manager Alerts

When setting alert detail criteria for alerts originating from the Server Manager, specific string values can be set.

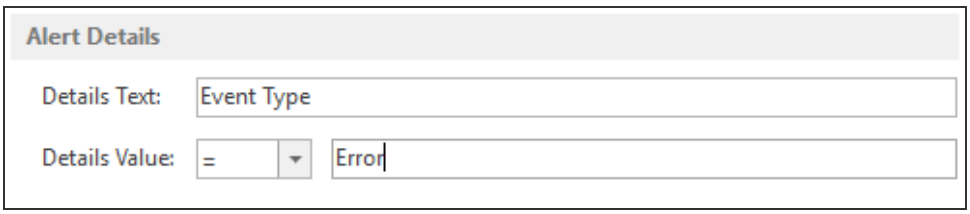
String Values

The following values are valid when entering Details Text for Server Manager alerts. The operator value is usually set to equal to '='.

Details Text	Valid Details Value
Event Type	Error, Audit Success, Information, Warning
Source	Halcyon SNMP Manager
Category	No specific value required
Event ID	Any valid Event ID number
User	No specific value required
Message	Any valid message is displayed in the Windows Event Log. The use of wildcards is recommended.

EXAMPLE: Examples of specifying alert detail criteria for Server Manager alerts may be similar to:

- **Details Text**: Event Type
- **Details Value**: = Error
- **Details Text**: Event ID
- **Details Value**: = 125
- **Details Text**: Message
- **Details Value**: = *Service: esInterface failed: NetMan*



In the above example, an alert is generated for any Server Manager Event Type with a value of error, that also passes other specified criteria.

Setting Alert Detail Criteria for SNMP Trap Alerts

Alert detail criteria for SNMP trap alerts can be specified in one of two ways, dependent on whether the incoming trap has been assigned with a valid MIB definition, instead of the basic OID value. Operator values are usually set to equals '='.

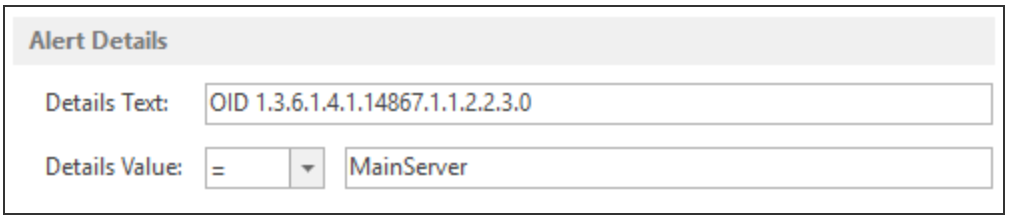
Therefore, the alert detail text for SNMP Trap alerts can be specified in a similar way as follows:

With a MIB definition:

- Details Text: halEsAlertDeviceName
- Details Value: = MainServer

With an OID definition:

- Details Text: OID 1.3.6.1.4.1.14867.1.1.2.2.3.0
- Details Value: = MainServer



In the above example, an alert is generated for SNMP Trap OID 1.3.6.1.4.1.14867.1.1.2.2.3.0 with a value of MainServer, that also passes other specified criteria.

Each trap entry has an associated type, such as ASN1_OCTSTR or ASN1_INT. Types ASN1_INT, ASN1_COUNTER, ASN_GAUGE and ASN1_TIMETICKS are converted to integer values and all operators can therefore apply.

Setting Alert Detail Criteria for Syslog Messages

When setting alert detail criteria for alerts originating from Syslog messages, specific string values can be set.

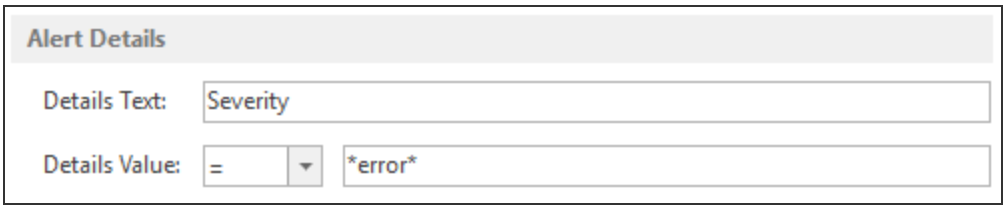
String Values

The following values are valid when entering Details Text for Syslog message alerts. The operator value is usually set to equals ('=').

Details Text	Valid Details Value
Facility	*user*
Severity	*error*
Raw Text	*This is a test message (Raw Text is the actual message that is received prior to formatting)

EXAMPLE: Examples of specifying alert detail criteria for Syslog messages may be similar to:

- **Details Text**: Facility
- **Details Value**: =*user*
- **Details Text**: Severity
- **Details Value**: =*error*



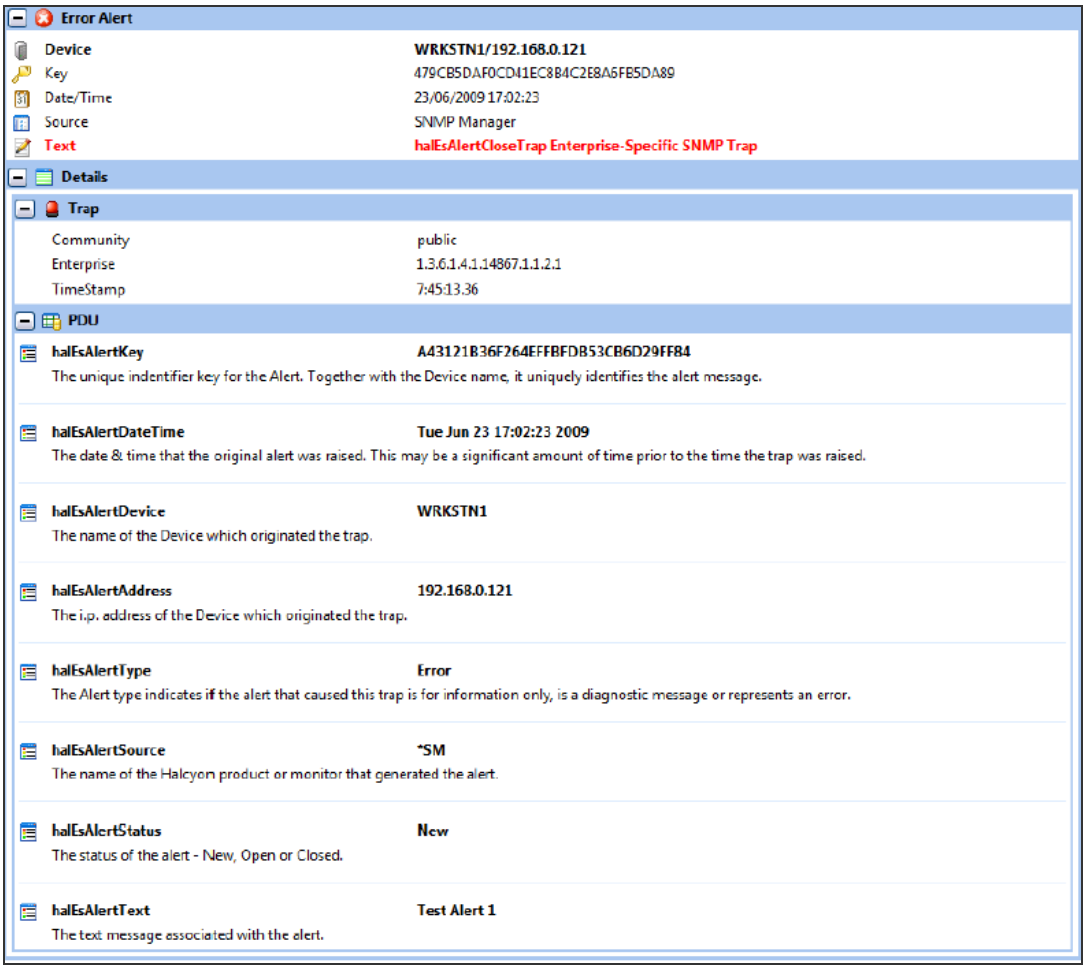
In the above example , an alert is generated for any Syslog Message Severity message with a value of *error*, that also meets other specified criteria.

Using Substitution Variables with Alert Detail information

For alerts that generate detail information (such as SNMP Traps), use the **&DetailsName** variable to replace any entry in the left hand column of the details section of the Alert Detail (as viewed by double-clicking the alert within Enterprise Console) with the corresponding entry in the right hand column.

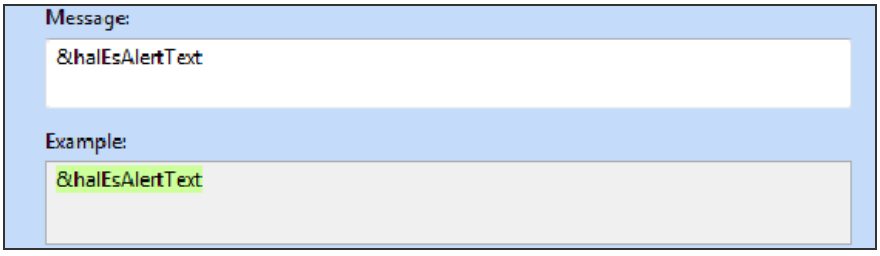
This feature is particularly useful when used for SNMP trap alerts as the Enterprise Console has no automatic way of recognizing which object in the trap payload actually represents the error message.

For example, in the SNMP Trap example below:

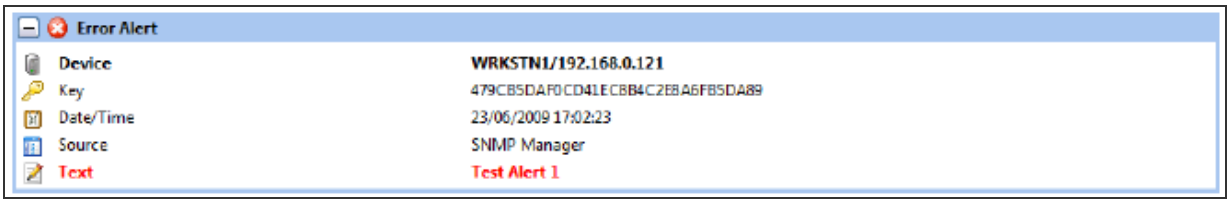


The trap payload is shown in the details section headed PDU. The payload contains a list of objects (left-hand side) and a corresponding value (right-hand side).

Any one of these PDU values can be used in the alert text by using the object name as a substitution variable. For the purpose of this example, the PDU value ‘halEsAlertText’ is used:



When the trap is received, software scans the payload looking for an object with the same name as the variable. If found, it inserts the corresponding value into the alert text (in this case; ‘Test Alert 1’).



NOTE: If this option is used with common or frequently occurring message text, be sure to specify other criteria to ensure that the alert message generated is correct for the actual alert received.

Setting Alert Detail Criteria for SNMP Trap Alerts

Alert detail criteria for SNMP trap alerts can be specified in one of two ways, dependent on whether the incoming trap has been assigned with a valid MIB definition, instead of the basic OID value. Operator values are usually set to equals '='.

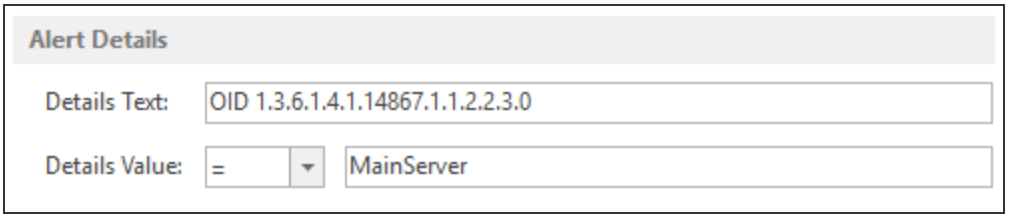
Therefore, the alert detail text for SNMP Trap alerts can be specified in a similar way as follows:

With a MIB definition:

- Details Text: halEsAlertDeviceName
- Details Value: = MainServer

With an OID definition:

- Details Text: OID 1.3.6.1.4.1.14867.1.1.2.2.3.0
- Details Value: = MainServer



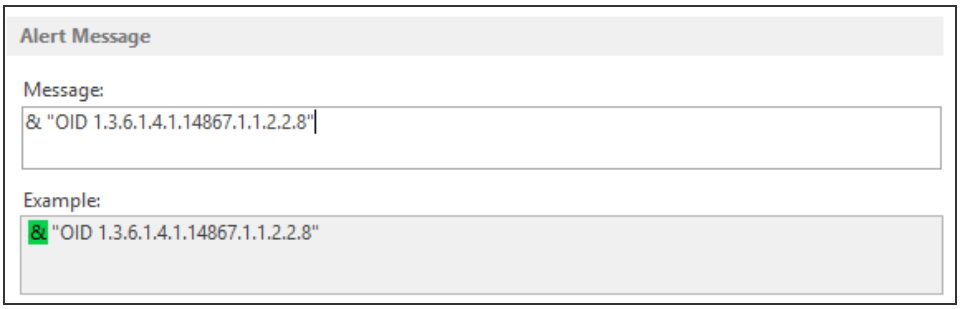
In the above example, an alert is generated for SNMP Trap OID 1.3.6.1.4.1.14867.1.1.2.2.3.0 with a value of MainServer, that also passes other specified criteria.

Each trap entry has an associated type, such as ASN1_OCTSTR or ASN1_INT. Types ASN1_INT, ASN1_COUNTER, ASN_GAUGE and ASN1_TIMETICKS are converted to integer values and all operators can therefore apply.

Using Substitution Variables with SNMP OID information

A matching SNMP MIB (Management Information Base) file can be used to map SNMP OIDs to object names. However, without the MIB data, the incoming trap would have been displayed as a series of unique numbers such as: OID 1.3.6.1.4.1.14867.1.1.2.2.8.

If there is no MIB available for the SNMP trap being received, it is possible to use substitution variables to override the alert text by specifying the unique OID number as the variable name as shown in the screen shot below.



> **NOTE:** When using any variable that contains a space, such as OID information, ensure that the variable text is enclosed in quotation marks.

To decide on the information that should be captured in order to get the most meaningful results in the alert text, setup a test rule first and see what is generated. From this information, it is possible to then determine the details to be captured and set the substitution variables accordingly.

> **NOTE:** For more information on using Substitution Variables within Enterprise Console, see Working with Substitution Variables.

Creating a Rule for IBM i Message ID Specific Events

There are many different events that are automatically generated if a specific event occurs during the day-to-day operation of the IBM i.

This section shows how to create a rule that monitors and reports to the Enterprise Console on a specific or any generic messages raised.

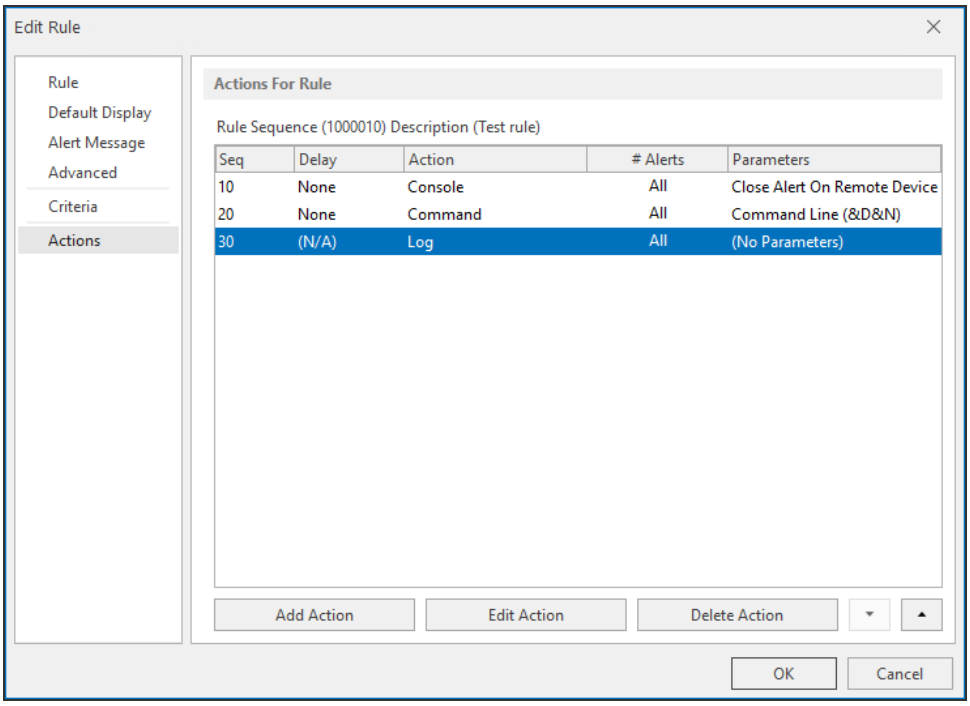
To create a rule for Message ID Specific Events:

1. From Windows Start select **Programs** | **Halcyon** | Enterprise Server Options.
2. Select the **Rules** tab and click **Add Rule**.
3. Keep all defaults and enter a **Description** for the new rule.
4. Select the **Criteria** tab and click **Add Criteria**.
5. Enter **Message ID** in the **Details Text** field.
6. Select the Details Value operand as '**=**' and enter either the specific message ID of the message on which you wish to filter or use the wildcard symbols '*****' and '**?**' to filter for generic message ID's.
7. Select the **Device Selection** option.
8. Select the Devices from which you wish to receive details of any messages. Click **OK**.
9. Select the **Actions** tab and click **Add Action**.
10. From the drop-down menu choice select **Send Console Action** as the Action Type.
11. Click **OK** to add the Action.
12. Click **OK** again to add the Rule.
13. Click **Apply** to save the settings.

Rules Tab - Actions

The options on the (**Add New Rule** | **Edit Rule** dialog) **Actions** page define rule actions. Any number of actions can be defined for each rule and these actions are processed in order if the rule selection criteria match the alert.

Action details are displayed in a five-column table (Seq, Delay, Action, #Alerts and Parameters).



Sequence (Seq)

Displays the sequence number assigned to each action. See Escalating the priority of Pending Alerts for information on how action sequence numbers are used.

Delay

Displays the time delay before this action is processed.

Action

Displays the name of the action to be processed.

#Alerts

Displays the number of alerts for which this action is processed.

Parameters

Displays the action that will be taken.

Display

Actions are added and edited in the **Action Detail For...** dialog. This dialog is displayed by clicking **Add Action** or **Edit Action** (edit is enabled for any selected items displayed in the table).

> **NOTE:** The dialog title includes the actual name of the Action Type which is user-selected from the Action Type: drop-down list.

Escalating the priority of Pending Alerts

Actions are listed in the **Actions For Rule** table by priority of sequence number and within each action sequence group, the time delay specified.

Actions within each sequence group can be escalated individually, by selecting an action and clicking the up and down arrows to reposition the action in the table.

Actions can only be prioritized individually; it is not possible to prioritize multiple actions simultaneously.

> **WARNING:** It is important to be aware that escalating or de-escalating the priority of any action also affects subsequent relationships between actions (within the same sequence).

Add Action For [Action]

Click **Add Action** to open the **Add Action For...(Action)** dialog.

Action Sequence

Either directly type or use the choice buttons to select the action sequence number required.

This sequence number does not have to be unique. If there are two or more sequence numbers with the same value, all actions are executed for the particular occurrence of that alert.

> **EXAMPLE:** If an alert is received which requires a command to execute and a log to be written every time, both actions would be assigned the same sequence number so both actions are executed for the same alert.

Action Type

Action types are selected from the **Action Type** drop-down menu.

When an action type is selected, an additional page is added to the navigation pane (except for Log Only, Play Sound at Console and Purge Alert actions). The additional options on these pages define parameters specific to the Action Type selected.

The following action types can be selected:

Action Selected	Action Description	Additional Page Option Displayed
Change Display Settings	Changes Enterprise Console display settings for received alerts	**Display** page: Options on this page are detailed within Default Display
Execute Command	Executes a command when an alert is generated	**Command** page: Enter the command that is run when the action is triggered
Forward Alert	Forwards all alerts raised by the rule to another instance of Enterprise Server. Forwarded alerts are displayed with an additional icon and extended information in the alerts panel of Enterprise Console	**Forward** page: Options on this page define the server to which the alerts are forwarded. Routing information is defined as per device or device group in Device Manager. If an alert is forwarded from a device that does not currently exist in the receiving server device list, a temporary device is added until the alert is closed. If an alert is received from an IBM i device and then forwarded onto another console, the receiving console must have the routing information of the forwarding device in order that a reply can be sent back to the IBM i device.
Hold Alert Rule	Holds the specified rule and prevents it being selected for action	**Rule** page: This page allows the selection of the existing rule to hold.
Log Only (No Action)	No action is taken. The alert is logged as received	**None**.
Play Sound At Console	Plays a sound when an alert is received at the Enterprise Console	**None**.

Purge Alert	Removes the alert from the Enterprise Console	**None**.
Raise Helpdesk Ticket	Sends an Instant Alert message to a nominated helpdesk when an alert is received	**Helpdesk** page: Fields on this page are used to generate an email message based upon a mixture of text and substitution variables. This can then be used to raise a ticket on a 3rd party helpdesk application.
Release Alert Rule	Releases the specified rule that was previously held using the Hold Alert Rule action	**Rule** page: Allows the selection of the held rule to be released.
Reset Alert Count	Resets the alert count of a specific rule	**Rule** page: Allows the selection of a rule and the Reset of the Alert Count back to a specified number (not necessarily zero).
Send Console Action	Closes or replies to an alert on the originating remote console	**Console** page. Options on this page allow the closing or replying to the alert with a user-defined message.
Send Instant Alert Message	Sends a message to other users on the network when a message is received. The message text can contain substitution variables	This action has two additional pages: **Recipients** page: Defines the users, from within the Instant Alert Address Book, that receive a message when an alert is triggered by this rule. **Message** page: Defines the message text to be sent and the format in which it is sent. Available Substitution Variables for use in the message are listed in a table below the text box. An example of variables content type is displayed in the read-only Example: text box as you enter each variable. The exact content displayed is defined by your system, network configuration and local conditions such as the date and time.

Send SNMP Trap	Sends an SNMP Trap	**SNMP Trap** page: Options on this page define the SNMP Trap options and the selection of a device to which the SNMP Trap is sent. Device attributes can be viewed. **SNMP Version**: Select the trap version from: v1 v2c v3 (only available if you have at least one SNMPv3 user) **SNMPv3 User**: Select the SNMPv3 User as defined in the SNMPv3 Users page of Device Manager **Select Device**: If a device is not currently available, a new one can be added from the Device Manager. Device details can be reviewed in the **View Device** dialog displayed by clicking **Details** in the **Select Device** window. In order to be an SNMP Target device, an IP address and Trap Port must be defined. Edit the device if these are options are not displayed. If an application is associated with the device, the application can be launched by double-clicking its name in the **Support** page.
Speak at Console	Plays a spoken message when an alert is received	**Speech** page: Options on this page define whether the device name is included in the message and if the actual alert text or text entered on this page is spoken.

Action Options section

Options in this section determine how the alert is processed.

Delay Before Action ... Minutes

If required, specify a time delay before the action is active. The default setting is zero minutes. This setting allows the investigation of an alert prior to an action occurring. For example, if an alert is sent to the Enterprise Console, a secondary action may be to send an Instant Alert message to recipients to advices of an issue. Building a time delay of, for example, 15 minutes allows for the cause of the issue to be investigated and possibly resolved before the Instant Alert message is sent.

Perform Action For

Specifies the alerts for which this action is performed.

- **All Alerts**: The specified Action Type is applied to all alerts
- **This Number of Alerts**: Specify the number of alerts for which the specified action is performed. See Advanced Rule Settings - Rule Count Method for more information

Comments

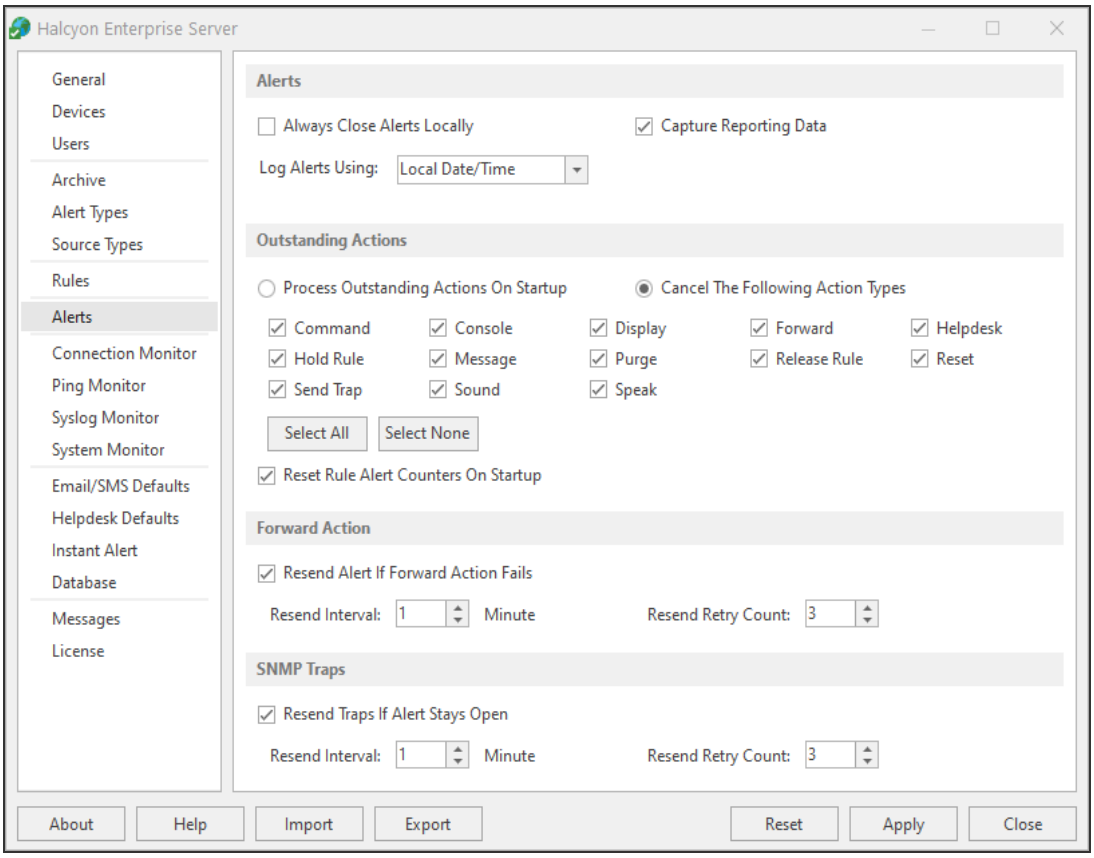
Add any comments you would like added to the status of this alert.

Click **OK** to apply the action.

Click **OK** to add the rule.

> NOTE: Use the **Edit Rule** option from the main Rule dialog display to amend any settings, criteria or actions for this rule.

Enterprise Server Options - Alerts



The Alerts tab of Enterprise Server Options is used to set global options for alert actions.

Alerts section

Always Close Alerts Locally

Check to enable the ability to close alerts locally even if an error occurred while trying to close or reply to an alert on the originating remote device.

Log Alerts Using

This setting allows you to choose whether alerts are logged using the local date and time at which the Enterprise Console received the alert or the remote date and time of the device from which the alert was sent.

IMPORTANT: This setting must be set to Remote Date and Time if the Time Zone setting of the Device is active, otherwise all alerts received from the device are displayed with the Local Date and Time setting from this field. See Time Zone for more information regarding this setting.

Outstanding Actions section

Settings in this section determine what happens to any outstanding actions when opening a session of Enterprise Console. Outstanding actions can either be processed or canceled. Individual actions and action types can be included or excluded from the instruction.

Process Outstanding Actions on Startup

Select this option to specify that all pending actions are executed upon starting a new session of Enterprise Console. No further action selection is required.

Cancel The Following Action Types On Startup

Select this option to activate the following action types that can then be canceled when the Enterprise Console service is restarted. If this option is selected and an action type in this section is left unchecked, the outstanding actions are processed on restart. This allows, for example, leaving all outstanding Console actions to be processed upon restart.

- **Message**: Select this option to cancel all outstanding message actions.
- **Display**: Select this option to cancel all outstanding display actions.
- **Sound**: Select to cancel all outstanding sound actions.
- **Speak**: Select to cancel all outstanding speech actions.
- **Reset**: Select this option to cancel all outstanding reset actions.
- **Command**: Select this option to cancel all outstanding command actions.
- **Console**: Select to cancel all outstanding Console actions, such as Close, on restart.
- **Send Trap**: Select to cancel all outstanding Send Trap actions.
- **Forward**: Select this option to cancel all outstanding forwarding actions.
- **Hold Rule**: Select this option to cancel all outstanding hold rule actions.
- **Release Rule**: Select to cancel all outstanding release rule actions on restart.
- **Help Desk**: Select to cancel all outstanding Help Desk actions on restart.
- **Purge**: Select this option to cancel all outstanding purge actions.

Select All

Click **Select All** to select all of the Action Types to be canceled on start-up of the Enterprise Console.

Select None

Click **Select None** to specify that all of the Action Types are processed on start-up of the Enterprise Console.

Reset Rule Alert Counters On Startup

Check this box to specify that all rule counters are reset back to zero when starting a new session of Enterprise Console.

The system remembers the current count of all active rules so for example, if a counter has an action of sending a message on the third instance of being raised and the current count is two, the system will reset this setting back to zero if this option is selected.

Forward Action section

This section is used to define what happens to forwarded alerts that fail to reach their target destination.

Resend Alert If Forward Action Fails

Select this option to ensure that any alerts that are raised with the forward action, are resent if the initial forwarding action fails.

Resend Interval

Specifies the time delay (in minutes) in re-sending forwarding alerts that fail the initial action. The default setting is 1 minute.

Resend Retry Count

Specifies the number of times that the resend action is attempted. The default setting is 3 attempts.

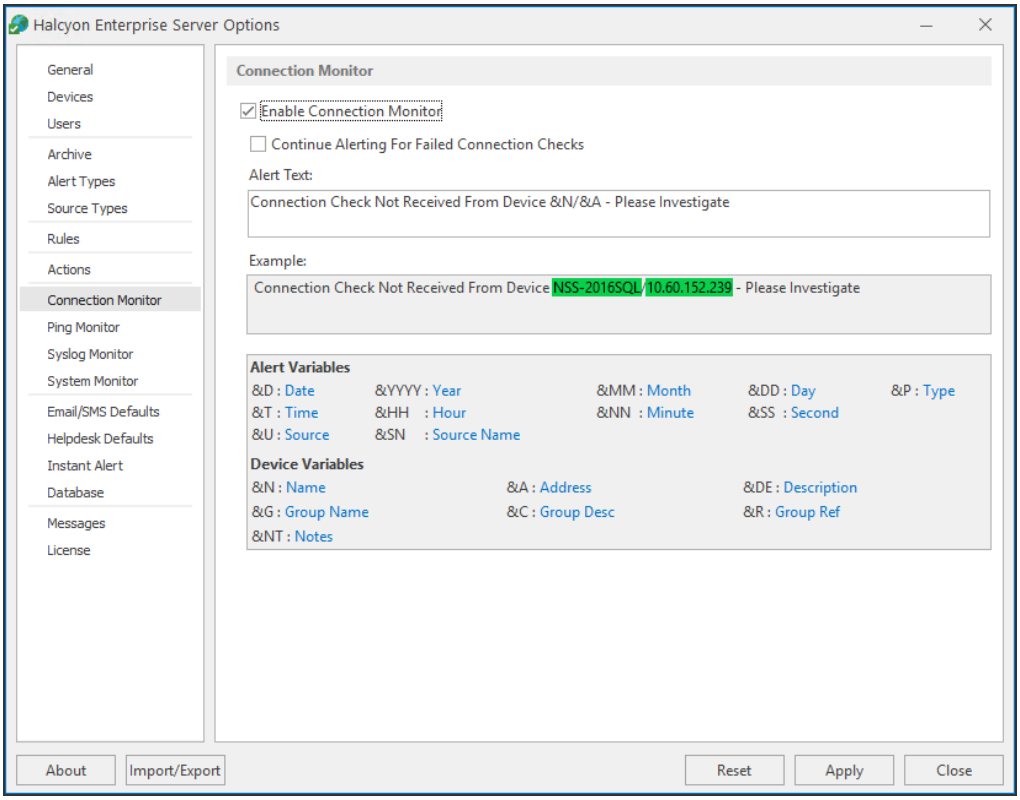
Enterprise Server Options - Connection Monitor

The Connection Monitor allows you to monitor connections to IBM i devices.

The Handshake Interval setting from within the Remote Locations menu option on the IBM i device specifies the frequency with which the device connects to the Enterprise Server Options.

Therefore, if the 'Handshake Interval' field entry is set to 5, the IBM i device attempts to connect to the Enterprise Console every five minutes. The lower the number the greater the frequency with which the contact is made, thus giving a faster indication of an error should connection be lost.

Enable the Connection Monitor to indicate that the Enterprise Console is active whenever the IBM i device connects. If no communication is received from the IBM i device within any sixty minute period (+ 2 minute grace period) an alert is generated with the text as defined in the **Alert Text** field.



Connection Monitor section

Enable Connection Monitor

Check this box to enable the Connection Monitor and associated settings.

Continue Alerting For Failed Connection Checks

Check this box to ensure that the connection monitor alerts when it is not possible to make contact with any device on which the Server Manager software is installed.

> TIP: A Device may be reporting as **Status - OK** in the Devices panel of the Enterprise Console but this may be because no alerts have been received as the connection has been lost. Enabling this option means that alerts are generated if a connection is unable to be made.

Alert Text

Default alert text (Connection Check Not Received From Device &N/&A - Please Investigate) is displayed in this field. This text can be edited as required. You can also add alert and device variables to clarify the details of the message.

Example

An example of how the actual alert will be displayed if generated, based upon the text and variables used, is shown in the Example field.

> TIP: When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

Substitution Variables

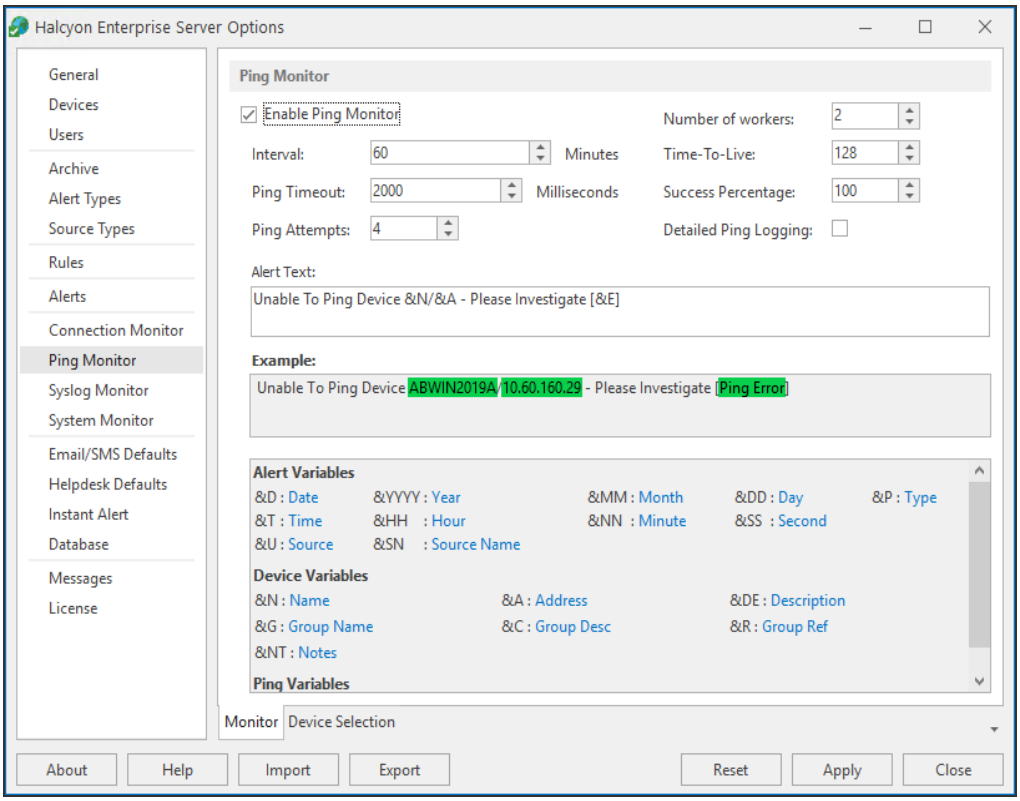
Connection Monitor substitution variables comprise:

- **Alert Variables**: (such as Date, Time, Source, Type and so on)
- **Device Variables**: (such as Name, IP Address, Group name and so on)

These variables can be added to the error message as required to identify the name and/or address of devices whose connections are monitored.

Enterprise Server Options - Ping Monitor

These options allow you to ping devices (selected in the Device Selection page) at regular intervals. If a device ping is unsuccessful, an error alert is generated with the error text as specified in the Alert Text field.



There are two tabs of information to complete when specifying Ping Monitor criteria. These are accessed at the bottom of the main display panel.

Monitor tab

Settings on this page define how the Ping Monitor operates and the text of any alerts that it generates.

Ping Monitor section

The fields in this section define how the Ping Monitor is configured.

> **TIP:** The settings in this section can be amended at any time without the need to restart the service.

Enable Ping Monitor

Check this box to enable the Ping Monitor and its associated settings.

Interval - Minute(s)

This option sets the ping interval in minutes. The default setting is 60 minutes. Either overtype the current entry or use the up/down arrows to adjust the setting.

Ping Timeout - Milliseconds(s)

This setting defines the time period after which any attempted ping is deemed to have failed. The default setting is 2000 milliseconds. Either overtype the current entry or use the up/down arrows to adjust the setting. .

Ping Attempts

This setting defines how many attempts are made to successfully connect with the device before the alert is raised. The default setting is 4 attempts. Either overtype the current entry or use the up/down arrows to adjust the setting.

Number of workers

This setting defines the number of connections made between the Enterprise Console and the Ping Monitor to ensure a continuous connection is maintained. The range is between 1 and 25 workers. Larger numbers in this field are intended for enterprises that contain many devices that are being simultaneously monitored. Performing a reload of devices from an Enterprise Console client refreshes the list of devices in the monitor and restarts processing.

Time-to-Live

This setting specifies the IP packet time-to-live value. The packet is valid only for the number of router hops specified by this parameter. The default setting is 128 hops.

The time-to-live value acts as a "hop counter". The counter is decremented each time the packet passes through a router or gateway.

Limiting the validity of the datagram by the number of hops helps to prevent internet routing loops. If the value reaches 0 then the packet is dropped and the ping will time-out.

Success Percentage

This setting determines the percentage of attempts required to be successful in order to prevent an alert being generated. The default setting is 4 attempts.

> **EXAMPLE:** With this field set to 100% and Ping Attempts set to 4, it would only take one failure to generate a success percentage of 75% and therefore raise an alert.

Either over type the current entry or use the up / down arrows to adjust the setting. It is advised that the success percentage is a multiple of the setting in the Ping Attempts field. The default setting is 100%.

Detailed Ping Logging

Enable Detailed Ping Logging in order to capture additional logging information generated by the use of the Ping Monitor.

Alert Text

This is the text message used to report a system monitoring issue. This text can be edited as required. Alert, device and specific system monitor variables can be added to clarify the details of the message.

Example

An example of how the actual alert will be displayed if generated, based upon the text and variables used, is shown in the **Example** field.

> TIP: When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

Variables

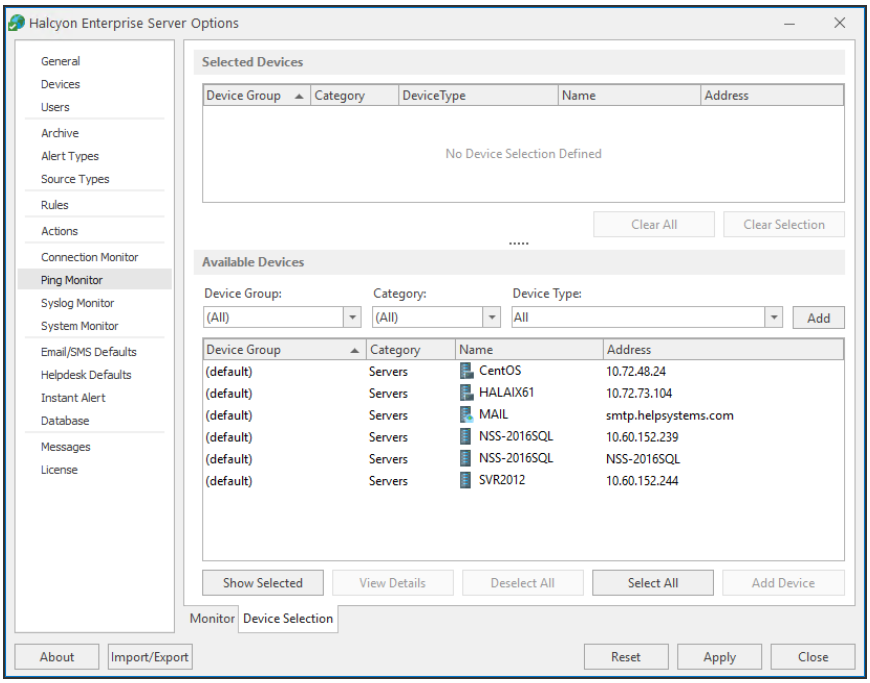
Ping Monitor substitution variables comprise:

- **Alert Variables**: (such as Date, Time, Source, Type and so on)
- **Device Variables**: (such as Name, IP Address, Group Name and so on)
- **Ping Variables**: (such as Ping Attempts, Failed Attempts and so on)

These variables can be added to the error message as required to identify the name and / or address of devices whose connections are monitored.

Device Selection tab

The **Device Selection** tab is used to select the Devices to which the monitor connects and raises alerts if the success percentage figure is not attained.



Selected Devices section

This section shows the devices that are currently selected for use with the monitor. When this tab is opened for the first time, this section is empty.

Information is listed in five columns:

- **Device Group**: Displays the name of the Device Group to which the device belongs.
- **Category**: Displays the category in which the device is defined.
- **Device Type**: Displays the Device Type of the device.
- **Name**: Displays the name of the device.
- **Address**: Displays the IP Address or Host name of the device.

Clear All

Click **Clear All** to remove all of the currently selected devices from selection.

Clear Selection

Highlight a device in the **Selected Devices** section and click **Clear Selection** to remove this device from selection. Multiple devices may be selected in one action.

Sorting columns

Column order can be rearranged by left-clicking on a column heading and keeping the mouse button depressed, dragging the column to the new position and releasing the button. Information in each column can be sorted in ascending or descending order by clicking on each column title to change the sequence.

Available Devices section

This section lists all of the devices that have been defined in Device Manager.

> **NOTE:** The IBM i Ping Monitor is multi-threaded. It sends an additional value to the IBM i to indicate if data needs to be encrypted to and from the Enterprise Console.

Filter options

These options allow the filtering of available devices on the network in order to restrict the list of available devices to just those that meet the filter criteria.

The categories comprise:

- **Device Group**: Device groups are collections of similar devices, such as all those that belong to a specific department. Device groups are set up and maintained in Device Manager
- **Category**: Devices, such as servers that can be divided into specific types. Items listed here are by default. No other items can be added to this list.
- **Device Type**: Device types, such as proxy servers are listed on this drop down and comprise a mix of default items and any other items identified on the network, which are automatically added to this list.

Add Device

To load a device into the **Selected Devices** section of this page, select the required device in the **Available Devices** section and click **Add Device** to move it into the **Selected Devices** section.

Show/Hide Selected

Click to show in the **Available Devices** section, only those devices not already listed in the **Selected Devices** table. This avoids duplicating device information in both

tables. Click again to show all available devices, including those that have already been selected.

View Details

This button is used to open the **View Device** dialog, which displays the attributes of a selected device. No amendments can be made on this display. If changes are required, use Edit Device in Device Manager.

Deselect All

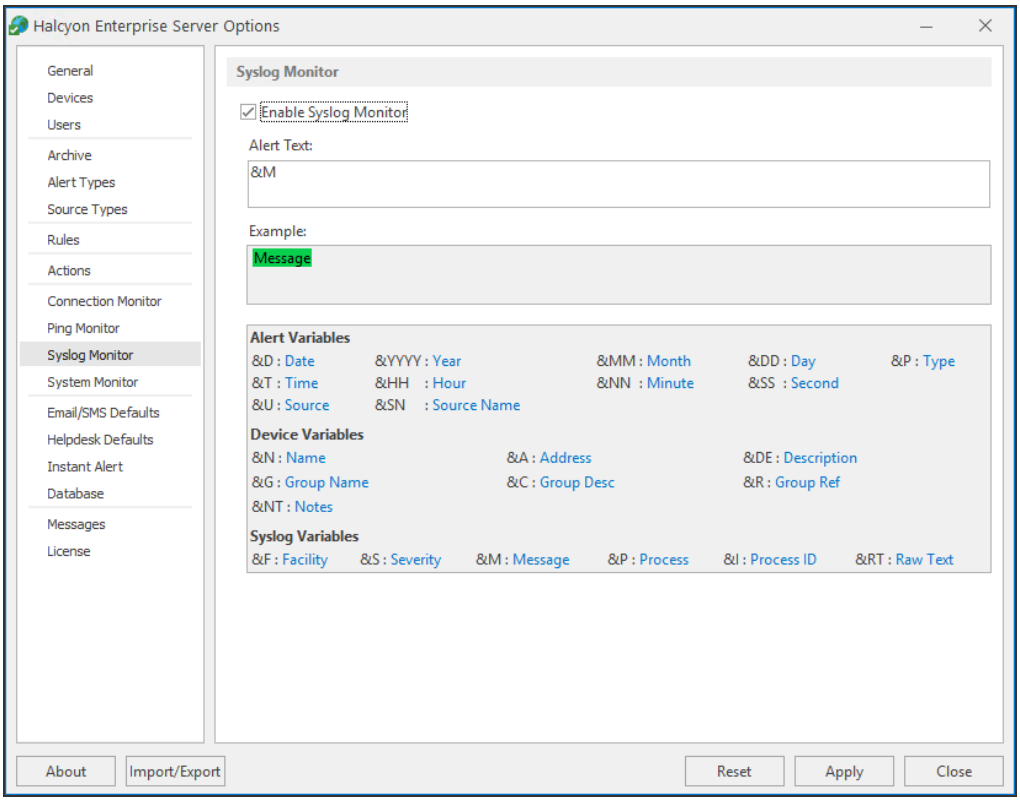
Click to deselect all of the currently selected devices in the **Available Devices** section.

Select All

Click to select all of the devices listed in the **Available Devices** section.

Enterprise Server Options - Syslog Monitor

The Syslog Monitor is used to capture system log information from identified devices (typically from UNIX and Linux servers) and forward it to the Enterprise Console.



Syslog Monitor section

This section is used to activate the Syslog Monitor and define the text of any alerts that it generates.

Enable Syslog Monitor

Check the box to enable the Syslog Monitor.

Alert Text

This is the text message used to report an error (default is: &M). This text can be edited as required. Alert, device and syslog variables can be added to clarify the details of the message.

Example

An example of how the actual alert will be displayed if generated, based upon the text and variables used, is shown in this field.

TIP: When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

Variables

Syslog Monitor variables comprise of:

- **Alert Variables**: (such as Date, Time, Source, Type and so on)
- **Device Variables**: (such as Name, IP Address, Group Name and so on)
- **Syslog Variables**: (such as Facility, Severity, Message and so on)

These variables can be added to the error message as required to identify the name and/or address of devices whose connections are monitored.

Syslog Facilities

The following table shows the Syslog Facility Numerical Code and the Facility that it represents.

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security / authorization messages (note 1)
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem

9	clock daemon (note 2)
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Syslog Message Severity

The following table shows the Syslog Severity Numerical Code and the Severuty that it represents.

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

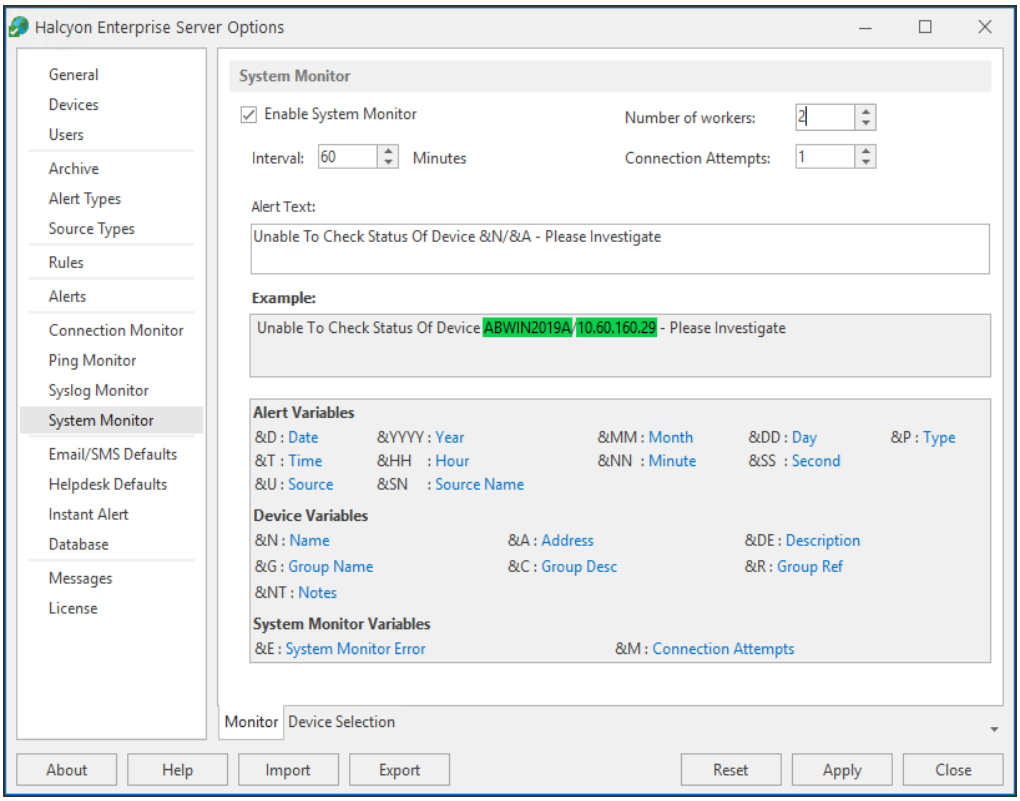
Forwarding Syslog Messages from a Linux Device

In order to be able to forward syslog messages to the Enterprise Console from a Linux device, the following configuration steps must be implemented:

1. Log on to the required Linux device as a super user.
2. Type the command:
   `vi/etc/syslog.conf` to open the configuration file called **syslog.conf**.
3. Type ***.*** and press the **Tab** key
4. Type the name of the host device on which Enterprise Server is running, for example:
   `*.* @ENTCON`
5. Restart the syslog service using the command:
   /etc/rc.d/init.d/syslog restart

Enterprise Server Options - System Monitor

The System Monitor is used to send a Halcyon specific request to any identified remote system Network Manager. If no response is received, an alert is raised. This is useful to ensure that all systems are constantly being monitored and highlights any connection or power issues that may be affecting a remote system.



There are two tabs of information to complete when specifying System Monitor criteria. These are accessed at the bottom of the main display panel.

Monitor tab

System Monitor section

This section is used to activate the System Monitor and define the text of any alerts that it generates.

> TIP: The settings in this section can be amended at any time without the need to restart the service.

Enable System Monitor

Check this box to enable the System Monitor and associated settings.

Interval Minutes

This option sets the monitoring interval in minutes. Either over type the current entry or use the up/down arrows to adjust the setting. The default setting is 60 minutes.

Number of workers

This setting defines the number of connections made between the Enterprise Console and the System Monitor to ensure a continuous connection is maintained. The range is between 1 and 25 workers. Larger numbers in this field are intended for enterprises that contain many devices that are being simultaneously monitored. Performing a reload of devices from an Enterprise Console client refreshes the list of devices in the monitor and restarts processing.

Connect Attempts

This setting defines the number of connection attempts that are made on each check to deem if the remote Network Manager is answering. For slow machines it is recommended that the setting is increased to handle any lack of response in inter-connectivity. The default setting is 1 attempt.

Alert Text

This is the text message used to report a system monitoring issue. This text can be edited as required. Alert, device and specific system monitor variables can be added to clarify the details of the message.

Example

An example of how the actual alert will be displayed if generated, based upon the text and variables used, is shown in the **Example** field.

> TIP: When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

Variables

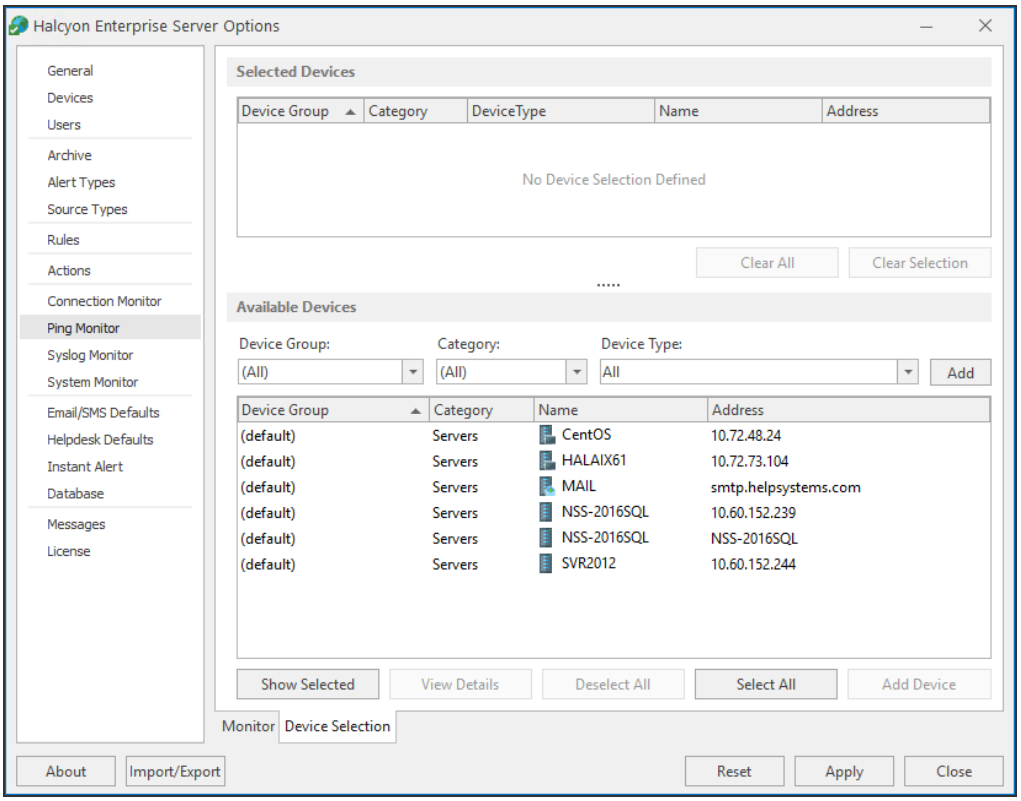
System Monitor variables comprise of:

- **Alert Variables**: (such as Date, Time, Source, Type and so on)
- **Device Variables**: (such as Name, IP Address, Group Name and so on)
- **System Monitor Variables**: (includes System Monitor Error and Connect Attempts)

These variables can be added to the error message as required to identify the name and/or address of devices whose connections are monitored.

Device Selection tab

The **Device Selection** tab is used to select the Devices to which the monitor connects and raises alerts if the success percentage figure is not attained.



Selected Devices section

This section shows the devices that are currently selected for use with the monitor. When this tab is opened for the first time, this section is empty.

Information is listed in five columns:

- **Device Group**: Displays the name of the Device Group to which the device belongs.
- **Category**: Displays the category in which the device is defined.
- **Device Type**: Displays the Device Type of the device.
- **Name**: Displays the name of the device.
- **Address**: Displays the IP Address or Host name of the device.

Clear All

Click **Clear All** to remove all of the currently selected devices from selection.

Clear Selection

Highlight a device in the **Selected Devices** section and click **Clear Selection** to remove this device from selection. Multiple devices may be selected in one action.

Sorting columns

Column order can be rearranged by left-clicking on a column heading and keeping the mouse button depressed, dragging the column to the new position and releasing the button. Information in each column can be sorted in ascending or descending order by clicking on each column title to change the sequence.

Available Devices section

This section lists all of the devices that have been defined in Device Manager.

Filter options

These options allow the filtering of available devices on the network in order to restrict the list of available devices to just those that meet the filter criteria.

The categories comprise:

- **Device Group**: Device groups are collections of similar devices, such as all those that belong to a specific department. Device groups are set up and maintained in Device Manager
- **Category**: Devices, such as servers that can be divided into specific types. Items listed here are by default. No other items can be added to this list.

- **Device Type**: Device types, such as proxy servers are listed on this drop down and comprise a mix of default items and any other items identified on the network, which are automatically added to this list.

Add Device

To load a device into the **Selected Devices** section of this page, select the required device in the **Available Devices** section and click **Add Device** to move it into the **Selected Devices** section.

Show/Hide Selected

Click to show in the **Available Devices** section, only those devices not already listed in the **Selected Devices** table. This avoids duplicating device information in both tables. Click again to show all available devices, including those that have already been selected.

View Details

This button is used to open the **View Device** dialog, which displays the attributes of a selected device. No amendments can be made on this display. If changes are required, use Edit Device in Device Manager.

Deselect All

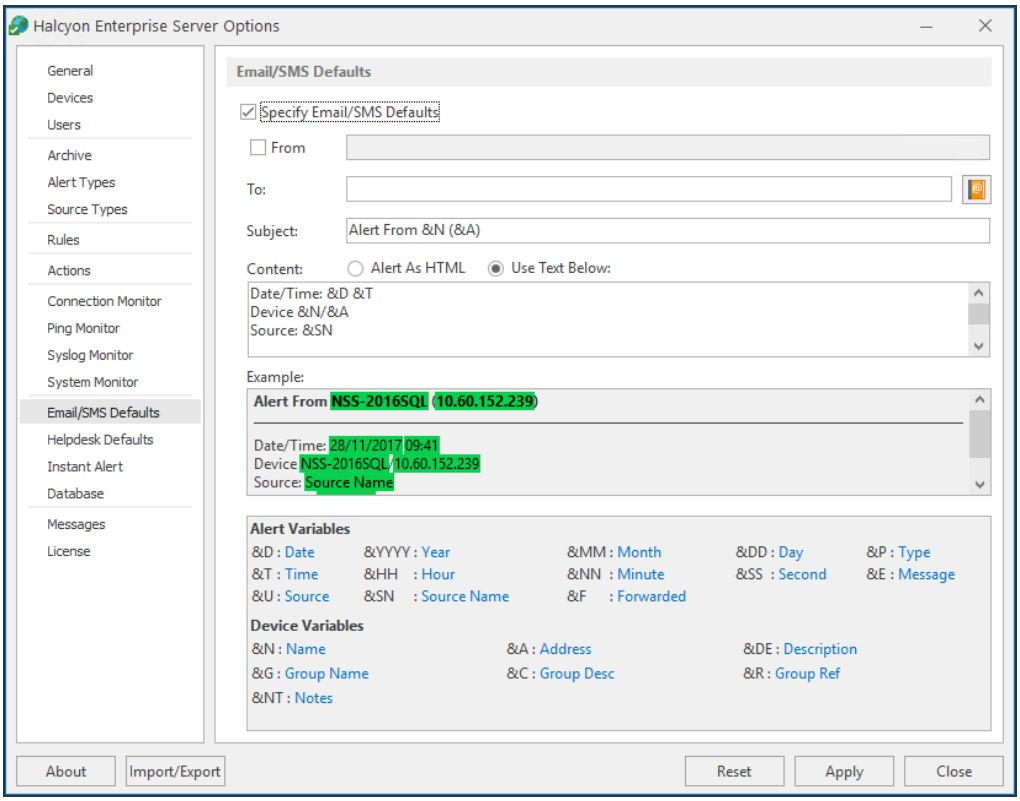
Click to deselect all of the currently selected devices in the **Available Devices** section.

Select All

Click to select all of the devices listed in the **Available Devices** section.

Enterprise Server Options - Email/SMS Defaults

The Email/SMS defaults page of Enterprise Server Options provides access to default settings when sending alerts via email or SMS.



Email/SMS Defaults section

Specify Send Alert as Email / SMS Defaults

Check this box to specify email/SMS defaults when sending alerts from Enterprise Console.

From

Check this box to enable the entry of the default sender details. Any emails/SMS messages that are sent via the **Send Alert As** option from the Enterprise Console, default to being sent from the entry in this field.

To

Enter the default recipient details to where the email/SMS message is sent. Any email/SMS messages that are sent via the **Send Alert As** option from the Enterprise Console, default to being sent to the entry in this field.

Click  **Address Book** to open the Instant Alert Address Book from where pre-defined email users can be selected.

Subject

Enter the default text for the Email/SMS subject title. This could be something simple such as **Enterprise ConsoleAlert** to identify the origins of the message. The default setting is '**Alert From**' followed by the name of the device '&N' and the IP Address or Host name '(&A)'.

Content

The message content can be made up from typed text, substitution variables listed at the bottom of this dialog, or a mixture of both. The message content can be delivered either as:

- **HTML**: The message content is generated in HTML format by default
- **Use Text Below**: The message content is generated using the entered text as the default

Example

Displays a textual example of how the message is generated using the current selections in the Subject and Content fields.

> TIP: When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

Variables

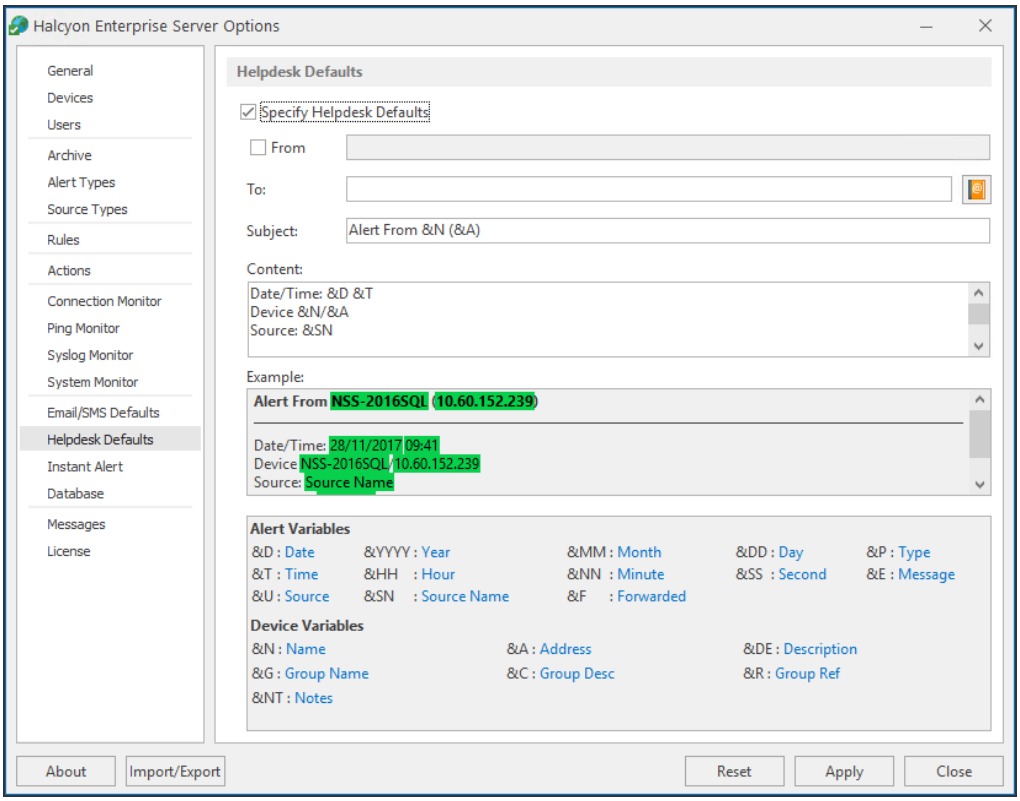
Use variables to assist in the building of the message content. Send Alert as Email/SMS substitution variables comprise:

- **Alert Variables**: (such as Date, Time, Source, Type and so on)
- **Device Variables**: (such as Name, IP Address, Group name and so on)

Enterprise Server Options - Helpdesk Defaults

The Helpdesk Defaults page is used to specify defaults used when sending alerts to third party helpdesk applications.

If a rule is triggered with the action of **Raise Helpdesk Ticket**, or as a right-click | **Send Alert As** | **Helpdesk Email** directly from an Enterprise Console Alert is selected, the default information entered in this dialog can be used to generate an email that when received by the third party helpdesk application, can automatically raise a ticket.



Helpdesk Defaults section

Specify Helpdesk Defaults

Check this box to specify helpdesk defaults when sending alerts from Enterprise Console.

From

Check this box to enable the entry of the default sender details.

> **NOTE:** A 'From Address' is a mandatory requirement of some helpdesk applications.

To

Enter the default recipient details to where the alert message is sent. This is usually a generic helpdesk email address.

Click **Address Book** to open the Instant Alert Address Book from where pre-defined email users and helpdesk entries can be selected.

Subject

Enter the default text for the helpdesk message subject title. This could be something simple such as **Enterprise ConsoleAlert** to identify the origins of the message. The default setting is '**Alert From**' followed by the name of the device '&N' and the IP Address or Host name '(&A)'.

Example

Displays a textual example of how the message is generated using the current selections in the Subject and Content fields.

> TIP: When using substitution variables throughout Enterprise Console, any entries that are made correctly are highlighted in green and those that will result in an error are highlighted in red.

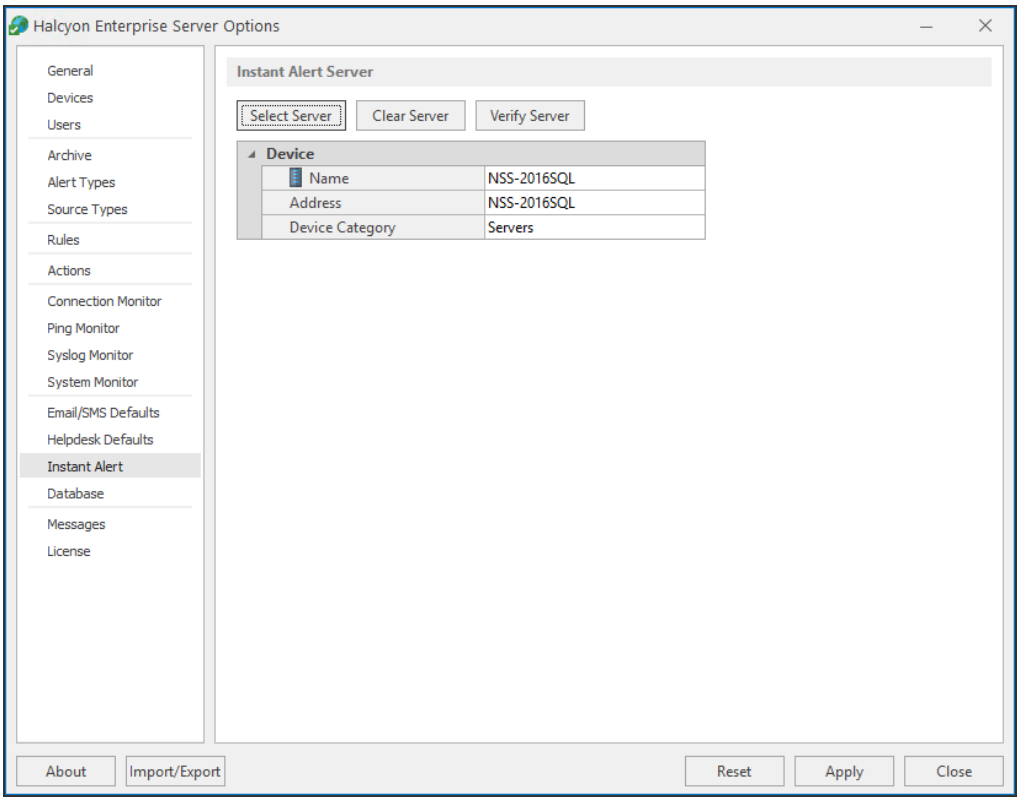
Variables

Use variables to assist in the building of the message content. Send Alert as Email/SMS substitution variables comprise:

- **Alert Variables**: (such as Date, Time, Source, Type and so on)
- **Device Variables**: (such as Name, IP Address, Group name and so on)

Enterprise Server Options - Instant Alert

Instant Alert settings are used to specify the server on which the instance of Instant Alert used by Enterprise Console is running.



Instant Alert Server section

The following options are available on the Instant Alert page:

Select Server

This is used to select the server on which the instance of Instant Alert is running.

To select the Instant Alert Server:

1. From the **Enterprise Server Options - Instant Alert** page, click **Select Server**. The **Select Device** dialog from which the Instant Alert device can be selected is displayed. The device on which Enterprise Console is installed is listed by default.
2. Highlight the required device and click **Select**. The selected device is now installed as the Instant Alert Server.

Clear Server

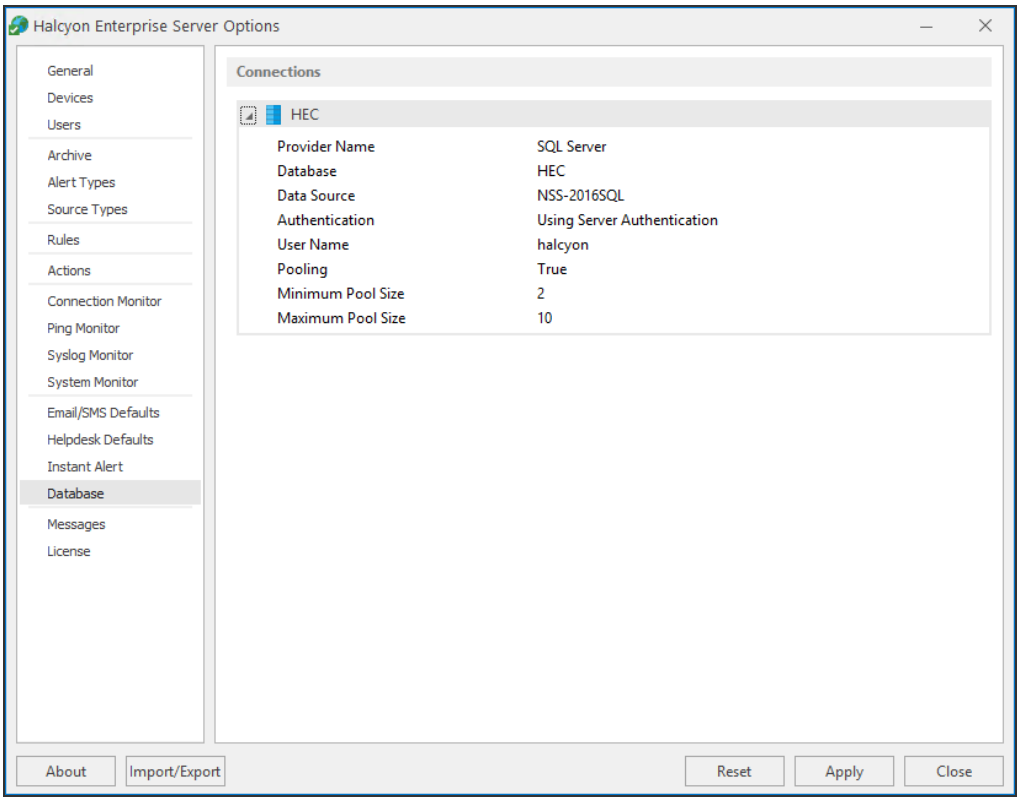
Click to remove the currently displayed device as the Instant Alert Server.

Verify Server

Click to test the connection between the current device and the Instant Alert Server.

Enterprise Server Options - Database Settings

The Database page is used to display the current details of the SQL or Postgres server package being used.



Connections section

This section displays the details of the current database instance being used by this instance of Enterprise Console.

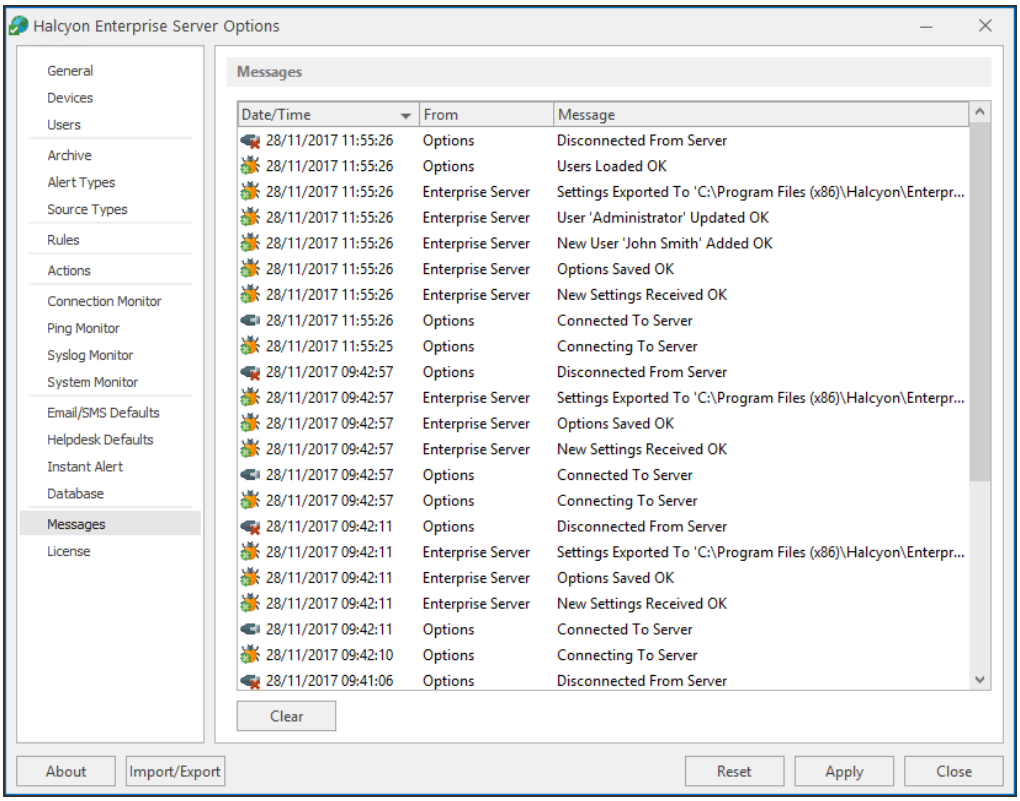
It is possible to view, but not amend, the details of the current instance.

Enterprise Server Options - Messages

The Messages page is used to display any system messages generated by the Enterprise Console since the last logon session was activated.

These can be used as an audit trail showing all actions undertaken since the Enterprise Server Options program was opened.

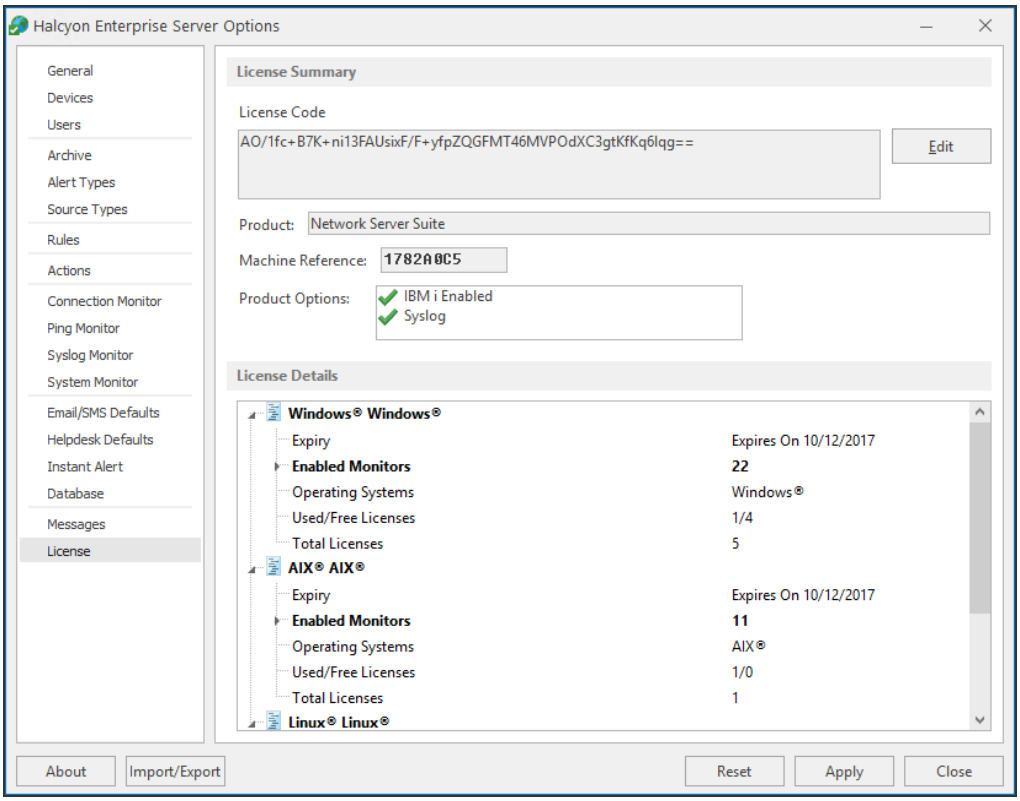
The messages in this display are generated regardless of the settings in the Message Logging Settings section of Enterprise Server Options- General page.



Click **Clear** to delete all of the current messages from this display.

Enterprise Server Options - License

The licenses page of Enterprise Server Options shows the current licensing configuration.



There are two forms of licensing in Network Server Suite:

- An overall product license that allows the use of Network Server Suite.
- Individual licenses that are applied to single systems to be monitored within Network Server Suite.

License Summary section

The fields in this section provide information relating to the license assigned to this installation.

License Code

This displays the current license code for this installation. You may need to change this code if you are on a demonstration or temporary version of the software. See Editing licenses for more information on how to update the current license.

Product

Displays the name of the product for which this license currently applies.

Machine Reference

Displays the machine reference number that is unique to the device on which this installation resides. The machine reference must be supplied to Fortra when requesting a new license code to ensure that a valid license is generated.

Product Options

Displays the details of any additional products, outside of the usual license agreement that are included in this installation.

License Details section

This panel shows the details of the individual licenses that have been applied and are still available for use for each operating system for which licenses are included with this installation. For each operating system, the following information is displayed:

- **License Name**: Displays the name that was attributed to the license at the time it was generated by Fortra. In most cases, this will be the name of the Operating system to which the license applies but it could be a customized entry, depending on specific requirements.
- **Expiry**: Displays the date on which the current license for these systems expires.
- **Enabled Monitors**: Displays the number of monitors enabled for use in this operating system
- **Operating Systems**: Displays the name of the Operating System to which the licenses apply; Windows, AIX and Linux.
- **Used/Free Licenses**: Displays the number of used licenses against the number of free licenses for this operating system. For example, an entry of 1/5 indicates that 1 out of 5 licenses is currently being used.
- **Total Licenses**: Displays the total number of licenses (Used + Free) available for this operating system.

Editing the license code

A license may required editing if it is a demonstration or periodic version of the software, as the codes for these versions expire.

If the system is transferred to a different machine, a new license will be required.

WARNING: If using the **Paste** method below, the **License Code** must be cut or copied from the Fortra communication (usually an email) prior to pasting into the **License Code** field.

To edit a license:

1. Open **Enterprise Server Options** and select the **License** page.
2. From the **License Summary** section, click **Edit**. The **Edit Product Code** dialog is displayed.

   Via Import: Click **Import** to open a new window allowing navigation to the directory containing the file **license.hli**. This is a specialist file supplied by Fortra containing the license information for the system based on the supplied machine reference. Once located, click **Open** to load the license information contained within the license.hli file.

   Via Paste: Click **Paste** to paste a previously cut or copied code into the **License Code** field.
3. Click **OK** to confirm. The date in the **Expiry** fields changes accordingly.

Enterprise Server Options - Button Options

There are five buttons available at the bottom of the Enterprise Server Options dialog.

About

Click to display version and ownership details of the Enterprise Server Options software.

Import / Export

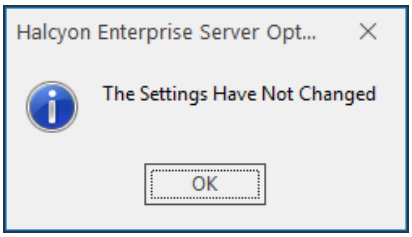
Click **Import/Export** to import or export current Enterprise Server Options settings from one device to another. See Exporting and Importing Data for more information.

Reset

Click to restore the settings to the last previously saved version of Enterprise Server Options. You are prompted to confirm this action.

Apply

Click to apply any changes to the Enterprise Server Options. If this is clicked without any settings having changed, the following dialog is displayed:



Close

Closes the Enterprise Server Options dialog. If you have not saved any changed options, you are prompted to do so prior to closing.

Exporting Data from Enterprise Server Options

Exporting settings from Enterprise Server Options provides a quick method of transferring data and settings between servers without having to re-enter all of the information. Exported data can be saved to a network drive or memory stick making it easy to transfer between remote devices.

Settings exported from Enterprise Server Options include:

- User data
- Defined rules

To export Enterprise Server Options settings:

1. Open **Enterprise Server Options**.
2. Click **Import/Export** in the Footer section of the Enterprise Server Options dialog.
3. Select**Export** and enter a **Path** and **File Name** or click **...** **Browse** to select a directory and file name to which the exported data is saved.
4. Click **OK** to save the data in the named file and location. The file is saved with an extension of .eco.

Importing Data to Enterprise Server Options

> WARNING: By importing settings from another instance of Enterprise Server Options, you overwrite any existing data. This action cannot be undone.

You must have previously Exported Settings from an existing instance of Enterprise Server Options prior to using the Import functionality.

To import Enterprise Server Options settings:

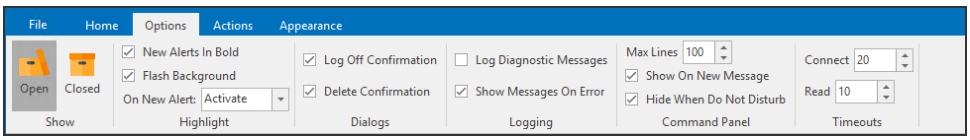
1. Open Enterprise Server Options.
2. Click **Import/Export** in the Footer section of the Enterprise Server Options dialog.
3. Select **Import** and click ... **Browse** to select a directory and an .eco file.
4. Click **Open** to import the data into this instance of Enterprise Server Options and override any existing data. Click **OK**.
5. When prompted, click **Yes** to confirm the import and overwriting of the existing Enterprise Server Options data.

Enterprise Console Options

Enterprise Console Options provide additional operating and connection parameters for the Enterprise Console.

> **NOTE:** Enterprise Console Options should not be confused with Enterprise Server Options which are used to set up and maintain rules, set user access rights and license software components.

Enterprise Console Options are accessed from the Enterprise Console menu bar. Click **Options** to open the Enterprise Console Options menu ribbon.



There are five panels available from within the Enterprise Console Options menu ribbon:

Highlight panel

The highlight panel contains options for displaying the alert when it is first displayed in the Enterprise Console.

Highlight New Alerts In Bold

Check this box to enable any incoming alerts to the Enterprise Console to be displayed in bold.

Flash Background

Check this box to enable the Flash mode for the device status if the highest priority alert for that device has an alert type that can flash when displayed in the Enterprise Console.

On New Alert

Use the drop-down menu to determine the action to be taken if the Enterprise Console is minimized or not active when an alert is received. This ensures that you do not miss any important alerts.

- **Activate**: Activates the Enterprise Console window and brings it to the foreground. Please see the note below.

- **Flash**: Flashes the Enterprise Console window and task bar icon.
- **No Action**: The Enterprise Console remains in a minimized or inactive state.

> **NOTE:** Automatic pop-up of windows has been disabled by Microsoft from Windows 10 onwards.

Dialogs panel

The Dialogs panel determines which dialog boxes, if any, are prompted for display as a result of a specific action being taken.

Log Off Confirmation

Check this box to enable the display of a message prompt to confirm or cancel the Enterprise Console log off action.

Delete Confirmation

Check this box to enable the display of a message prompt to confirm or cancel the deletion of closed alerts.

Logging panel

The Logging panel is used to specify logging message options for Enterprise Console.

Log Diagnostic Messages

Check this box to enable the display of diagnostic messages in the Message panel of Enterprise Console. Informational messages are logged by default.

Show Messages On Error

Check this box to automatically display the Message panel as the visible panel in the Details section of Enterprise Console whenever an error message is received.

Command panel

These settings are used to determine the behavior of the Enterprise Console Command panel in certain scenarios.

Max Lines

Defines the maximum number of lines to be displayed in the Command panel at any one time. The default setting is 100 lines. Either overtype the current entry or use the up/down arrows to select a new number.

Show On New Message

Check this box to automatically display the Command panel whenever a new Command message is received.

Hide When Do Not Disturb

Check this box to specify that any new Command messages arriving at a user console are hidden while they have an active mode of ‘Do Not Disturb’.

Timeouts panel

The timeouts panel is used to specify connectivity parameters.

Connect

The entry in this field sets the time, in seconds, within which the Enterprise Console must connect to the Enterprise Server before timing out. The default setting for this field is 20 seconds.

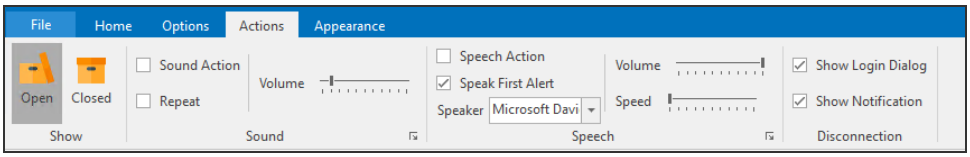
Read Timeout

The entry in this field sets the read timeout limit between the Enterprise Console and the Enterprise Server. This is time taken to read data between the two components. The default setting is 10 seconds.

Enterprise Console Actions

Enterprise Console Actions provide additional Sound, Speech and Disconnection options for the Enterprise Console.

Enterprise Console Actions are accessed from the Enterprise Console menu bar. Click **Actions** to open the Enterprise Console Options menu ribbon.



There are three panels available from within the Enterprise Console Options menu ribbon:

Sound panel

This panel is used to define the playing of sound alerts on the Enterprise Console.

> **NOTE:** In order for the sound to be played, a rule must have an action of Play Sound on Alert set.

Sound Action

Check this box to enable the standard Enterprise Console sound action. A sound card must be installed on the device on which this option is enabled.

Repeat

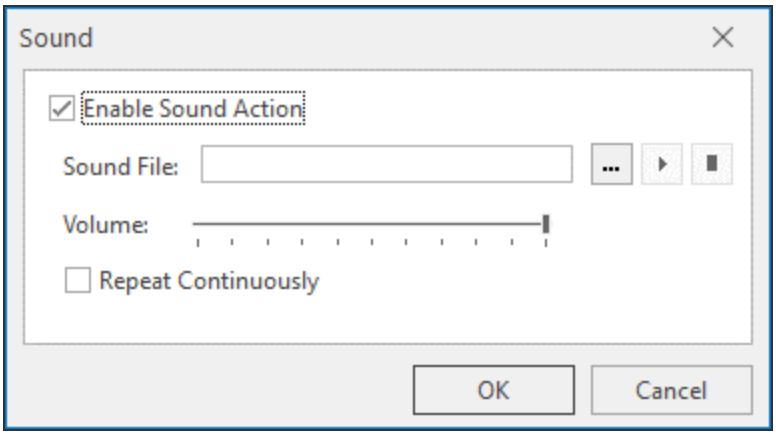
Check to have the sound played repeatedly until either **Mute Sound** or **F12** is pressed.

Volume

Use the slider control to set the volume level at which the sound is played.

Expanded options

Click **Expand** in the bottom-right corner of this panel to open a dialog contains additional options for the **Sound** panel.



Sound File

Enter the **directory path** or click ... **Browse** to navigate to your own preferred sound file. MP3 files are compatible with this option.

Click **Play** to play the selected file.

Click **Stop** to end play.

Click **OK** to confirm the selections.

Speech panel

This panel is used to define the playing of speech alerts on the Enterprise Console. Message content is taken from the setting specified in the **Speech** page of the Speak at Console action. This can be the actual error message text as raised by the alert or user-defined bespoke text.

> **NOTE:** To allow the speech function to work, the Microsoft Speech API (SAPI) version 5.1 runtime must be installed. This is included in the Enterprise Console installation. Additionally, in order for the speech played, a rule must also have an action of Speak at Console set.

Speech Action

Check this box to be enable the speech option. A sound card must be installed on the device on which this option is enabled.

Speak First Alert

This setting governs the action taken when simultaneous alerts arrive at the Enterprise Console. Check this box to have just the first of the simultaneous alerts announced. Leaving this field unchecked results in all alerts being announced if the speech option is enabled.

Speaker

Use the drop-down menu to select the voice variant used to announce the alerts as they arrive at the Enterprise Console.

Volume

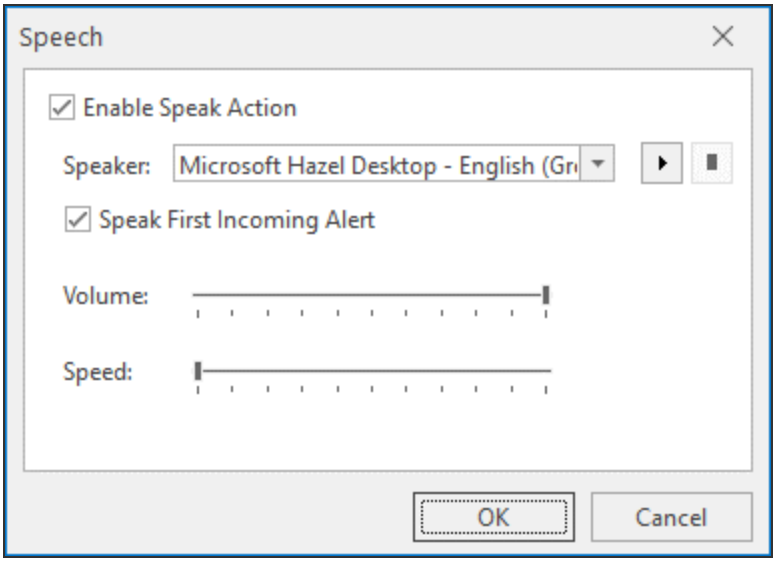
Use the slider bar to control the volume level of the speech.

Speed

Use the slider bar to control the speed at which the speech is spoken.

Expanded options

Click **Expand** in the bottom-right corner of this panel to open a dialog contains additional options for the **Speech** panel.



Speaker

Use the drop down menu to select additional voice variants used to announce alerts as they arrive at the Enterprise Console.

Click **Play** to play a test speech.

Click **Stop** to end play of the test speech.

Click **OK** to confirm the selections.

Disconnection panel

This panel is used to define what happens in the event of an unexpected disconnection from the Enterprise Console.

Show Login Dialog

Check this box to automatically display the Login dialog box should the Enterprise Console be unexpectedly disconnected from the Enterprise Server.

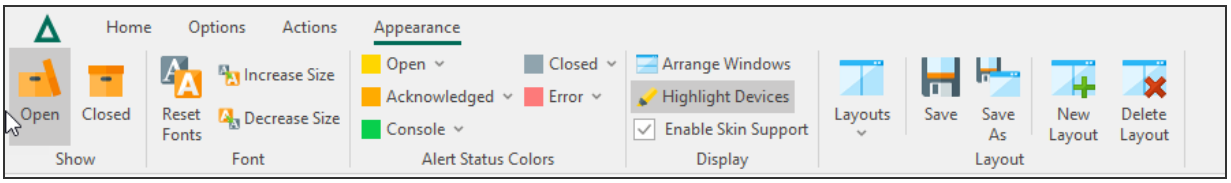
Show Notification

Check this box to display a balloon hint in the System Tray at the bottom of your screen if the Enterprise Console unexpectedly disconnects from the Enterprise Server.

Enterprise Console - Appearance

There are a variety of methods that can be deployed to suit personal viewing preferences when accessing the Enterprise Console.

From the Enterprise Console menu bar, select **Appearance**. The associated Appearance tool icons are now displayed in the Enterprise Console menu ribbon.



TIP: The following options only apply when the Enterprise Console is in **View** mode. To amend panel details, add or delete panels and change the Layout settings, use Edit mode.

There are five panels available from within the Enterprise Console **Appearance** menu ribbon:

Show

Use the options in this panel to determine whether open or previously closed alerts are displayed.

The view of Open alerts is the default view and displays any alert which is in a status of Open, Acknowledged, Console or Error. Closed alerts are viewed in the Closed option. Click **Closed** to open the Closed alerts options. See Closed Alerts for more information.

If the current view is showing Closed alerts, click **Open** to return to the default view.

Font

Fonts

Click **Fonts** to open a drop-down menu to select whether any font size changes affect all fonts across all panels and/or windows. All displayed text is then resized when either the increase size or decrease size option is selected.

Reset Fonts

Click **Reset Fonts** to reset any fonts that have been resized, and according to the options selected in Fonts, back to their original settings.

Increase Size

Click **Increase Size** to increase the font size of all text in accordance with the settings selected in the **Fonts** option.

Decrease Size

Click **Decrease Size** to decrease the font size of all text in accordance with the settings selected in the **Fonts** option.

Alert Status Colors

These four options define the alert colors for each of the following four statuses, as shown in the **Status** column for alerts displayed in the Enterprise Console.

- **Open**: The default status color for any open alerts is Yellow.
- **Acknowledge**: The default status color for any acknowledged alerts is Orange.
- **Error**: The default status color for any alerts in error status is Pink.
- **Console**: The default status color for any alerts replied to from the Console is Green.
- **Closed**: The default status color for any alerts that are closed is Gray.

Changing the Default color

To change the default color:

1. Click the down arrow to the right of each option to select a new color schema.
2. Select a new color schema from those colors displayed or click **More Colors** to define a unique color schema.

Display

These settings define the display formatting.

Arrange Windows

This feature is used when viewing multiple instances of the Enterprise Console on a single screen. Selecting this option automatically arranges multiple console windows into the optimized viewing display.

Select **Arrange Windows** to initialize.

> **NOTE:** Selecting this option when only one instance of Enterprise Console available for view has no effect.

Highlight Devices

Use **Highlight Devices** to highlight the status column of any devices listed within the Devices panel of Enterprise Console.

Enable Skin Support

This option is enabled by default and controls the color schemes used in Enterprise Console printed reports, such as the Device List, individual alerts or the contents of the alert panel (see Printing Alerts). In some circumstances, the report may display contents with an incorrect background color, which can make the reports illegible or harder to interpret. In these instances, click this option to remove skin support so that the report contents can be printed correctly.

Layout

Options in this panel allow the selection and saving of any layout changes (created while in Edit mode). Saved layouts can be selected using the drop-down list from **Layouts**. You can also add a new layout or delete an existing layout.

Layouts can be one of:

- **Private**: Only the user who created the layout is able to view, edit and delete it
- **Public**: The layout is available to anyone to view but only an administrator can edit or delete it.

Layouts

Click **Layouts** to display a drop-down menu containing previously saved Layout formats. The current format being used is indicated by a tick mark. If available, click on another listed layout to select.

> **NOTE:** If no other layouts have been defined and saved, the only available option in this list is the Default format. Even if this is deleted, the next user that logs on to the Enterprise Console causes the default layout to be regenerated and available to all users.

> **NOTE:** Views are unique to the user. Therefore it is possible to have multiple instances of Enterprise Console showing different panel views (containing the same data) if more than one user is logged on simultaneously.

> **NOTE:** Enterprise Console remembers the last panel setting as used by the user and defaults to that display upon opening.

Save

Click **Save** to save any modified layout as the current layout name. Layouts are modified using the Edit mode.

Save As

Click **Save As** to save any modified layout with a new layout name. Additional, saved layouts can be viewed from **Layouts**.

Adding A New Layout

You can create a new layout that customizes just the information you personally want to view, or a layout that is tailored to the specific requirements of a department or specialist team.

This enables multiple views of the same or different information to be displayed in a way that is convenient to each user.

Switching layout views enables another user to have this information displayed in their own preferred display format.

From the **Enterprise Console** | **Appearance** tab, click **New Layout** and click **Yes** when prompted.

> **NOTE:** Once confirmed, the mode automatically changes from View to Edit.

Adding a new layout to the Enterprise Console starts with a blank canvas. Further panels can then be added to the new layout as required. Select from the following:

Action panel

Click **Add Action Panel** to create a new Actions panel on the layout.

The Action panel shows what actions have been processed against an alert since it was first logged on the Enterprise Console.

> **NOTE:** Only one Action panel can be included within a layout.

See Action History panel for details of the parameters displayed in this panel.

Alert panel

Click **Add Alert Panel**. The Add Panel dialog opens.

The Add Panel dialog is split into three separate pages.

Panel page

These parameters define the panel name and alert configuration of the new panel.

Panel Details section

Caption

Enter the text to appear in the heading of this panel in the Enterprise Console

Icon

From the drop-down menu, select the icon to identify this panel Enterprise Console.

Alert Kind section

Settings in this section define the kind of alert that is displayed in this panel.

Alert Kind

Choose the alert kind option for this panel.

- **Both**: Both kinds of alert are displayed. This is the default setting.
- Information: These are alerts that are raised and provide information to the user.
- **Inquiry**: These are alerts that usually require some form of action to be taken on the part of the user.

Alert Text section

The parameters in this section specify the default alert text of any alerts displayed in this panel, if not overridden at rule level.

Text

Enter the alert text based on conditional parameters (equals, less than, greater than, and so on).

Wildcards

Wildcard characters can be used when defining the ‘Alert Text’. The default setting is to use '*' as a substitute for zero or more characters, and '?' as a substitute for single characters.

Alert Selection section

Settings in these panels determine the status, type and source of alerts that can be displayed in this panel.

Alert Type

This panel is used to select the type of alerts that are allowed to be displayed in this panel. By default, alerts of any type can be displayed.

Click **Any Alert Type** to remove the default setting and enable the panel from which specific alert types can be selected.

Alert Status

This panel is used to select the statuses of alerts that are allowed to be displayed in this panel. By default, alerts of any status can be displayed.

Click **Any Alert Status** to remove the default setting and enable the panel from which specific alert statuses can be selected.

Source Type

This panel is used to select the originating source from which generated alerts are allowed to be displayed in this panel. By default, alerts originating from any source type can be displayed.

Click **Any Source Type** to remove the default setting and enable the panel from which specific source types can be selected.

Select All

With the default setting of Any Alert Status, Any Alert Type and/or Any Source Type removed, click **Select All** to reselect all of the options in the respective panel.

Select None

With the default setting of Any Alert Status, Any Alert Type and/or Any Source Type removed, click **Select None** to deselect all of the options in the respective panel.

OpenDevices page

The Device page determines the devices from which you can receive alerts in this panel. Devices must have previously been loaded using the Device Manager in order for them to be available for selection in this screen.

Selected Devices section

This section shows the devices that are currently selected for use with the monitor. When this tab is opened for the first time, this section is empty.

Information is listed in five columns:

- **Device Group**: Displays the name of the Device Group to which the device belongs.
- **Category**: Displays the category in which the device is defined.
- **Device Type**: Displays the Device Type of the device.
- **Name**: Displays the name of the device.
- **Address**: Displays the IP Address or Host name of the device.

Clear All

Click **Clear All** to remove all of the currently selected devices from selection.

Clear Selection

Highlight a device in the Selected Devices section and click **Clear Selection** to remove this device from selection. Multiple devices may be selected in one action.

Available Devices section

This section lists all of the devices that have been defined in Device Manager.

Filter options

These options allow the filtering of available devices on the network in order to restrict the list of available devices to just those that meet the filter criteria.

The categories comprise:

- **Device Group**: Device groups are collections of similar devices, such as all those that belong to a specific department. Device groups are set up and maintained in Device Manager
- **Category**: Devices, such as servers that can be divided into specific types. Items listed here are by default. No other items can be added to this list.
- **Device Type**: Device types, such as proxy servers are listed on this drop down and comprise a mix of default items and any other items identified on the network, which are automatically added to this list.

Add Device

To load a device into the Selected Devices section of this page, select the required device in the Available Devices section and click Add Device to move it into the Selected Devices section.

Show/Hide Selected

Click to show in the Available Devices section, only those devices not already listed in the Selected Devices table. This avoids duplicating device information in both tables. Click again to show all available devices, including those that have already been selected.

View Details

This button is used to open the View Device dialog, which displays the attributes of a selected device. No amendments can be made on this display. If changes are required, use Edit Device in Device Manager.

Deselect All

Click to deselect all of the currently selected devices in the Available Devices section.

Select All

Click to select all of the devices listed in the Available Devices section.

Display page

Options on this page define display settings of the information contained within this panel.

Alert Display Settings section

Settings in this section define how alerts are displayed in this panel.

Display Device Color

Select this option to display the color of each device as defined in Device Manager when alerts are displayed in this panel within the Enterprise Console.

Show Alerts From Unknown Devices

Select this option to display alerts from unknown devices for alerts that are displayed in this panel within the Enterprise Console. Unknown devices are those devices for which alerts exist on the Enterprise Console but for which the device no longer exists within Device Manager. These alerts are indicated by a symbol in the alert detail on the Enterprise Console main display.

Display Source Color

Select this option to display the color of each source type as defined in Enterprise Server Options - Source Types when alerts are displayed in this panel within the Enterprise Console.

Display Status Color

Select this option to display the default status color of each alert as defined in Enterprise Console Options - Alert Types when alerts are displayed in this panel within the Enterprise Console.

Column Headers section

This setting defines whether column headers are displayed

Display Column Headers

Select this option to display column headers at the top of each column within this panel.

Auto-refresh section

This setting defines the time period between the auto-refresh of data in this panel.

Auto-refresh interval

Specifies the time, in seconds, after which the data in this panel is automatically refreshed. The default setting is 30 seconds. Either over type this entry or use the up/down arrows to select a new time period.

> IMPORTANT: The Devices Panel refreshes independently of any other panel in the display. Therefore, the Status of a Device may update before the alert is visible in the alert panel due to the difference in auto-refresh intervals between the panels.

Grouping section

Group Alerts

Select this option to indicate that any alerts in this panel that have identical criteria are grouped together and displayed as a single alert within this panel on the Enterprise Console. This alert can then be expanded to view the group of identical alerts beneath. The purpose of this functionality is to reduce the possibility of the Enterprise Console being hit by a 'message storm' where a source can produce multiple alerts with the same criteria.

> NOTE: See Grouping Alerts for more information.

Once the parameters have been entered for the new panel, click **OK**.

The alert panel is then automatically added to the current Enterprise Console view, from where it can be resized and repositioned.

Command panel

Click **Add Command Panel** to create a new command panel on the layout. The Command panel is used to send system messages to other users.

> **NOTE:** Only one Command panel can be included within a layout.

See Command panel for details of the parameters displayed in this panel.

Device panel

Click **Add Device Panel** to create a new Device panel on the layout. The Device panel shows all the devices that are currently defined in Device Manager.

> **NOTE:** Only one Device panel can be included within a layout.

See Device panel for details of the parameters displayed in this panel.

Detail panel

Click **Add Detail Panel** to create a new Details panel on the layout. The Details panel has a dual purpose and can be used to display the details of any device selected from the Devices panel or the details of an alert selected from any Alert panel.

> **NOTE:** Only one Detail panel can be included within a layout.

See Details panel for details of the parameters displayed in this panel.

Message panel

Click **Add Message Panel** to create a new Message panel on the layout. The Messages panel shows details of any system messages that may have been generated as a result of Enterprise Console activity.

> **NOTE:** Only one Message panel can be included within a layout.

See Messages panel for details of the parameters displayed in this panel.

User panel

Click **Add User Panel** to create a new User panel on the layout. The Users panel displays the details of all users that have been defined for use with this Enterprise Console.

> **NOTE:** Only one User panel can be included within a layout.

See Users panel for details of the parameters displayed in this panel.

Saving new layouts

Once the new layout has been created and configured, it must be saved so it can be used at a later date.

Click  **Save** to save changes to the current layout.

Click  **Save As** to create a new layout with the new name provided at the **Save As** prompt.

Enter the **Name** of the layout.

Leave the **Public Layout** check box set to the default of enabled to indicate that this layout will be able to viewed by all users of this Enterprise Console. Otherwise, click the Public Layout check box to remove the tick mark and indicate that this layout will only be available as a private view to the user that created it.

Click **OK** to complete the save of the layout.

> WARNING: Failure to save the layout means that any changes that you have made are lost.

All changes to layouts are only visible once a user has logged off the Enterprise Console and logged back in again.

Changing Layouts

To change the design of an existing layout, reposition the panels within the Enterprise Console as required. The following methods can be used.

Drag and Drop

It is possible to reposition each of the panels to a new location within the display window.

To use drag and drop:

1. Position the pointer over the title bar section of the panel that you wish to move.

2. Click and hold the left mouse button down and drag the panel to the desired position.
A position highlighter is displayed to assist by highlighting the area to which the panel will be re-positioned.

3. Once satisfied with the position, release the mouse button. The panel is now repositioned.

> **NOTE:** This takes practice to achieve the desired result. Use **Layouts** | **Default Layout** from the Enterprise Console menu ribbon to return to the default display setting.

Stretch and Shrink

Individual panels of the Enterprise Console can be re-sized by using the stretch technique. As a result, other panels on the display shrink to accommodate the new size.

To use stretch and shrink:

1. Position the pointer over either the horizontal or vertical dividing bars between the panel. The pointer changes to a or **Move Border** shape.
2. Hold the left mouse button down and drag the border in the direction that you wish to resize.
3. Release the button when the desired position is reached.

Maximize and Hide

Maximize and Hide functions allow you to remove or fully display single panels within the main Enterprise Console window.

To use Maximize and Hide panels:

Click **Expand** on the panel title bar to maximize the view of any panel (the arrow orientation changes depending on the panel).

Click **Resize** to return to the previous view.

Click **Close** on the panel title bar to remove the panel from view. Use **Appearance** | **Layouts** | **Default Layout** from the Enterprise Console menu ribbon to return to the default display setting.

> **NOTE:** See Resizing Fonts and Stretch and Shrink options for additional layout manipulation tools.

Deleting A Layout

Deleting a layout removes it from selection in Layouts from within **Enterprise Console | Appearance**.

If you accidentally delete the default layout and it is the only layout in use, then the next user who logs on to the Enterprise Console will automatically recreate the initial default view.

All changes to layouts are only visible once a user has logged off the Enterprise Console and logged back in again.

To delete a layout:

1. Select the **Appearance** tab
2. Click **Layouts** and from the drop-down menu, click on the Layout that you want to delete. The view changes to this layout.
3. Click **Delete Layout**.
4. Click **Yes** to confirm the deletion.
5. Click **Layouts** again and select another layout.

Importing Layouts

This process is only used to import any layouts that were previously saved in Enterprise Console v10.3.

WARNING: If you have any saved layouts in Enterprise Console v10.3, they are deleted upon an upgrade unless you rename and save them to another location first.

IMPORTANT: This process is only required when upgrading from v10.3 to v11.x of Enterprise Console as layouts are saved in the database from version 11.0 onwards.

To save the layouts in v10.3

1. Use Windows Explorer to navigate to C:\ProgramData\Halcyon\EnterpriseConsole\Layouts (assuming a typical install).
2. Select all the Layout (.lyt) files and copy them to a different file directory on your system.
3. Rename the files to prevent them overwriting the new layouts supplied with v11 onwards.

To import the previously saved layouts

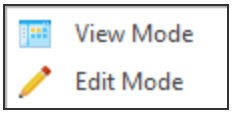
1. Open Enterprise Console.
2. From the top menu bar click and from the drop-down menu click **Import Layout**.
3. Use Windows Explorer to navigate to the location of the previously saved Enterprise Console Layout (.lyt) files.
4. Select the required .lyt files to be imported into Enterprise Console and click **Open**.
5. The files are now imported into Enterprise Console.

> **NOTE:** Due to enhancements made within the Enterprise Console in v11.0, the saved layouts may not exactly match with how they appeared in v10.3.

Switching Between View And Edit Mode

From the Information bar on the bottom of the Enterprise Console display, the current operational mode is displayed. In the screen shot below, the current mode is View.

1. Click the current option to display a pop-up menu.



2. Click on the option not currently selected to change to the new operational mode.

Using keyboard shortcuts

Use the following keyboard shortcuts to switch between modes:

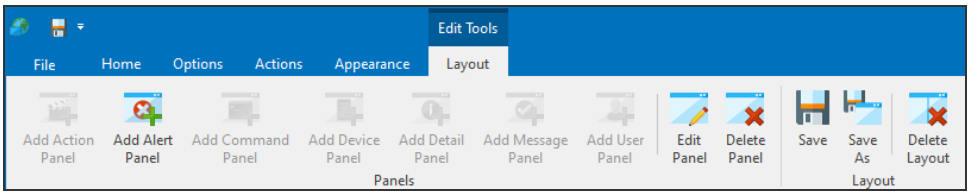
- **For View mode**: Ctrl+Alt+V
- **For Edit Mode**: Ctrl+Alt+E

The new operational mode is now displayed in the Information bar.

Enterprise Console Edit Mode

By default, the Enterprise Console is shown in View-only mode which prevents accidental changes being made to the layout configuration.

Edit mode allows the re-confguration of an existing layout or the design of a completely new layout that can the be used from the Layouts option when operating in View mode.



TIP: See Switching between View and Edit Modes for more information on how to access Edit mode.

Editing Panels

Editing an existing panel within the Enterprise Console allows you to define and control the information displayed within the panel and from which devices the information originates.

To edit an existing panel, click **Edit Panel** from the **Edit Tools** | **Layouts** menu bar. The **Edit Panel** dialog opens.

NOTE: **Edit Mode** is required in order to edit the existing panels. See Switching between View and Edit Mode for more information.

The Edit Panel options are exactly the same as when adding a new layout to the Enterprise Console.

Deleting Panels

Should an existing panel no longer be needed it can be deleted from the current Enterprise Console view.

To remove a panel from the Enterprise Console, click **Delete Panel** from the **Edit Tools** | **Layouts** menu bar.

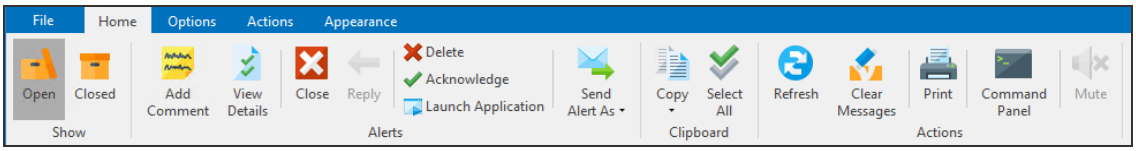
NOTE: **Edit Mode** is required in order to delete an existing panel. See Switching between View and Edit Mode for more information.

You are prompted to confirm the request. Click **Yes** to confirm the deletion or **No** to cancel and return to the Enterprise Console previous state.

Working with Alerts

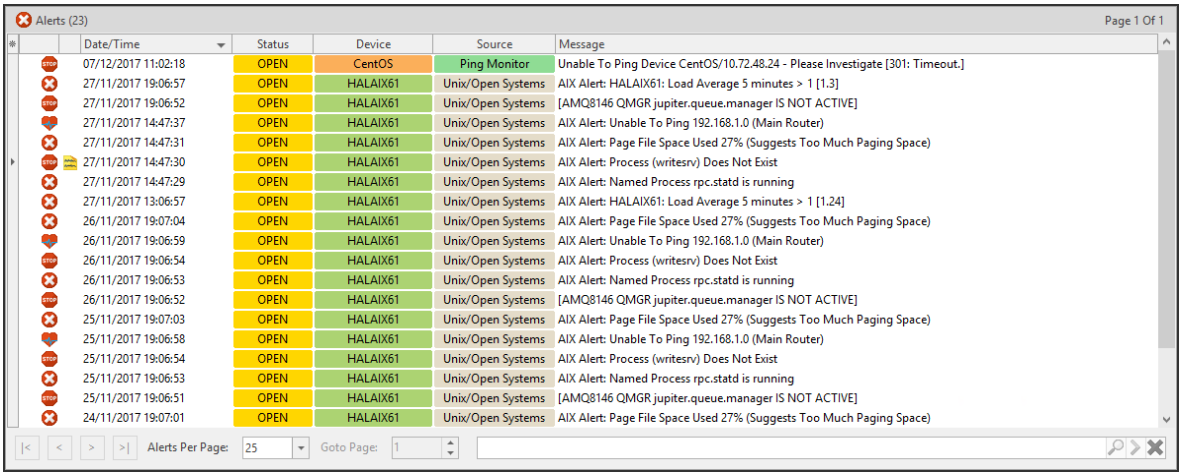
Alerts are generated as a result of rules that have been set up to monitor your network for any issues or problems. When alerts (that have an action of Send Console Action) are received they are displayed in the **Alerts** panel (by default) on the Enterprise Console.

Icons used when working with alerts are displayed from the **Home** option on the Enterprise Console tool bar.



Displaying Alerts

In its **Open** default view, the Alerts panel of Enterprise Console shows Open, Error, Console and Acknowledged alerts. Closed alerts can be viewed by selecting **Closed** from the **Home** menu ribbon.



Alert Status

In the **Open** view, alerts may have one of the following statuses:

- **Open**: The alert is open and has one or more actions against it.
- **Acknowledged**: The alert has been acknowledged and for IBM i alerts only, all outstanding actions against the alert have been canceled.

- **Console**: Indicates that an alert has been closed/replied to from the Enterprise Console. The alert remains visible until the console action has completed. Any pending actions are canceled when a user closes or replies to an alert.
- **Error**: The alert is open but one or more actions have failed.

Specifying the number of alerts displayed per page

Alerts are displayed in sequential pages within the **Alerts** panel. The default setting is to display 25 alerts per page.

To change the number of alerts displayed per page:

1. Locate the **Alerts Per Page** option in the footer of the **Alerts** panel.
2. Use the drop-down menu to select the new **Alerts Per Page** value. The possible values are 25, 50, 100, 200 and 500. It is not possible to enter a user-defined figure in this field.

The display changes to reflect the change. Depending on the change in value, other options in the **Alerts** panel become available or are made unavailable.

> TIP: Use the vertical scroll bar to view alerts included on the page but not visible as part of the initial view.

Goto page

If the number of alerts displayed per page exceeds the capacity of a single page in this panel, then additional pages become available. For example, if the **Alerts Per Page** setting is 100, and there are currently 346 alerts of a qualifying status in the system, then 4 pages will be available for selection.

To go to a different page of alerts:

To display a different page of alerts, use one of the following methods. Either:

- Over type the existing **Goto Page** value with a new page value. If the available page value is exceeded, the last page of alerts is returned. For example, If there are only 4 pages of alerts and 8 is entered in this field, the last available page of alerts is displayed.
- Use the **Goto Page** drop-down menu to select a new page value.

- Use the **Page Arrows** in the **Alert Page** footer to move between pages as follows:
  - Go to the next page of alerts
  - Go to the previous page of alerts
  - Go to the first page of alerts
  - Go to the last page of alerts

Searching for alerts

It is possible to search for a specific alert message text by entering text in the **Search** field in the **Alerts** panel footer.

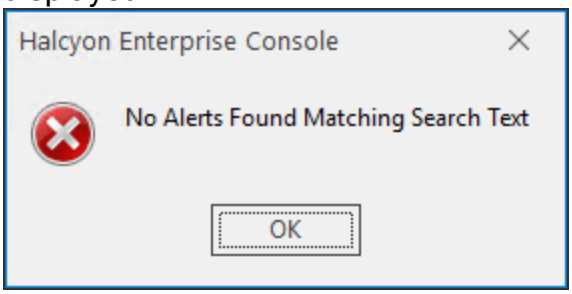
NOTE: The search option only operates on the current page of displayed alerts.

To search for specific alert text:

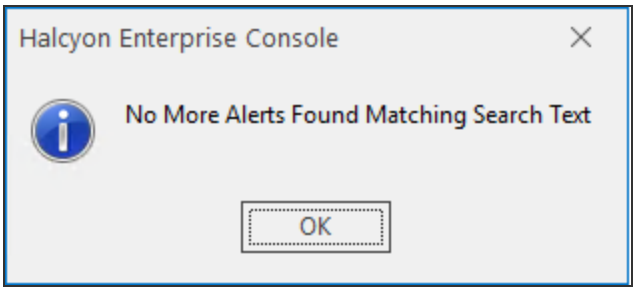
1. Type the text (either partial or full) of the alert message to be found on the current page and click **Search**.

   If the text is found, the first alert containing the full or partial text on this page is highlighted in the alert panel. Click **Next** to find the next instance of the search criteria on this page.

   If no message text matching the entered search string is found the following message is displayed.



   If there are no remaining alerts on the current page that contain the search text when **Next** is clicked, the following message is displayed.



2. Use **Delete** to remove the message text search criteria from the **Search** bar.

Selecting Alerts

Selecting alerts from the **Alerts** panel allows actions to be applied to single, multiple, consecutive or all alerts displayed in this panel.

To select a single alert:

1. Single-click directly on the alert line in the Alerts panel to highlight the alert. Actions can then be applied to this alert.

To select multiple, non-consecutive alerts:

1. Hold down the Ctrl key on the keyboard and left-click on each required alert line in the Alert panel to select. If a mistake is made, click again to remove the highlight.

To select multiple, consecutive alerts:

1. Hold down the SHIFT key on the keyboard and left-click on the first alert required for selection in the group.
2. Position the cursor to the last alert in the group to be selected and then left-click the last alert required for selection. All alerts in the group are now selected.
3. Release both the Shift key and the mouse button.

To select all alerts:

1. To select all alerts in the displayed **Alerts** panel page, click on any single alert.
2. Click **Select All** from the **Enterprise Console Home** menu ribbon. All alerts in the chosen panel are now selected.
3. To de-select all the alerts, click on a single alert within the panel. Only this alert is now selected.

Grouping Alerts

On occasions, host systems can legitimately generate hundreds or thousands of messages which Halcyon then processes and routes through to the Console. This is often described as a message storm.

The Enterprise Console has the ability to group alerts associated with a message storm within a single row on the display, with just the most recent alert visible. The main advantage of this feature is that it lessens the likelihood of important other alerts getting missed or scrolling off the bottom of the screen.

In order to be included in a group, alerts need to be from the same device and have identical alert text.

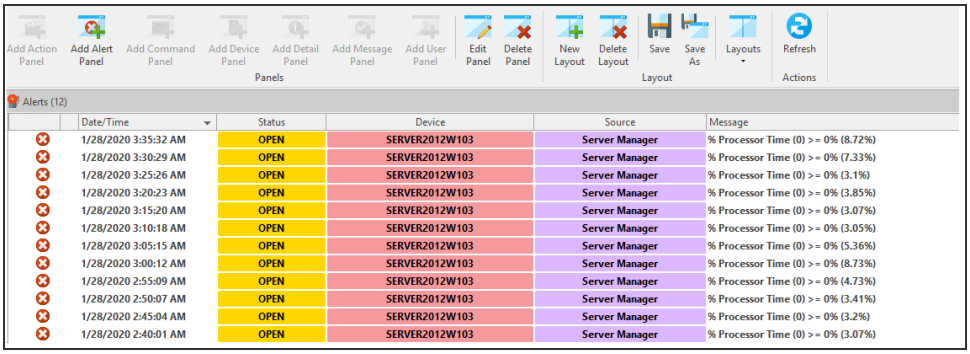
Setting up alert grouping

Alert grouping is set on a 'per panel' basis. In order to activate the grouping of alerts, each panel to which you want to apply alert grouping must be edited and the Group Alerts option selected.

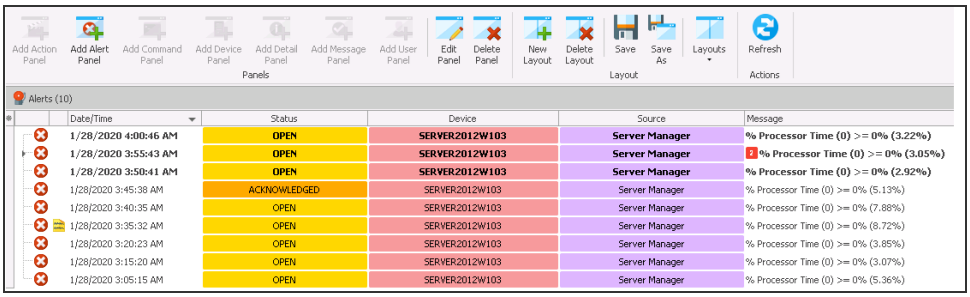
> **NOTE:** See Adding A New Layout - Grouping section for more information.

Display of Grouped Alerts

The first screen shot below shows a panel within the Enterprise Console where alert grouping has not been set. Note that all the alerts carry the same information.



When alert grouping has been activated, only one alert line appears on the display, but is marked with a '>' symbol in the far left column, indicating that more than one alert exist on this line. Click '>' to expand the group. The number of alerts contained within the group is displayed in the Message column as a white digit in a red square.



Closing Grouped Alerts

Grouped alerts can be closed individually or as a group. The grouping mechanism simply controls the method in which the alerts are displayed.

For example, you can close a group of alerts directly from the single displayed alert or you can expand the group and close the alerts individually. Additionally, you can still use SHIFT and select a series of adjoining alerts.

Alert Details

The Alert Details dialog is an enlarged version of the Alert Details panel in the Enterprise Console.

To open the View Alert Details dialog:

Do one of the following:

- Double-click an alert listed in the alert panel to display the full details of the individual alerts in the **Alert Details** dialog.
- Right-click on an alert listed in the alert panel and select **View Details** from the pop-up menu.
- Click on an alert to select and then click **View Details** from the Enterprise Console menu ribbon.

Alert information is displayed in a tree view within collapsible categories.

The default view of the **Alert Details** dialog is to show the expanded details of the alert in a series of panels.

Click the arrow next to the each panel header to close the panel and display just the header. Click again to expand the view.

Action History

In addition to the Alert Details being displayed, the current Action History for the selected alert is also shown at the bottom of the dialog.

Printing the Alert Details dialog

The full contents of the **Alert Details** dialog can be printed, either as hard copy or to a PDF. Click **Print** to open the Print dialog that provides a full range of printing options.

Alert Details Navigation

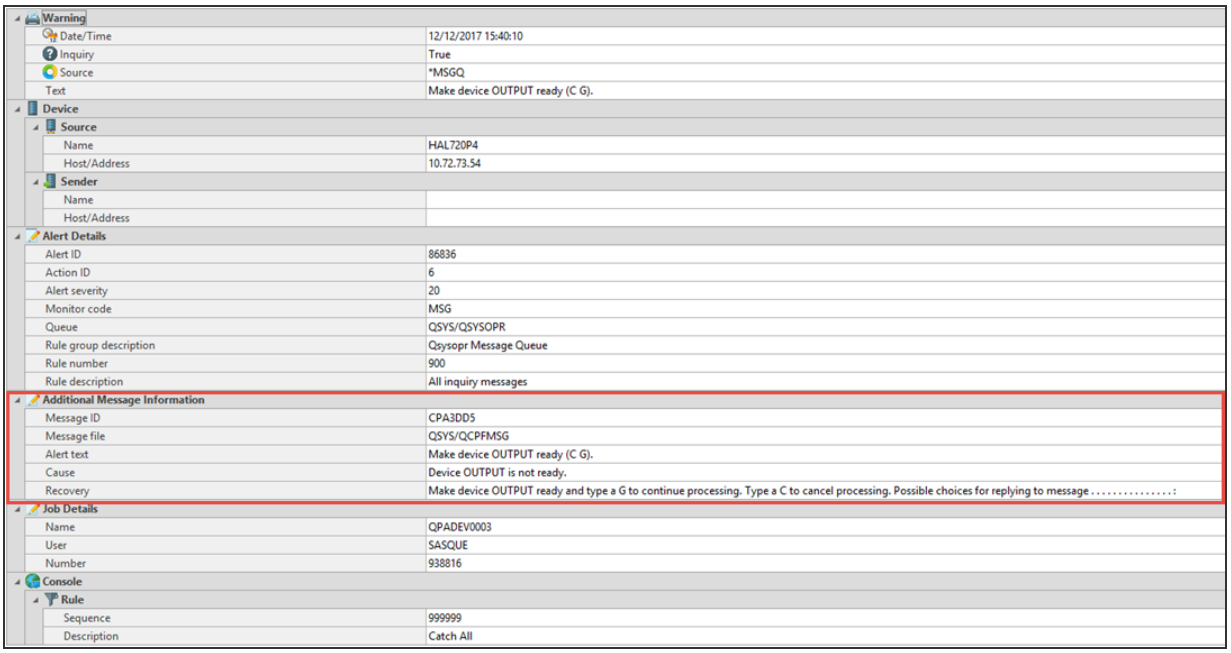
Four buttons along the bottom of the window allow you to navigate sequentially through alert details of all the alerts in the selected panel.

-  Go to the next alert
-  Go to the previous alert
-  Go to the last alert
-  Go to the first alert

Second Level Help Text

Second level help text can be displayed for applicable IBM i alerts. This information can assist in rectifying the problem that caused the alert to be generated.

If second level help text is available it is displayed as an Additional Information panel within the **Alert Details** dialog of the relevant IBM i alert.



Closing the Alert Details dialog

Click **Close** in the navigation bar to exit the **Alert Details** dialog.

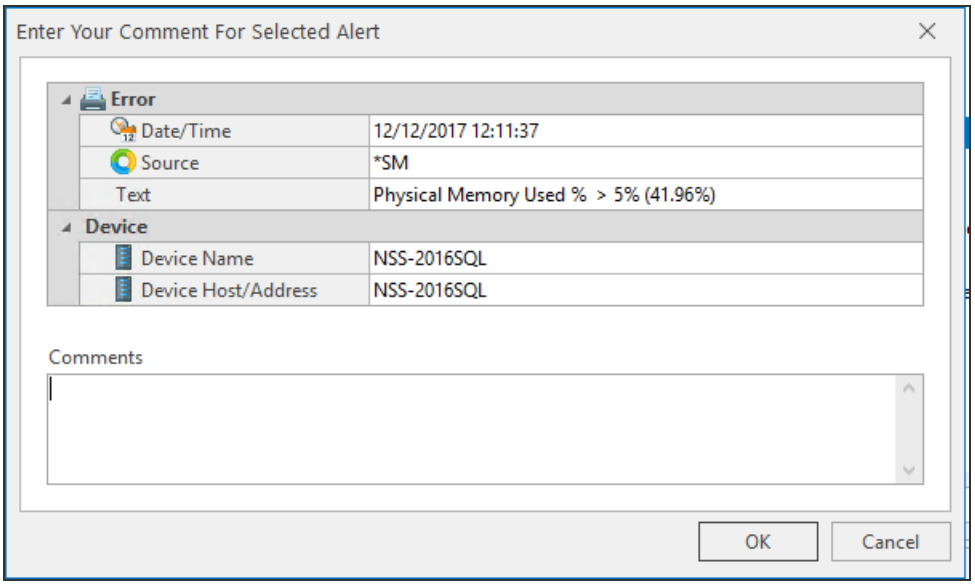
Adding Alert Comments

Comments can be used to add any miscellaneous text to an open alert in order to provide more information to any other Enterprise Console users.

To add comments to alerts:

Do one of the following:

- Select **Add Comment** from the Enterprise Console | **Home** menu ribbon.
- Right-click on the alert and select **Add Comment** from the pop-up menu.
- Select the alert and use Ctrl+N from the keyboard.



The top panel of this dialog, provides details of the alert.

Enter any free text comments in the **Comments** panel which are then be available against the alert.

Click **OK** to confirm the Comments entry.

Once added, the **Comment** icon is displayed next to the alert in the Alerts panel to make other users aware that comment text has been added.

TIP: Multiple comments can be added to a single alert.

Entered comments can be viewed in the Alert Details dialog.

Copying Alerts for use in Third Party Applications

Information held within an alert can be copied and exported (as a Paste command) into a third party application, such as Microsoft® Notepad.

To copy alert information:

Do one of the following:

- Select an alert and click **Copy** from the **Enterprise Console** | **Home** menu ribbon.
- Select an alert and right-click to display a pop-up menu. Select **Copy** followed by the option to be performed.

There are three options that can be used for copying alert information.

Copy Alert Detail

This option copies the complete detail of the alert message.

To copy the alert detail:

1. Select the required alert. Multiple alerts can be selected.
2. Click **Copy** and select **Detail** from the drop-down menu.

   The full alert detail is now copied and ready for pasting into a third party application.

Copy Alert Summary

This option copies just the following items of the alert:

- Date/Time
- Device
- Inquiry
- Product
- Source
- Text
- Type

To copy the alert summary:

1. Select the required alert. Multiple alerts can be selected.
2. Click **Copy** and select **Summary** from the drop-down menu.

   The alert detail is now copied and ready for pasting into a third party application.

Copy Alert XML

This option copies the same alert detail as in the Copy Detail function but in XML format.

To copy the alert detail in XML format:

1. Select the required alert. Multiple alerts can be selected.
2. Click **Copy** and select **XML** from the drop-down menu.

   The alert detail is now copied and ready for pasting into a third party application.

Replying to IBM i Inquiry Alerts

Inquiry alerts that arrive from IBM i devices must have a reply sent instead of being closed. The Close Alert option is unavailable for these types of alert. This process is used to send a recognized message back to IBM i.

Inquiry alerts are indicated by the **Question Mark** symbol in the **Status** column of the alert panel.

To reply to an inquiry alert:

Do one of the following:

- Select the IBM i inquiry alert and click **Reply** from the Enterprise Console | **Home** menu ribbon.
- Right-click on the IBM i inquiry alert and select **Reply** from the drop-down menu.

1. In the **Reply to Alert** dialog, type the required response.
2. Click **OK**. The inquiry alert is removed from the Enterprise Console.

Alerts received via forwarding systems

There may be instances where a direct connection cannot be made between the IBM i device and the Enterprise Console. In such instances it is possible to route the data via another IBM i device that does have a direct connection.

> **NOTE:** A guide on how to configure data forwarding from the IBM i is provided in the relevant Halcyon software suite or individual product user reference documentation. Please refer to this documentation when creating data forwarding routines.

From within the Enterprise Console, it is important to be able to identify the device from which the alert originated and not the devices that were used for the forwarding. The **Description** column provides descriptive text of the device and is used for identifying originating systems of forwarded alerts.

When an alert is received from a device that is not in direct connection with the Enterprise Console, the **Description** column displays both the originating and forwarding devices. Ensure that the Description column is displayed in the Alert panel in order to view this information.

> **NOTE:** This feature is not the same as the Forward Alert action.

Printing Alerts

There two options available when printing alerts.

- **Individual alert details**: The details of an individual alert.
- **Alert panel details**: The panel view (as shown on screen) containing multiple alert summaries but no individual alert details.

Both options use the same **Print Preview** display.

To print individual alert details:

1. From the alerts panel, double-click on the alert to open the **Alert Details** dialog.
2. Click **Print** to open the **Print Preview** dialog containing the alert details.

To print alert panel details

- From the alerts panel, click **Print** from the **Enterprise Console** | **Home** menu ribbon.

Print Preview

The following options are available on the **Print Preview** dialog:

Refresh

Click **Refresh** to update the report with any changes, such as added comments, to the alert detail or alert panel that have been made since the Print Preview Dialog was opened.

Print

Click **Print** to print the alert report with the current settings.

Print Dialog

Click **Print Dialog** to open the standard **Windows Print** dialog from where you can select the Printer, Page Range, Orientation and Number of Copies options.

Export To PDF

Click **Export To PDF** to open the **PDF Export Options** dialog which contains standard parameters for creating the printout as a Portable Document Format (PDF) file.

Page Setup

Click **Page Setup** to open the **Page Setup** dialog containing parameters that define how the detail appears on the page.

Page Settings

Use the Page setting options, **Whole**, **Two pages**, etc. to specify the number of alert pages that are displayed at any one time in the **Print Preview window**. This setting just affects the Print Preview view and not the actual printout.

> TIP: To generate more than one page of alerts for this option, increase the default value of 25 alerts per page to a higher value. Providing enough alerts exist in the database, options to view additional pages become available.

Zoom Settings

Use the **Zoom** settings to increase and decrease the view of the report on screen.

Page Width

Click **Page Width** to fit the view of the report into the full width of the **Print Preview** dialog,

Navigation Settings

If there is more than one page of alerts to view in the **Print Preview** dialog, use the **Navigation** arrows to move to the first page, previous page, next page and last page in the report.

Thumbnails

Click **Thumbnails** to display a panel showing thumbnail images of the pages of the printout.

View

Click **View** to display a series of quick links to margin settings and status views on the **Print Preview** dialog.

Margins

Use the **Margin** settings to quickly reposition the report data on the page. If not already displayed, Margins can be viewed by selecting **View** | **Margins** and **View** | **Margins Bar**.

Close Print Preview

Click **Close Print Preview** to close the dialog and return to the main Enterprise Console display.

Launching applications directly from Alerts

When an alert is received at the Enterprise Console it is possible to launch a remote desktop session to the device/application directly from the Enterprise Console, providing it was not sent from the device on which Enterprise Console is running.

Such sessions can take the form of, for example; Remote Desktop, VNC, PCAnywhere (Client Access when logging on to an IBM i machine).

> **NOTE:** In order to use this functionality the device must have an existing application association relationship created within Device Manager - Applications.

To launch an application directly from an alert:

Do one of the following:

- Highlight the alert and click **Launch Associated Application** from the **Enterprise Console** | **Home** menu ribbon.
- Right-click on the alert and select **Launch Associated Application** from the pop-up menu.
- Highlight the alert and use CTRL+L from the keyboard.

Follow the instructions as per the application used.

Sending Alerts to Third Party Help Desk Applications

Alerts can be sent to third party Help desk applications by using email to transmit the message detail.

> **NOTE:** The helpdesk application inbox or applicable email address must have been pre-defined in the Instant Alert Address Book prior to using this functionality.

> **TIP:** Use **Send Alert As Helpdesk Email (Default)** (Ctrl+H)to send the alert directly to the email address setting defined in the Enterprise Server Options Helpdesk settings to send the email without any further interaction.

To send an alert as a helpdesk email:

Do one of the following:

- Select the required alert (multiple selections are permitted), click  **Send Alert As** and select **Helpdesk Email** from the drop-down menu.
- Right-click on the alert and select **Send Alert As** | **Helpdesk Email** from the drop-down menu.
- Select the alert and use Ctrl+E from the keyboard.

The **Send Helpdesk Email** dialog is displayed.

1. Check the **From** option to allow an entry in this field enabling the receiving party to identify the originator of the message. It is also a requirement of some help desk applications that a recognized originating address is supplied, otherwise the email message can be rejected. The entry in this field must be in a format acceptable to the third party application.
2. Enter a valid **To** address. This is either that of the help desk application inbox or an address pre-defined in the Instant Alert Address Book. Click  to open the **Address Book**.
3. The **Subject** field is automatically completed from the alert, although this can be overwritten if desired.

   The **Content** of the email is based upon a selection of substitution variables. An example of the text as defined by the substitution variables is shown. The Content entry is automatically created from the alert but can be amended if required, using the substitution variables listed.
4. Click **OK** to send the email message to the defined help desk application.

Sending an Alert as an Email

Alerts can be sent as an email to any pre-defined email address in the Instant Alert Address Book.

To send an alert as an email

Do one of the following:

- Select the required alert (multiple selections are permitted), click  **Send Alert As** and select **Email** from the drop-down menu.
- Right click on the alert and select **Send Alert As** | **Email** from the pop-up menu
- Select the alert and use Ctrl+M from the keyboard.

The **Send Alert As Email** dialog is displayed.

1. Check the **From** option to allow an entry in this field enabling the receiving party to identify the originator of the message.
2. Enter a valid **To** address (pre-defined in the Instant Alert Address Book, opened by clicking  **Address Book**.
3. The **Subject** field is automatically completed from the alert, although this can be overwritten if desired.

   The **Content** of the email is based upon a selection of substitution variables. An example of the text as defined by the substitution variables is shown. The Content entry is automatically created from the alert but can be amended if required, using the substitution variables listed.
4. Click **OK** to send the email message.

Sending an Alert as an SMS

Alerts can be sent as an SMS to any pre-defined SMS contact address in the Instant Alert Address Book .

To send an alert as an SMS

Do one of the following:

- Select the required alert (multiple selections are permitted), click **Send Alert As** from the **Enterprise Console Home** menu ribbon and select **SMS** from the drop-down menu.
- Right click on the alert and select **Send Alert As** | **SMS** from the drop-down menu.
- Select the alert and use Ctrl+S from the keyboard.

The **Send Alert As SMS** dialog is displayed.

1. Check the **From** option to allow an entry in this field enabling the receiving party to identify the originator of the message.
2. Enter a valid **To** SMS address (pre-defined in the Instant Alert **Address Book**, opened by clicking **Address Book**.
3. The **Subject** field is automatically completed from the alert, although this can be overwritten if desired.

   The **Content** of the SMS is based upon a selection of substitution variables. An example of the text as defined by the substitution variables is shown. The Content entry is automatically created from the alert but can be amended if required, using the substitution variables listed.
4. Click **OK** to send the SMS to the selected recipients.

Acknowledging Alerts

Only alerts with a status of **Open** can be acknowledged. Closed alerts cannot be acknowledged.

The acknowledging of alerts is optional, and allows users in multiple environments to take ownership of individual alerts.

> **NOTE:** When acknowledging alerts received from IBM i devices, all pending actions set against the rule criteria that generated the alert are canceled.

To acknowledge an open alert

Do one of the following:

- Select the required open alert (multiple open alert selections are permitted), click **Acknowledge** from the **Enterprise ConsoleHome** menu ribbon.
- Right-click on the alert and select **Acknowledge** from the pop-up menu.
- Select the alert and use Ctrl+K from the keyboard.

When you select to acknowledge an alert, the **Acknowledge Alert** dialog is displayed. You may enter comments referring to the reason for the acknowledgment although this is not mandatory.

Acknowledging an alert changes the status to **ACKNOWLEDGED** when displayed in the alert panel.

Click **OK** to acknowledge the alert.

Closing Alerts

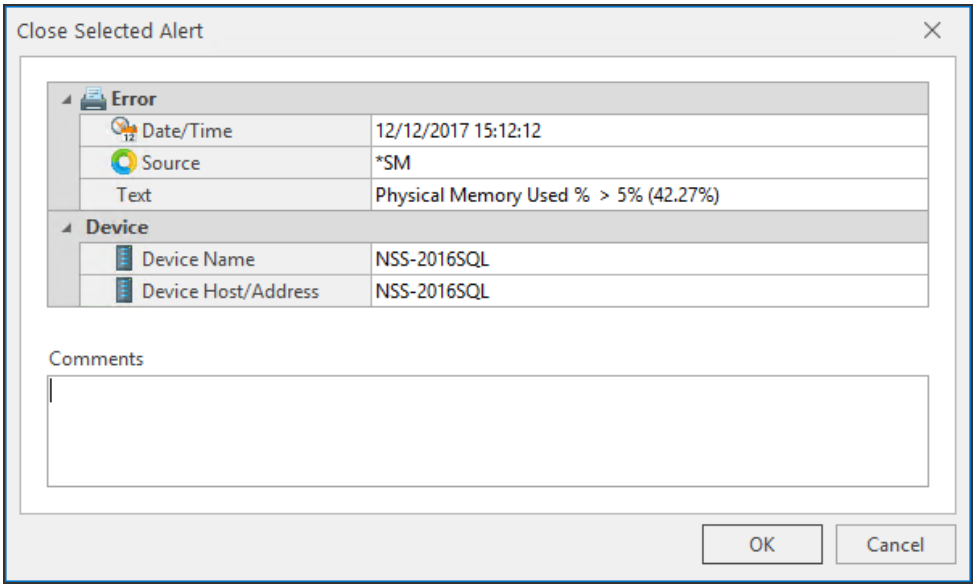
Alerts remain on the **Enterprise Console Open** alerts page, until they are closed at which point they disappear from the live console but can still be viewed using the Closed Alerts option. Multiple selections of alerts in a single Close operation are permitted.

To close an alert

Do one of the following from the **Open Alerts** view of Enterprise Console:

- Select the alert and click **Close** from the **Enterprise Console** | **Home** menu ribbon.
- Right-click on the alert and select **Close** from the pop-up menu.
- Select the alert and used Ctrl+C from the keyboard.

The **Close Selected Alert** dialog is displayed.



1. If required, and it is recommended, add a **Comment** for the reason of the closure of the alert.
2. Click **OK**.

The alert is now removed from the **Open Alerts** view of Enterprise Console.

Closing alerts received from IBM i devices

If an alert is being closed that has been generated by an IBM i, the close request is sent to the IBM i and the connection then closed.

The status of the alert changes to **CONSOLE** and it remains in this status until the IBM i connects back with a response.

Auto-Close Options

The Windows agent allows the auto-closure of alerts when the criteria condition that caused the alert no longer exists.

When creating a rule, within the Advanced tab of the rule criteria, an Auto-Close Options section is available.

The Auto-Close Enterprise Console Alerts parameter within the Auto-Close Options section of the Rule Criteria - Advanced tab defines whether Enterprise Console alerts for the rule are to be auto-closed and if there is any grace period before they are closed.

When the rule is checked, if the criteria selection would not currently result in an alert and there are previously raised outstanding alerts in existence, the existing alerts are closed after the specified **Delay** period if the criteria is still not triggering.

EXAMPLE:

- A CPU rule has criteria to alert if the CPU % Processor Time is above 75%.
- It also has Auto-Close specified to Auto-Close Enterprise Console Alerts with a Delay period of 5 minutes

The rule criteria is checked and triggers as the CPU is above 75%. An alert is sent to the Enterprise Console. At the next check interval, including any time for which the rule is suspended, the rule criteria is checked again and the CPU is below the required threshold. As the criteria has auto-close specified, the outstanding alert is tagged to be automatically closed five minutes later.

The rule criteria continues to be checked and if the CPU does not cause any further triggers, the existing alert is closed at the tagged auto-close time.

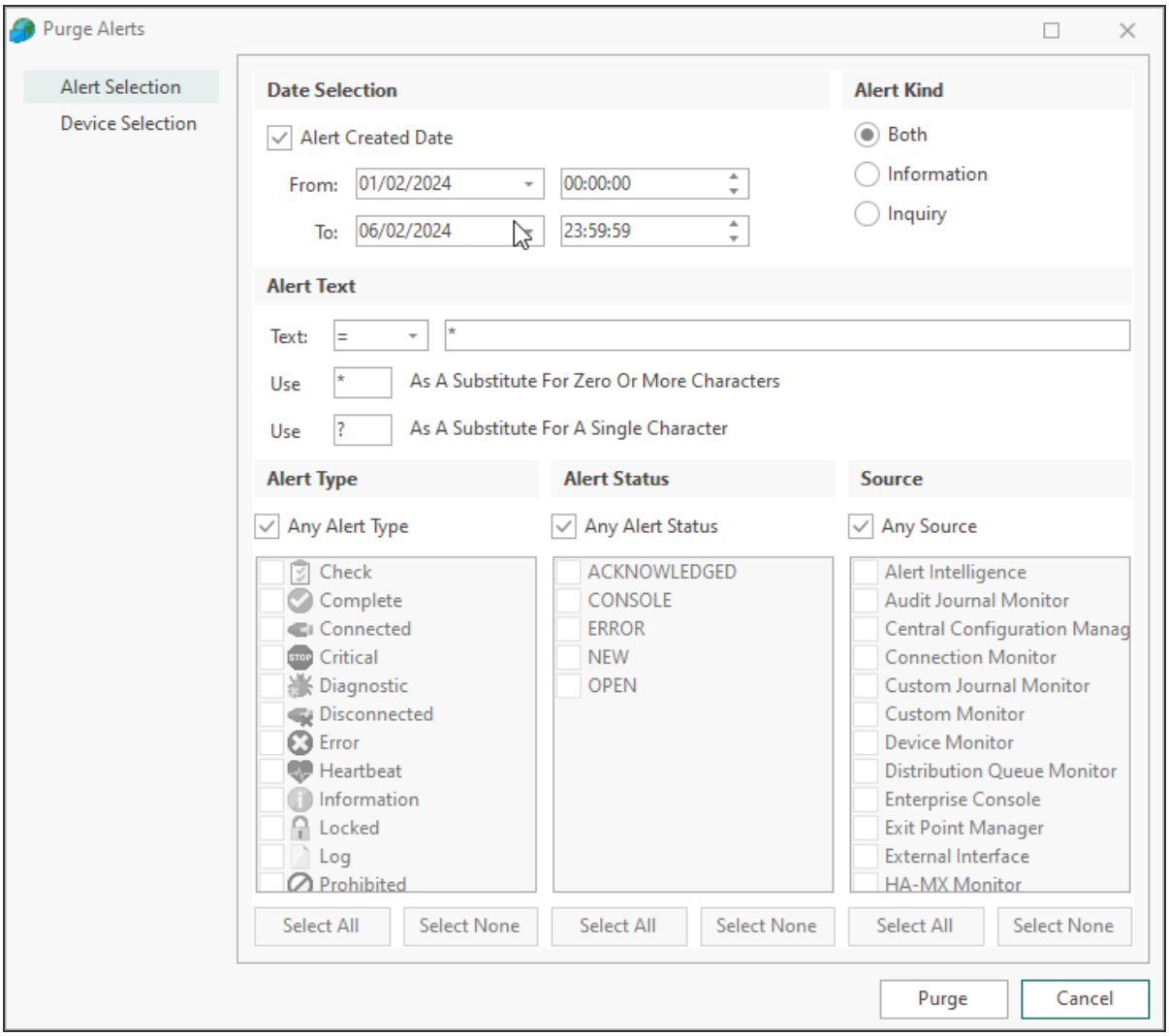
Purging Alerts

Purging alerts allows you to remove alerts from the database based on alert and device selection. At least one device must be selected for the purge action.

Alerts are purged using the **Purge Alerts** dialog.

To purge alerts

1. From the **Enterprise Console** menu bar, click .
2. From the drop-down menu select **Purge**.



Alert Selection page

Use the following sections to determine the alerts to be purged:

Date Selection section

The fields in this section define the dates and times between which alerts are purged.

Alert Created Date

Check this box to enable options to select alerts to be purged between a specified date and time range.

From Date/Time

The **From Date** field defaults to the first day of the current month and the **From Time** field defaults to midnight 00:00:00. Either over type the current entry or use the drop-down menu or arrows to select a new date/time.

To Date/Time

The **To Date** field defaults to the current date and the **To Time** field defaults to 23:59:59. Either over type the current entry or use the drop-down menu or arrows to select a new date/time.

Alert Kind

Select whether to purge just **Inquiry Alerts**, **Info Alerts** or **Both**. The default setting is Both.

Alert Text section

Text

Defines the alert text based on conditional parameters (equals, less than, greater than, etc.) when used in combination with entry in the subsequent field. This can be generic or free text and can also use specific textual values that vary depending on the type of alert to be purged. Wildcard characters can be used when defining this text.

Use ... As A Substitute For Zero or more Characters

Enter the character to use as a substitute for this search span. '*' is defined as the default search span character.

Use ... As A Substitute For A Single Character

Enter the character to use as a substitute for a single character. '?' is defined as the default single wildcard character.

Alert Selection section

The fields in this section define the status, type and originating source for alerts to be purged.

Alert Status

By default, alerts of any status are selected. Click the **Any Alert Status** box, to be able to select alerts by individual status type.

Alert Type

By default, alerts of any type are selected. Click the **Any Alert Type** box, to be able to select alerts by individual status type.

Source

By default, alerts from any source are selected. Click the **Any Source Type** box, to be able to select alerts by individual source type.

Select All

With the **Any Alert Status**, **Type** or **Source** defaults removed, use **Select All** to select all the entries in the corresponding panel.

Select None

With the **Any Alert Status**, **Type** or **Source** defaults removed, use **Select None** to remove the selection from all the entries in the corresponding panel.

Device Selection tab

The **Device Selection** tab is used to select the devices that currently hold the alerts to be purged.

Selected Devices section

This section shows the devices that are currently selected. When this tab is opened for the first time, this section is empty.

Information is listed in five columns:

- **Device Group**: Displays the name of the Device Group to which the device belongs.
- **Category**: Displays the category in which the device is defined.
- **Device Type**: Displays the Device Type of the device.
- **Name**: Displays the name of the device.
- **Address**: Displays the IP Address or Host name of the device.

Clear All

Click **Clear All** to remove all of the currently selected devices from selection.

Clear Selection

Highlight a device in the **Selected Devices** section and click **Clear Selection** to remove this device from selection. Multiple devices may be selected in one action.

Sorting columns

Column order can be rearranged by left-clicking on a column heading and keeping the mouse button depressed, dragging the column to the new position and releasing the button. Information in each column can be sorted in ascending or descending order by clicking on each column title to change the sequence.

Available Devices section

This section lists all of the devices that have been defined in Device Manager.

Filter options

These options allow the filtering of available devices on the network in order to restrict the list of available devices to just those that meet the filter criteria.

The categories comprise:

- **Device Group**: Device groups are collections of similar devices, such as all those that belong to a specific department. Device groups are set up and maintained in Device Manager
- **Category**: Devices, such as servers that can be divided into specific types. Items listed here are by default. No other items can be added to this list.
- **Device Type**: Device types, such as proxy servers are listed on this drop down and comprise a mix of default items and any other items identified on the network, which are automatically added to this list.

Add Device

To load a device into the **Selected Devices** section of this page, select the required device in the **Available Devices** section and click **Add Device** to move it into the **Selected Devices** section.

Show/Hide Selected

Click to show in the **Available Devices** section, only those devices not already listed in the **Selected Devices** table. This avoids duplicating device information in both tables. Click again to show all available devices, including those that have already been selected.

View Details

This button is used to open the **View Device** dialog, which displays the attributes of a selected device. No amendments can be made on this display. If changes are required, use Edit Device in Device Manager.

Deselect All

Click to deselect all of the currently selected devices in the **Available Devices** section.

Select All

Click to select all of the devices listed in the **Available Devices** section.

Click **Purge** to purge alerts that match the specified criteria.

Deleting Alerts

The delete alert action allows users with the appropriate authority to remove alerts from the Enterprise Console panels without the need to add comments or reply.

> **NOTE:** See User and Administrator Privileges for more details.

Single or groups of alerts can be deleted in one go by selecting the alerts to be deleted and then clicking **Delete Alert** from the Enterprise Console menu ribbon or by using right-click and selecting **Delete** from the pop-up menu.

You are then prompted to confirm the deletion.

No connection is made back to the originating system and so the delete action does not filter through to forwarded alerts.

Reloading Address Book

If you add entries to the Instant Alert address book while the Enterprise Console is open you can use the **Reload Address Book** option direct from the Enterprise Console without having to re-open Instant Alert.

To use the Reload Address Book option:

1. Select **File** |  **Reload** |  **Address Book** option from the Enterprise Console menu bar.

The Address Book is now updated with any changes since the Enterprise Console was opened.

Instant Alert

Overview

Instant Alert is the Halcyon component used to send text messages to mobile phones from either the Server Manager or Instant Alert. Email messages can also be sent.

Instant Alert has three separate modules:

Server Options

This module provides the parameters to configure Instant Alert and the way it interacts with other components.

Learn more about Instant Alert Server Options

Address Book

An address book is provided so that the details of frequently used contacts can be recorded.

Broadcast groups and schedules can be setup so messages are sent to the appropriate on-call personnel.

Learn more about Instant Alert Address Book

Message Sender

Message Sender is used to compose and send the actual messages.

A message log is provided to monitor the status of the messages.

The date/time of any message sent through Instant Alert is automatically adjusted to take account of any time zone settings. This assumes that the remote device from which the message is sent has been configured to specify a time zone other than the current local setting and that alerts are logged using the Remote Date/Time setting.

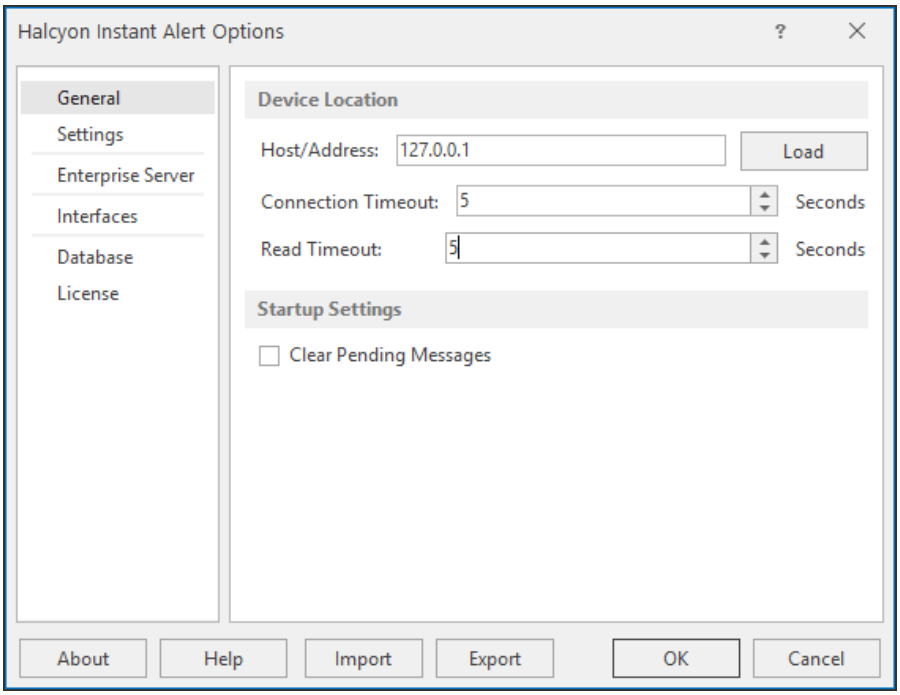
Learn more about Instant Alert Message Sender

Instant Alert Server Options

Instant Alert Server Options are used to configure various interfaces associated with Instant Alert and Enterprise ConsoleNetwork Server Suite.

To open Instant Alert Server Options select **Start** | **All Programs** | **Halcyon** | **IA Server Options**.

The **Instant Alert Options** dialog is displayed.



Instant Alert Server Options is split into six pages into which configuration information can be entered.

General page

This page is used to define the device location and start-up settings.

Device Location Settings section

Host/Address

If Instant Alert is running on another server from the main installation, enter the **Host/IP Address** of where Device Manager is installed and click **Load** to load recognized network devices. If all the components are installed on the same machine (recommended), the default setting of 127.0.0.1 can be retained.

Connection Timeout

Specify a time (in seconds) in which the connection to the selected device must be made before the session is deemed unsuccessful.

Read Timeout

Specify a time (in seconds) in which the data must be read from the device before the session is deemed unsuccessful.

Startup Settings section

Clear Pending Messages

Enable this option to clear any pending messages are cleared when Instant Alert is started. This is useful if a high volume of messages have been generated as the result of an error but are no longer required for information purposes. This type of message could include test messages, for example.

Settings page

This page is used to specify the informational and/or diagnostic messages that you want to record. Both types of message are useful should technical support need to investigate any issues or problems.

Message Log Settings section

Save to Log File

Click to enable the logging of Instant Alert informational and diagnostic messages.

> TIP: Instant Alert log files are stored in: **%Program Files%\ProgramData\Halcyon\Instant Alert\Logs**.

Maximum Log Size

The entry in this parameter specifies the maximum size of the log file. The default setting is 10240KB. You may need to increase this if both informational and diagnostic messages are being saved.

Log Informational Messages

Click to enable the logging of any Instant Alert information messages that are generated.

Log Diagnostic Messages

Click to enable the logging of any Instant Alert diagnostic messages that are generated.

Purge Settings section

Purge settings are used to set time periods after which various types of Instant Alert messages are purged. Purged Instant Alert messages are saved to the log file; PurgeManager.hlf.

Purge Closed Messages After

Use this option to specify the number of days after which closed messages are removed from the system. The default setting is 30 days.

Purge Error Messages After

Use this option to specify the number of days after which error messages are removed from the system. The default setting is 30 days.

Purge Old Pending Messages After

Use this option to specify the number of days after which any messages that are still in pending status are removed from the system. The default setting is 7 days.

Enterprise Server page

This page is used to specify on which server the Enterprise Server is installed. This ensures that any problems within Instant Alert are transmitted to the Enterprise Server device and then on to the Enterprise Console.

> **NOTE:** The entry on this page is usually selected as part of the Enterprise Console installation process.

Select Server

Click to open the **Select Device** dialog from where a new device, on which an instance of Enterprise Server must be installed, can be selected to replace the existing entry.

Single-click on the required device and then click **Select** to select the new device used to host Enterprise Server.

> TIP: Click **Details** to be able to view, but not amend, the details of any of the devices displayed in the **Select Device** dialog.

Clear Server

Click to clear the current server details from this display. A new device must be chosen in order for Instant Alert to be able interact again with Enterprise Server.

Interfaces page

This page shows the various interfaces currently defined on the system.

> NOTE: When Instant Alert Server Options is opened for the first time, this screen is empty.

See Working with Instant Alert Interfaces for more information regarding the options available from this dialog.

Database page

The Database page of Instant Alert Server Options allows you to view, but not amend, the current settings of the chosen database being used for Instant Alert.

License page

The License page shows the summary details of the license currently authorizing this product.

You can edit the details of the current license directly from this page.

See Editing Licenses for more information.

Export/Import Server Options

These options allow you to save and re-distribute Instant Alert Server settings between Windows devices, thus saving the need to re-enter information for each machine.

Export

Use **Export** to save the Instant Alert Server Options from one Windows device in order that they can be imported onto another.

Exporting Instant Alert Server Options exports:

- IA Settings
- Interfaces
- Address Book entries

The exported file is saved to a destination of your choice with a file extension of .ias.

Import

Use **Import** to upload a previously exported Instant Alert Server Options file to the current Windows device.

Browse to the location where the previously exported .ias file is saved, select the file and click **Import**.

Importing Instant Alert Server Options results in the following:

- IA Server Options are updated with imported values
- Interfaces are replaced with imported values
- Existing Address Book entries are updated if a match was found in the imported values otherwise new members will be added.

Instant Alert Interfaces

There are three types of interface that can be used with Instant Alert.

GSM interface

GSM (Global System for Mobile Communications) is a standard to describe the protocols for second-generation digital cellular networks used by mobile devices.

A GSM modem is a specialized type of modem which accepts a SIM card (required for successful Instant Alert operation), and operates over a subscription to a mobile operator, just like a cell phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network.

Attaching a GSM data terminal to the device on which Instant Alert is installed, allows SMS messages and email to be sent (as an action) from the Enterprise Server. The message can be sent to nominated contacts held in the Instant Alert Address Book.

NPort interface

A NPort device is a small data communications device that allows control of RS-232 serial devices over a TCP/IP-based Ethernet and can be used as an interface between multiple GSM devices and a server.

Most NPort interfaces support Simple Network Management Protocol (SNMP), which can be used to send trap messages automatically to the SNMP manager when user-defined errors are encountered.

SMTP interface

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission.

> **NOTE:** Instructions on how to attach and configure GSM and NPort NETGSM terminals on the network can be found in the current version of the Enterprise ConsoleNetwork Server Suite InstallationConfiguration Guide.

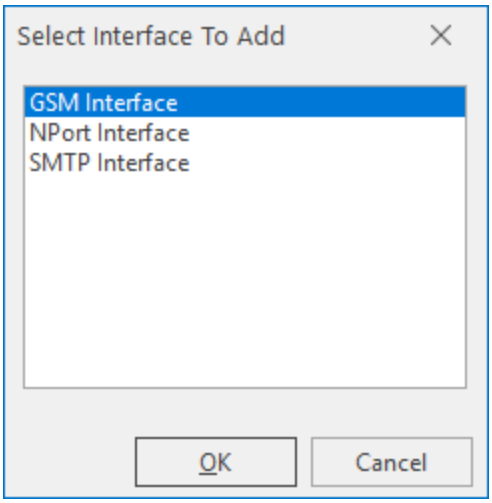
Adding Instant Alert Interfaces

Interfaces are added using the Server Options component of Instant Alert.

To open Instant Alert Server Options select **Start** | **All Programs** | **Halcyon** | **IA Server Options**.

From the Halcyon **Instant Alert Options** dialog select the **Interfaces** page.

Click **Add** to open the **Select Interface To Add** dialog.



Adding a GSM Interface

WARNING: If you use a GSM data terminal, it must be installed on the same machine as Instant Alert.

1. On the **Select Interface To Add** dialog, click **GSM Interface**.
2. Click **OK**.

The **Add GSM Interface** dialog is displayed.

When adding a GSM Interface there are five pages of field definitions to complete.

General page

This page contains fields that define the general settings of the GSM interface.

General Details section

Description

If the default entry of **GSM Interface** is insufficient, enter a textual description of the GSM Interface.

Backup

If this interface is going to be the primary interface for Instant Alert then leave the Backup option unchecked. Only enable this option if this interface is intended as a secondary interface should another defined interface fail.

Prefix Settings section

Prefix Date And Time To Message

Select this option to prefix all messages, sent via this interface, with the date and time at which the message is sent.

Prefix Message Reference To Message

Select this option to prefix all messages, sent via this interface, with a unique message reference. This can be useful for message identification purposes.

Advanced page

New Message Processing section

Process Immediately

Select this option to send the message the instant that is created.

Process Every nn Minute

Select this option to batch process all messages received between instances of the specified time interval (where nn is equal to the number of minutes). The default setting is 1 minute.

Message Sending section

Delay Between Messages

If required, specify the time delay, in milliseconds, between which messages are sent. The default setting is 250 milliseconds.

Interface section

When In Error, Retry Connection Every nn Minutes

Specify the time delay, in minutes, between which a connection attempt to the GSM interface is retried, should the interface be found to be in error. The default setting is 2 minutes.

Logging page

This page contains fields that define logging options for the GSM interface.

Message Log Settings section

Save To Log File

Select this option to enable the logging of messages for the GSM interface.

Maximum Log File Size

Specifies the maximum file size allowed for the logging of messages. This defaults to 10240 KB. You may want to consider increasing this value if you are logging both Informational and Diagnostic messages for this interface.

Log Informational Messages

Select this option to log any informational messages that may be generated by this GSM interface.

Log Diagnostic Messages

Select this option to log any informational messages that may be generated by this GSM interface.

Log Debug Messages (SMTP Interfaces only)

Select this option to enable additional logging to be recorded for any email issues that may arise through the use of an SMTP interface. Additional logging is recorded in the SMTP_*.HLF file.

Error page

Retry Settings section

Retry Sending Messages In Error

Select this option to enable the resend of any messages that end in error while being sent.

Retry Count

Specifies the number of retries that are allowed per message before the attempt to send is deemed unsuccessful.

Retry Interval

Specifies the frequency with which the message is attempted to be resent. This setting can be either specified in seconds or minutes.

Settings page

Communications Port section

Port Number

Enter the Communications Port Number on the PC to which this GSM interface is attached. The default setting is COM1.

Speed

Select the transmission rate speed. If using a TC65 GSM terminal use 115200.

Command Timeout

Specify the time allowed, in seconds, for the Communications Port to recognize that a command is being sent. The default setting is 15 seconds.

Message Options section

Truncate Message To nn Pages

Specifies the number of pages to which to limit the size of long messages. The default setting is 3 pages.

> WARNING: Limiting the message size too severely in this field, may result in vital information being omitted from messages.

Use Concatenation Mode

Select to enable the joining of successive messages when the number of characters per message exceeds the permissible length.

Character Options section

Character Set

Specify the character type in which messages are sent via the GSM interface.

- **Automatic**: Attempts to translate a UCS2 message into 7-bit
- **7 bit**: Uses the ASCII character set
- **UCS2**: Double Byte character set used for non-basic text

> NOTE: Any messages sent in UCS2 format use double characters so a 160 character text will only contain 80 readable characters.

Click **OK** to add the new GSM interface.

Adding an NPORT Interface

> WARNING: If you use an NPORT GSM data terminal, it must be installed on the same machine as Instant Alert.

1. On the **Select Interface To Add** dialog, click **NPORT Interface**.
2. Click **OK**.

The **Add NPort Interface** dialog is displayed.

When adding an NPORT Interface there are five pages of field definitions to complete.

General page

This page contains fields that define the general settings of the NPORT interface.

General Details section

Description

If the default entry of **NPort Interface** is insufficient, enter a textual description of the NPort Interface.

Backup

If this interface is going to be the primary interface for Instant Alert then leave the Backup option unchecked. Only enable this option if this interface is intended as a secondary interface should another defined interface fail.

Prefix Settings section

Prefix Date And Time To Message

Select this option to prefix all messages sent via this interface with the date and time at which the message is sent.

Prefix Message Reference To Message

Select this option to prefix all messages sent via this interface with a unique message reference. This can be useful for message identification purposes.

Advanced page

This page contains fields that define the message processing options.

New Message Processing section

Process Immediately

Select this option to send the message the instant that is created.

Process Every nn Minute

Select this option to batch process all messages received between instances of the specified time interval (where nn is equal to the number of minutes).

Message Sending section

Delay Between Messages

If required, specify the time delay, in milliseconds, between which messages are sent.

Interface section

When In Error, Retry Connection Every nn Minutes

Specify the time delay, in minutes, between which a connection attempt to the NPORT interface is retried, should the interface be found to be in error.

Logging page

This page contains fields that define the logging options for the NPORT interface.

Message Log Settings section

Save To Log File

Select this option to enable the logging of messages for the NPORT interface.

Maximum Log File Size

Specifies the maximum file size allowed for the logging of messages. This defaults to 10240 KB. You may want to consider increasing this value if you are logging both Informational and Diagnostic messages for this interface.

Log Informational Messages

Select this option to log any informational messages that may be generated by this NPORT interface.

Log Diagnostic Messages

Select this option to log any informational messages that may be generated by this NPORT interface.

Error page

This page contains fields that define the settings for resending messages that are in error status.

Retry Settings section

Retry Sending Messages In Error

Select this option to enable the resend of any messages that end in error while being sent.

Retry Count

Specifies the number of retries that are allowed per message before the attempt to send is deemed unsuccessful.

Retry Interval

Specifies the frequency with which the message is attempted to be resent. This setting can be either specified in seconds or minutes.

Settings page

This page contains fields that are used to specify communication, message and character set options.

Network Settings section

IP Address

Enter the unique IP Address for this NPORT device on the network.

Port Number

Enter the Communications Port Number on the PC to which this NPORT interface is attached. This parameter defaults to Port 4001.

Command Timeout

Specify the time allowed, in seconds, for the Communications Port to recognize that a command is being sent. The default setting is 15 seconds.

Message Options section

Truncate Message To nn Pages

Specifies the number of pages to which to limit the size of long messages. The default setting is 3 pages.

> WARNING: Limiting the message size too severely in this field, may result in vital information being omitted from messages.

Use Concatenation Mode

Select to enable the joining of successive messages when the number of characters per message exceeds the permissible length.

Character Options section

Character Set

Specify the character type in which messages are sent via the NPORT interface.

- **Automatic**: Attempts to translate a UCS2 message into 7-bit.
- **7 bit**: Uses the ASCII character set.
- **UCS2**: Double Byte character set used for non-basic text.

> NOTE: Any messages sent in UCS2 format use double characters so a 160 character text will only contain 80 readable characters.

Click **OK** to add the new NPORT interface.

Adding an SMTP Interface

1. On the **Select Interface To Add** dialog, click **SMTP Interface**.
2. Click **OK**.

The **Add SMTP Interface** dialog is displayed.

When adding an SMTP Interface there are six pages of field definitions to complete.

General page

This page contains fields that define the general settings of the SMTP interface.

General Details section

Description

If the default entry of **SMTP Interface** is insufficient, enter a textual description of the SMTP Interface.

Backup

If this interface is going to be the primary interface for Instant Alert then leave the Backup option unchecked. Only enable this option if this interface is intended as a secondary interface should another defined interface fail.

Prefix Settings section

Prefix Date And Time To Message

Select this option to prefix all messages sent via this interface with the date and time at which the message is sent.

Prefix Message Reference To Message

Select this option to prefix all messages sent via this interface with a unique message reference. This can be useful for message identification purposes.

Advanced page

This page contains fields that define message processing options.

New Message Processing section

Process Immediately

Select this option to send the message the instant that is created.

Process Every nn Minute

Select this option to batch process all messages received between instances of the specified time interval (where nn is equal to the number of minutes).

Message Sending section

Delay Between Messages

If required, specify the time delay, in milliseconds, between which messages are sent.

Interface section

When In Error, Retry Connection Every nn Minutes

Specify the time delay, in minutes, between which a connection attempt to the SMTP interface is retried, should the interface be found to be in error.

Logging page

This page contains fields that define logging options for the SMTP interface.

Message Log Settings section

Save To Log File

Select this option to enable the logging of messages for the SMTP interface.

Maximum Log File Size

Specifies the maximum file size allowed for the logging of messages. This defaults to 10240 KB. You may want to consider increasing this value if you are logging both Informational and Diagnostic messages for this interface.

Log Informational Messages

Select this option to log any informational messages that may be generated by this SMTP interface.

Log Diagnostic Messages

Select this option to log any informational messages that may be generated by this SMTP interface.

Error page

This page contains fields that specify settings for resending messages that are in error status.

Retry Settings section

Retry Sending Messages In Error

Select this option to enable the resend of any messages that end in error while being sent.

Retry Count

Specifies the number of retries that are allowed per message before the attempt to send is deemed unsuccessful.

Retry Interval

Specifies the frequency with which the message is attempted to be resent. This setting can be either specified in seconds or minutes.

Server page

This page contains fields that define the details of the server used to send messages via this interface.

> **NOTE:** On first opening, no device has been specified so **Unknown Device** is displayed.

SMTP Server section

Port Number

Enter the port number on which this SMTP server interface connects. The default setting is 25.

Uses SSL/TLS Mode

Click this setting to specify that the server used for SMTP messages supports and uses Transport Layer Security (TLS) or Secure Sockets Layer (SSL). These are both cryptographic protocols that provide communications security over a computer network.

Select Server

Click **Select Server** to select the server to be used for SMTP messages (this device must have already been loaded using Device Manager). Highlight the required device and click **Select**.

Settings page

This page contains fields used to message and server authentication options.

Email Settings section

Override From Name/Address

Select this option to enable the overriding of the From Name/Address parameters for emails sent from this interface. If you do not enable this setting, emails are generated using the machine details.

From Name

Enter the name of the person from which you want emails sent via this interface to be addressed.

Email Address

Enter the email address of the person identified in the **From Name** parameter.

Authentication Settings section

Server Requires Authentication

Select this option if the server requires authentication in order to send messages.

User Name

Enter the user name required to authenticate this server.

Password

Enter the password associated with the entered **User Name**.

Click **OK** to add the new SMTP interface.

Working with Instant Alert Interfaces

Once Instant Alert Interfaces have been defined, they can be edited, deleted, held, and released.

Editing Instant Alert Interfaces

Should a change be required in the Interface configuration, the **Edit** option can be used to amend the current settings.

To edit an existing Interface:

1. Select **Start** | **All Programs** | **Halcyon** | **IA Server Options**.
2. From the Halcyon **Instant Alert Options** dialog select the **Interfaces** page.
3. Single-click on the **Interface** to be edited so that it is highlighted.
4. Click **Edit** to open the **Edit Interface** dialog.
5. The Interface can now be re-configured using the same fields as when it was added.

Deleting Instant Alert Interfaces

Should an Interface no longer be required, it can be removed using the **Delete** option.

To delete an existing Interface:

1. Select **Start** | **All Programs** | **Halcyon** | **IA Server Options**.
2. From the Halcyon **Instant Alert Options** dialog select the **Interfaces** page.
3. Single-click on the **Interface** to be deleted so that it is highlighted.
4. Click **Delete**.
5. When prompted, click **Yes** to delete the Interface from Instant Alert.

Holding Instant Alert Interfaces

It is possible to temporarily hold an Interface, rather than deleting it. This may be required for troubleshooting or maintenance requirements. No messages can be passed through the Interface while it is in a held state.

To hold an existing Interface:

1. Select **Start** | **All Programs** | **Halcyon** | **IA Server Options**.
2. From the Halcyon **Instant Alert Options** dialog select the **Interfaces** page.

3. Single-click on the **Interface** to be held so that it is highlighted.
4. Click **Hold**. A green tick mark  is displayed in the **Held** column of the **Interfaces** page to indicate that this Interface is now held.

The Interface can be made available for use again by using the Release option.

Releasing Instant Alert Interfaces

Once an Interface has been held, it can be released again for use in Instant Alert by using the **Release** option.

To release an existing Interface:

1. Select **Start** | **All Programs** | **Halcyon** | **IA Server Options**.
2. From the Halcyon **Instant Alert Options** dialog select the **Interfaces** page.
3. Single-click on the **Interface** that is in **Held** status so that it is highlighted.
4. Click **Release**.

The Interface is now available for use in Instant Alert.

Address Book

Instant Alert Address Book is the component used to add, edit and delete the following:

Contacts and Contact Details

Contacts are the people to which the details of any issues need to be communicated. Contacts may be internal or may belong to third party organizations. A comprehensive set of fields is available into which detailed information regarding the contact can be entered.

This information must be entered manually for each contact and a default message type (SMS or email) must be specified.

> TIP: The default message type can be overwritten by the message type selected from within Enterprise Server Options | Email/SMS Defaults.

Broadcast Groups

A broadcast group is a team of people who have an interest in a specific function or routine and allows all members of the group to receive instant email notifications or SMS for any issues that arise.

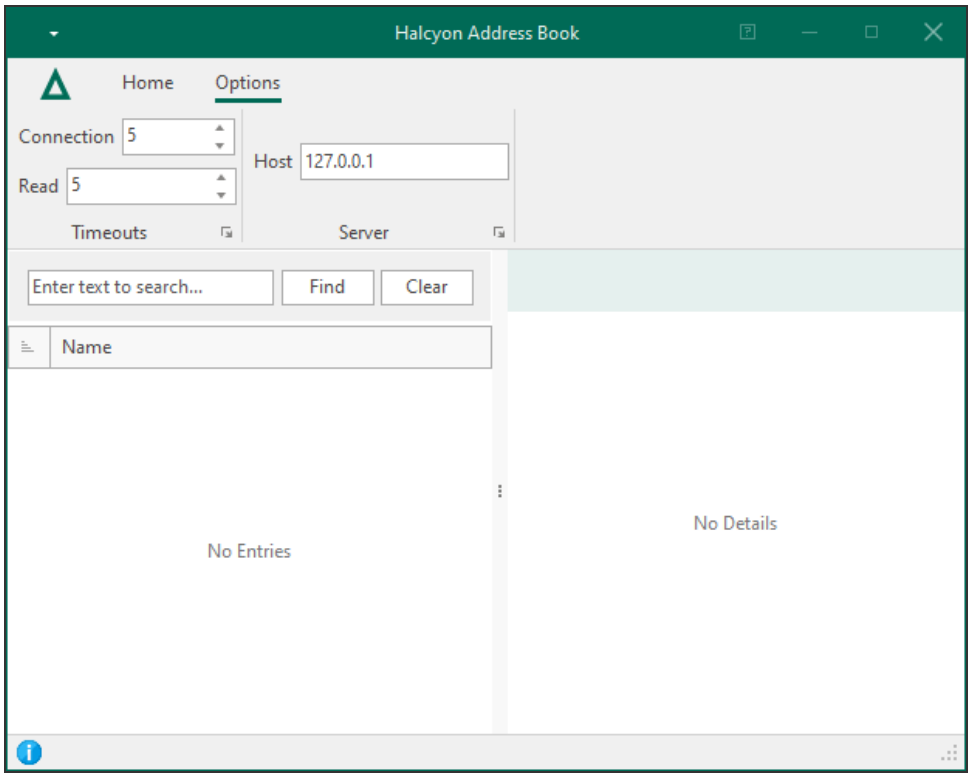
Call Schedules

A call schedule, often called a rota or roster, is a list of employees with responsibilities for a given time period. A call schedule is a method of ensuring that the correct person is contacted at the right time, in the event of an alert being raised.

Address Book Options

Use the Instant Alert **Address Book Options** to specify details of the server on which Instant Alert is installed, together with any connection timeout settings.

1. Open the Address Book using Windows **Start** | **All Programs** | **Halcyon** | **Address Book**.
2. From the menu bar, select **Options**. The menu ribbon changes to display the current Address Book option settings.



The following fields are available on the **Address Book Options** menu ribbon.

Timeouts panel

Connection Timeout

Specify the time, in seconds, after which Instant Alert a connection attempt to the PC specified in the **Host/Address** field is deemed unsuccessful.

Read Timeout

Specify the time, in seconds, after which data must be read from the device before the action is deemed unsuccessful.

Server panel

Host / Address

Enter the **Host Name** or **IP Address** of the PC on which Instant Alert is installed. This defaults to the local IP address of **127.0.0.1**.

Click **OK** to confirm and save the **Address Book Options** settings.

Finding Address Book Entries

If you have many address book entries configured within Instant Alert you can use the Search facility to pinpoint the entry that you want.

Begin typing the alphanumeric characters of the address book entry) that you want to find in the defined list. Click **Find** to move to the located entry in the list (providing that a match is made). Click **Clear** to remove the search criteria from the field.

Contacts

Should any issues arise from the system monitoring, contacts are the people to which the details need to be communicated.

Once added to the Address Book, contacts are available to be added to Call Schedules and Broadcast Groups.

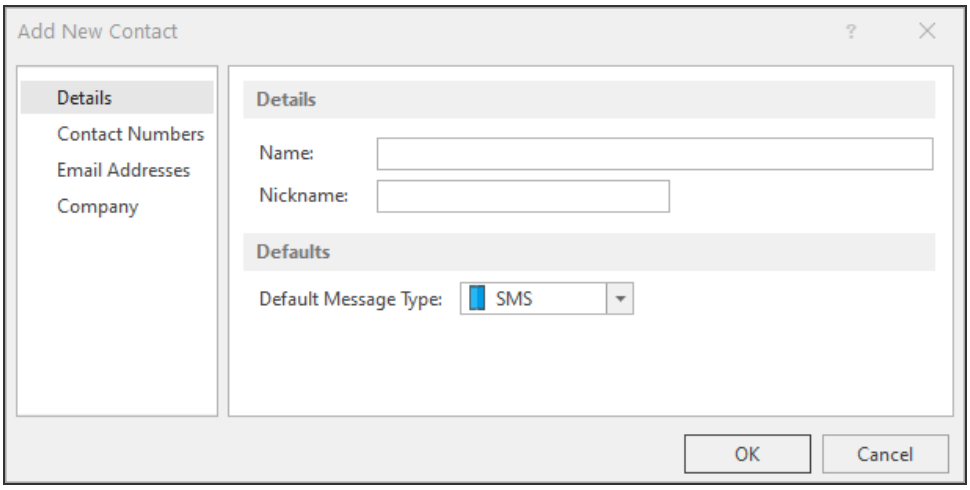
Adding a Contact to the Instant Alert Address Book

Unlimited contacts can be added to the Address Book. To be available for use in Broadcast Groups and Call Schedules, contacts must exist in the Address Book.

To add a new contact to the Instant Alert Address Book:

1. Click **Add** from the **Members** panel of the **Home** menu ribbon.
2. From the drop-down choice menu, select **Contact**.

The **Add New Contact** dialog is displayed.



This dialog consists of four separate pages into which contact information can be entered.

Details page

This page is used to enter the name and personal details of the contact.

Details section

Name

Enter the full name (First and Second name) of the contact.

Nickname

If required, enter the nickname by which this contact is known.

Defaults section

Default Message Type

Select the default method of sending a message to this contact. This can either be email or SMS.

Contact Numbers page

The contact numbers page shows the details of all contact numbers currently held in the Address Book for the contact.

The default message type, and cell phone number are displayed for this contact.

See Adding a Contact Number for instructions on how to enter this information for a contact.

Email Addresses page

This page shows the details of all email addresses currently held in the address book for the contact.

The email address details are displayed for this contact.

See Adding an email address for instructions on how to enter this information for a contact.

Company page

This page shows the details of the company and the that employs the contact.

Company section

Company

Specifies the name of the company for which this contact works.

Job Title

Specifies the job title of this contact.

Address

Specifies the first lines of the address of the company where this contact works.

City

Specifies the city in which the company for which this contact works is located.

County

Specifies the county (state) in which the company for which this contact works is located.

Postcode

Specifies the postcode (zip code) of the address of the company where this contact works.

Country

Specifies the country in which the company for which this contact works is located.

Group Code

In large organizations, this field can be used as a location or department identifier for the home address of the contact.

Website

Specifies the company website address for which this contact works.

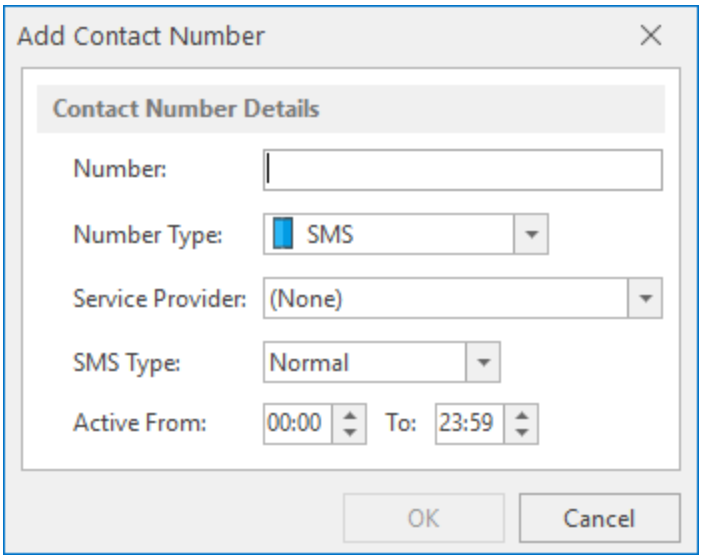
Adding a Number to a Contact

A contact number may be added as part of the process when a new contact is created. If the contact will only be contacted via email then this step can be omitted.

> WARNING: A contact must have either at least one contact number or email address defined against it before it can be saved to the database.

To add a number to a contact:

1. From the **Address Book - Contact Numbers** panel, click **Add** to open the **Add Contact Number** dialog.



The following fields are available to enter contact number details.

Number

Enter the number of the cell phone on which the person can be contacted.

Number Type

Only SMS is currently available in this field.

Service Provider

This field is not used in this release.

SMS Type

Select either **Normal** or **Flash** as the **SMS Type**. Flash messaging is a method of sending SMS messages to any phone, even if it is locked.

Active

Specify the times between which this phone is active for the receipt of messages sent via Instant Alert. If the message is sent to the phone outside of the period when the phone is active, it is queued and then sent as soon as the phone becomes available again.

2. Click **OK** to add the contact number to the contact.

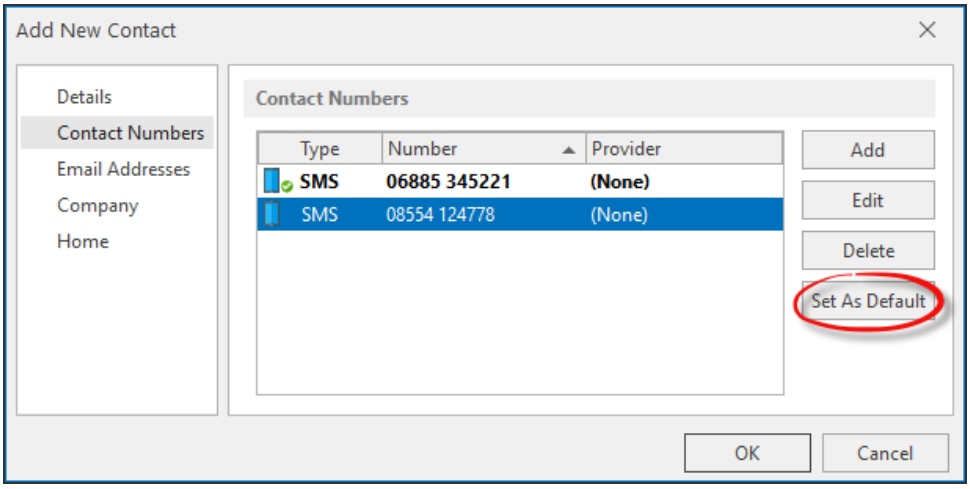
Working with Contact Numbers

The following section describes the options for working with contact numbers.

Setting a Contact Number as a Default

The default contact number is displayed in the **Contact Numbers** panel as having a green tick mark in the bottom right corner of the SMS icon.

From the **Add/Edit Contact** dialog and the **Contact Numbers** panel, highlight an entry and click **Set As Default** to use that number as the main number for the selected contact.



NOTE: The first contact number defined for this contact is automatically set as the default. This option is only available if there is more than one number specified for the contact.

Editing a Contact Number

Should a contact update their cell phone details, or the times of its availability change, it is possible to edit an existing entry to the new number.

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** for which the number information has changed.
3. From the **Home** | **Members panel**, select **Edit**. The **Edit Contact** dialog is displayed.
4. From the left navigation panel select **Contact Numbers**.
5. From the **Contact Numbers** panel select the number to be edited and click **Edit**.
6. The details of the number can now be edited using the same fields as when adding

the contact number.

7. Click **OK** to confirm the changes.

Deleting a Contact Number

Should a contact no longer have their cell phone, it is possible to remove the number.

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** for which the number is no longer required.
3. From the **Home** | **Members** panel, select **Edit**. The **Edit Contact** dialog is displayed.
4. From the left navigation panel select **Contact Numbers**.
5. From the **Contact Numbers** panel select the number to be deleted and click **Delete**.
6. When prompted, click **OK** to confirm the deletion.

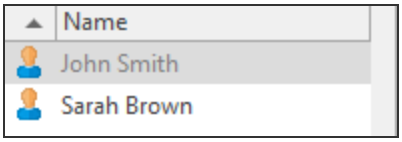
NOTE: If the default contact method is SMS, at least one number must remain available for the contact.

WARNING: Deleting a number also removes it from any Broadcast Groups or Call Schedules to which it belongs.

Working with Contacts

Once Instant Alert Contacts have been defined, they can be edited, deleted, copied and renamed. A search facility is also provided should an extensive list of contacts exist.

Contacts are displayed alongside call schedules and broadcast groups in the left-hand panel of the Address Book and, by default, are listed in alphabetical order.



TIP: The sort order can be reversed by clicking the arrow next to **Name** in the heading section of this panel.

Editing Contacts

The current details of any contact can be amended at any time. For assistance with editing a contact number please see: Editing a contact number.

> **NOTE:** It is not possible to amend the contact name using the Edit function. Use the Rename function instead.

To edit the details of an existing contact:

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** for which the information has changed.
3. From the **Home** | **Members** panel, select **Edit**. The **Edit Contact** dialog is displayed.
4. Use the same parameters as when adding a contact to update the contact information.
5. Once complete, click **OK** to confirm and save the changes.

Deleting Contacts

If a contact has left, or has changed roles and no longer needs to be informed of any system monitoring issues, they can be removed from the Address Book. For assistance with removing a contact number please see: Deleting a contact number.

To delete an existing contact:

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** that is to be removed from the Address Book.
3. From the **Home** | **Members** panel, select **Delete**.
4. When prompted, click **Yes** to confirm.

Copying Contacts

Copying contacts is a useful and quick way of adding contacts with a similar set of information, such as Company details, to the Address Book without having to create a new entry each time. When a contact is copied, all of the information is also copied and a new entry created with the suffix 'Copy' to identify it as a copied entry. Fields can then be updated with unique information for the copied contact. Once updated, the contact can be renamed to the actual contact name.

To copy an existing contact:

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** for which a copy will be created.
3. From the **Home** | **Clipboard** panel, select **Copy**.
4. From the **Home** | **Clipboard** panel, select **Paste**.

The copied contact is now displayed in the list as '**Contact Name - Copy**'. Use the Edit Contact functionality to amend the required details. Use the Rename functionality to give the copied contact a unique identity.

TIP: To copy all of the contact details in one action, use **Select All** from the **Clipboard** panel.

Renaming Contacts

The primary use of renaming contacts is to give a unique identity to contacts which have previously been copied. However, there may be other instances, such as marriage for example, where a contact name has changed. The Edit functionality cannot be used to change the name of a contact.

To rename an existing contact:

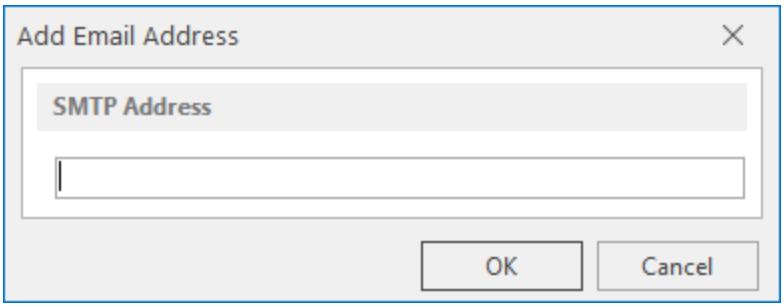
1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** that is to be renamed.
3. From the **Home** | **Members** panel, select **Rename**.
4. When prompted, enter the new name for the contact and click **OK**.

Adding an Email Address to a Contact

An email address may be added as part of the process when a new contact is created. If the contact will only be contacted via SMS then this step can be omitted.

WARNING: A contact must have either a default contact number or email address defined against it before it can be saved to the database.

1. From the **Address Book - Email Addresses** panel, click **Add** to open the **Add Email Address** dialog. This is used to enter the email details of the contact.



2. In the **SMTP Address** field, enter the email address for the contact.
3. Click **OK**.

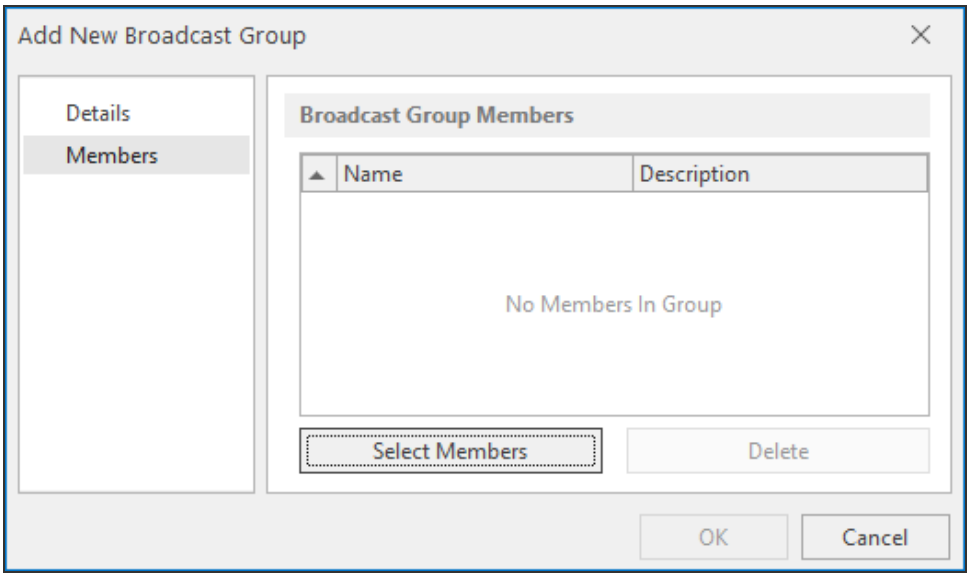
Working with Email Addresses

The following section describes the options for working with email addresses.

Setting an Email Address as a Default

The default email address is displayed in the **Email Addresses** panel as having a green tick mark in the bottom right corner of the **Email** icon.

From the **Add/Edit Contact** dialog, **Email Addresses** panel, highlight an entry and click **Set As Default** to use that email address as the main email address for the selected contact.



NOTE: The first email address defined for this contact is automatically set as the default. This option is only available if there is more than one email address specified for the contact.

Editing an email address

Should a contact update their email details, it is possible to edit an existing entry to the new address.

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** for which the email address has changed.
3. From the **Home** | **Members panel**, select **Edit**. The **Edit Contact** dialog is displayed.
4. From the left navigation panel select **Email Addresses**.
5. From the **Email Addresses** panel select the number to be edited and click **Edit**.
6. The address can now be edited using the same fields as when adding the email address.
7. Click **OK** to confirm the changes.

Deleting an email address

Should a contact no longer use this email address, it is possible to remove it.

1. Open the **Instant Alert Address Book**.
2. Find and select the **Contact** for which the email address is no longer required.
3. From the **Home** | **Members panel**, select **Edit**. The **Edit Contact** dialog is displayed.
4. From the left navigation panel select **Email Addresses**.
5. From the **Email Addresses** panel select the address to be removed and click **Delete**.
6. When prompted, click **OK** to confirm the deletion.

Call Schedules

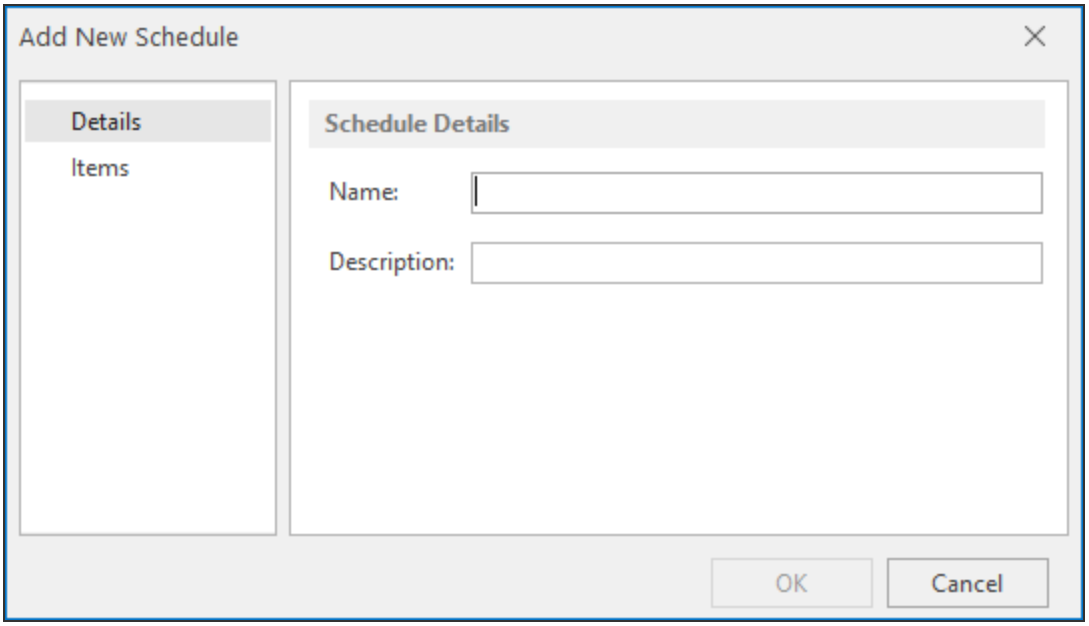
A call schedule is a method of ensuring that the correct person is contacted at the right time, in the event of an alert being raised.

> **NOTE:** An call schedule cannot be a member of another call schedule.

Adding a Call Schedule

1. Click **Add** from the **Members** panel of the **Home** menu ribbon.
2. From the drop-down choice menu, select **Schedule**.

The **Add New Schedule** dialog is displayed.



This dialog consists of two separate pages into which information can be entered.

Details page

This page is used to record the name and description of the call schedule.

Name

Enter the name by which the new schedule is identified throughout Instant Alert and Enterprise Console.

Description

Enter a meaningful textual description of the new schedule.

Items page

This page lists all of the items contained within this schedule. Upon first opening of this page, the panel is blank as no items have been added.

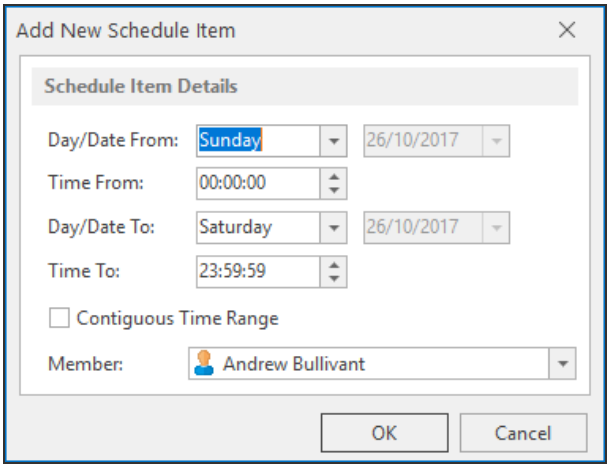
See Adding a Schedule Item for more information.

Adding a Schedule Item

A call schedule is comprised of at least one item that dictates when the schedule is active and dormant.

To add a schedule item:

1. From the **Add/Edit Schedule - Schedule Items** panel, click **Add** to open the **Add New Schedule Item** dialog.



The fields on this dialog are used add the details of the new schedule item.

Day/Date From

From the drop-down list, select a day of the week on which this schedule item is active. To specify an actual date, select (Date) from the list and then use the calendar to choose the required date.

Time From

Specify the time on the selected day/date at which this schedule item becomes active.

Day/Date To

From the drop-down list, select a day of the week up to which this schedule item is active. To specify an actual date, select (Date) from the list and then use the calendar to choose the exact date.

Time To

Specify the time on the selected day/date that this schedule item ceases to be active.

Contiguous Time Range

Click **Contiguous Time Range** to specify that this schedule item runs continuously between the dates and times specified.

> EXAMPLE: Entering Monday 09:00:00 and Friday 16:59:59 would mean that this schedule item would be available CONTINUOUSLY between those times. Leaving this option unchecked means that this schedule item would be available Monday between 09:00:00 and 16:59:59, Tuesday between the same times and so on. (Saturday and Sunday would be excluded using this example).

Member

From the drop-down list, select the Member to which this schedule item applies.

Click **OK** to add this schedule item to the current schedule.

Broadcast Groups

A broadcast group is a team of people who have an interest in a specific function or routine.

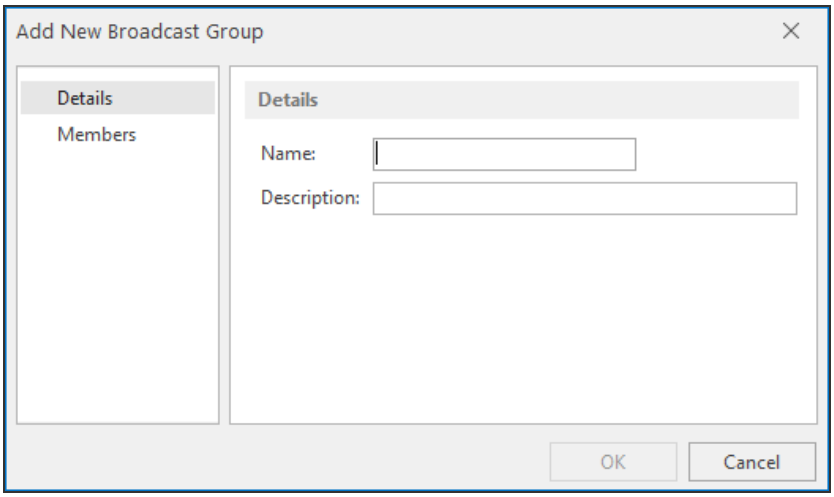
For large organizations it may be that many people are involved in very specific functions or routines across a department. For example, different support groups for different operating systems. In smaller organizations it is likely that one or two people have the responsibility of running all functions.

> **NOTE:** Call Schedules can be members of broadcast groups but broadcast groups cannot be members of other broadcast groups.

Adding a Broadcast Group

1. Click **Add** from the **Members** panel of the **Home** menu ribbon.
2. From the drop-down choice menu, select **Broadcast Group**.

The **Add New Broadcast Group** dialog is displayed.



The **Add New Broadcast Group** dialog consists of two separate pages into which contact information can be entered.

Details page

This page specifies the name and description of the broadcast group.

Name

Enter the name by which the new broadcast group is identified throughout Instant Alert and Enterprise Console.

Description

Enter a meaningful textual description of the new broadcast group.

Members page

This page lists all of the contacts and call schedules contained within this broadcast group. Upon first opening of this page, the panel is blank as no items have been added.

See Working with Broadcast Group Members for more information on how to add and remove members from this broadcast group.

Finding Contacts, Call Schedules and Broadcast Groups

If the database contains many contacts, call schedules and broadcast groups, the Find functionality can be used to search for entries with a unique or shared name.

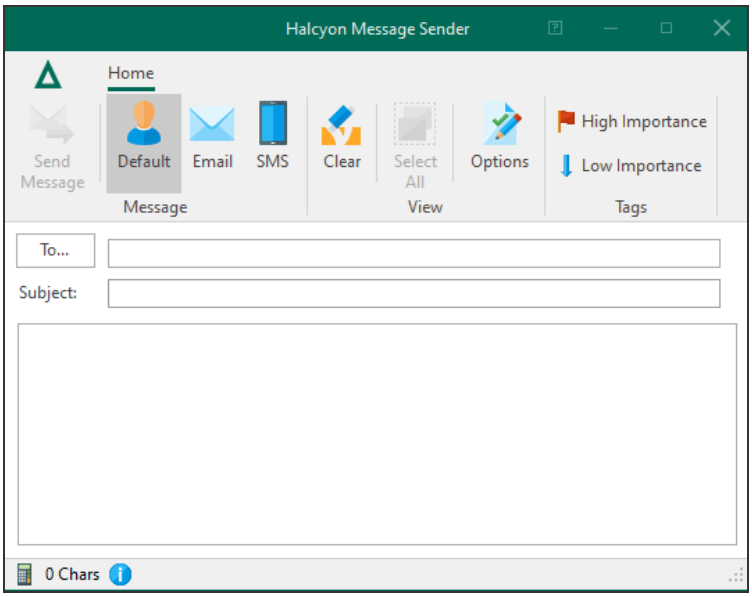
To find a contact, call schedule or broadcast group in the database

1. Open the **Instant Alert Address Book**.
2. From the **Home** | **Discovery** panel, select **Find**.
3. When prompted, enter the **Name** of the contact, call schedule or broadcast group to find and click **OK**. This can be full or part name of the entry.
4. If the entry is found it is displayed. If it is not the required contact, call schedule or broadcast group, select **Find Next** to locate the next instance.
5. Continue until the **Cannot Find 'Entry'** dialog is displayed.

Message Sender

Message Sender is an Instant Alert utility that can be used to send messages by either email or SMS to contacts in the Address Book and is similar in looks and functionality to many third party email applications.

To open Message Sender, select Windows **Start** | **Programs** | **Halcyon** | **Message Sender**. The **Message Sender** dialog is displayed.



Sending a Message

Use Message Sender to send a basic message. Additional options can be used to add extra detail.

To send a basic message

1. Open Instant Alert **Message Sender**.
2. Enter the name of the contact as the recipient of the message or click **To...** to display a list of all the contacts, call schedules and broadcast groups in the Address Book.
3. Enter the title of the message in the **Subject** parameter.
4. Enter the body text of the message in the main panel of Message Sender.

To send the message via the default method for the contact:

1. From the **Message Sender | Message** panel, click **Default**.
2. Click **Send Message** to send the message by the default method defined for the selected contact.

To send the message via email

1. From the **Message Sender | Message** panel, click **Email**.
2. Click **Send Message** to send the message to the default email address defined for the selected contact.

> **NOTE:** A valid email address must have been defined for the contact in the Address Book.

To send the message via SMS

1. From the Message Sender | Message panel, click **SMS**.
2. Click **Send Message** to send the message to the default contact number defined for the selected contact.

> **NOTE:** A valid contact number must have been defined for the contact in the Address Book.

> **TIP:** Click both and to send the message via both email and SMS to the contact simultaneously.

Message Priority

The default value for the sending of messages is **Normal**. If required, from the **Tags** panel of **Message Sender** select the message priority of **Low**, or **High** depending on the importance of the message content.

To send a message with additional options

1. To display additional options that can be used to send the message click **Options** from the **Message Sender** | **View** panel.

The following options become available:

Date

The default is today's date. Enter the date or select the required date from the drop-down calendar. If the date is earlier than today, the message is sent as soon as you click **Send Message**. If a later date is selected, the message is held until the date and time are reached.

Time

The default is the time at which Message Sender was opened. Enter the time or use the up / down arrows to select a time. If the time entered is earlier than now and the date is today, the message is sent as soon as you click **Send Message**. If a later time is selected, the message is held until the date and time are reached.

Count

Enter or select the number of times that you want this message to be sent.

Interval

Select the interval, in minutes, between which messages are sent. This setting is only used if the Count parameter is increased from 1.

TIP: If you make a mistake while typing the email or selecting options, use **Clear** to remove all of the entries and start again.