FORTRA

Network Server Suite 11.6

User Guide

Copyright Terms and Conditions

202412100131

Table of Contents

Table of Contents

Network Server Suite

Overview

This guide covers the configuration of Network Server Suite and component use. For installation guidance, please refer to the Installation Guide. For further queries and assistance, please refer to the support section at https://support.fortra.com/.

As there are a variety of installation options according to what you want to monitor, your network size, configuration and physical location, we recommend you review the function of each of the products and plan on which of your networked machines you wish to install specific products to meet your particular monitoring requirements.

At the simplest level, all Network Server Suite products can be installed onto one machine as detailed in the Installation Guide.

However, this assumes that the machine onto which the products are installed is the only machine to be monitored. In practice, multiple machines, possibly sited in different geographical locations, will require monitoring.

Network Server Suite products have been designed to simplify the task of dealing with a large number of error messages, and alerts and enable you to identify and handle critical problems easily. Multiple systems can be graphically displayed on a single screen, in an easy-to-read format. Administrators and operators can view and respond to events directly from any machine the on which the Enterprise Console is installed.

The suite also contains additional tools to help ensure that all systems are working correctly. For instance, a series of monitors, including the Ping Monitor, can periodically verify that a particular system is available, raising an alert if not.

Inquiry and informational messages are viewed and responded to directly from the Enterprise Console and other types of messages can be acknowledged.

Other alerts, displayed automatically, include TCP/IP connectivity problems, performance problems (resource hungry jobs or capacity thresholds exceeded).

> **NOTE:** Network Server Suite requires Windows scaling to be set to 100%. Check the **Scale and layout** properties in the **Display** settings of the server on which Network Server Suite is installed and adjust if necessary.

Component Overview

Network Server Suite products can be installed in a variety of ways to suit customized networking and monitoring requirements and also the physical location of devices.

Default installation options within the InstallShield package comprise:

Typical, Custom and Enterprise Console Client options:

- The Typical installation option installs all products including the Server Manager onto one machine (all visual monitoring and configuration would then have to be performed at this machine).
- The Custom installation option installs whichever products you select from a given list onto one machine.
- The Enterprise Console Client installation option installs just the Enterprise Console client component onto a single machine.

However, where these components are installed is dependent on the network location, configuration and accessibility to machines for monitoring and configuration.

Please refer to the following table for an overview of possible installation options:

Icon	Product	Function	Typically Installed On
	**Enterprise Console**	Displays alerts, messages and other system details. Works via a connection to Enterprise Server.	One or more server or client machines according to who needs access to view alerts and other network information.
	Enterprise Server	A configurable service (via Enterprise Server Options. Receives alerts from a variety of sources and allows users to manage them centrally through the Enterprise Console.	One (server or client) machine - multiple copies of the Enterprise Console on different machines allow users to view the same alerts processed by one Enterprise Server installation. **License**: Requires a separate license for each server where Enterprise Console is installed with its own database.

Icon	Product	Function	Typically Installed On
	**Enterprise Server Options**	Configures Enterprise Server settings.	The same machines as Enterprise Server.
	CCM Server	A background service associated with the Central Configuration Manager.	Automatically installed with the Central Configuration Manager.
	**Central Configuration Manager (CCM)**	A host or framework in which system monitors, templates and reporting is configured and controlled.	On machine. This can be any network server or client machine with remote access to the Server Managers and other hosted products. **License**: The CCM must have an authorization code applied but the actual machine on which CCM runs does not need to be assigned one of the resulting Windows licenses in order to operate, although it is recommended.
	Windows Server Manager	A configurable service hosted by the Central Configuration Manager. Used to setup and monitor the server environment.	The machine on the network to be monitored (these could be servers and/or client machines). **License**: An individual license is required for each installation of server manager of a Windows device.
	**Device Manager**	A configurable stand-alone product that defines devices for use throughout Network Server Suite and other Halcyon products. Allows the manual entry of network devices, device categorization and the launching of device associated applications.	Typically installed on the same machine as the Central Configuration Manager for convenience, however it could be installed on nay other networked server or client machine.

Icon	Product	Function	Typically Installed On
	**Instant Alert Server Options**	The configuration component of Instant Alert.	Usually installed on the same machine as the Central Configuration Manager. **License**: A separate license is required (for Instant Alert only) if this is installed an a separate machine.
	**Address Book**	The component of Instant Alert used to store cell phone numbers and email addresses of message recipients.	Usually installed on the same machine as the Central Configuration Manager.
	**Message Sender**	Used to send text messages to cell phones from the Enterprise Console or Server Manager. Email messages can also be sent.	Usually installed on the same machine as the Central Configuration Manager.
	Trap Receiver	Processes thresholds received from SNMP devices and passes the data to the Enterprise Server.	Usually installed on the same machine as the Server Manager.
	Network Manager	A background service that allows communication between all clients and server services and GUIs.	Automatically installed in conjunction with any other product.
	USM (AIX Agent)	Used to set-up and monitor the AIX server environment.	Must be installed on any monitored AIX machine. **License**: Each AIX machine to be monitored needs its own AIX license assigned.
	USM (Linux Agent)	Used to set-up and monitor the Linux server environment.	Must be installed on any monitored Linux machine. **License**: Each Linux machine to be monitored needs its own Linux license assigned.

Licensing

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

The initial licensing of Network Server Suite is undertaken as part of the installation.

> **NOTE:** Please refer to the Network Server Suite Installation Guide for more details on this procedure.

This version of Network Server Suite utilizes a licensing option that is more flexible and transparent to the user, allowing you to add, change, remove and re-assign licenses to servers across your network. It also includes Automatic License Assignment, whenever the Network Server Suite license is updated.

Network Server Suite system-wide licensing can be updated via Enterprise Server Options (as well as in Central Configuration Manager) but individual licensing of systems is solely maintained via the Central Configuration Manager.

Applying Individual Licenses to Systems

As systems are added to the Central Configuration Manager, they appear as unlicensed until a license has been assigned.

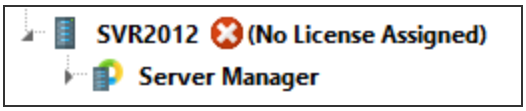
An unlicensed system is displayed as having **(No License Assigned**) and is identified by a  symbol next to the system name in the **Systems** tab of Central Configuration Manager.-

Systems must be defined within Device Manager before they can be added to Central Configuration Manager.

To apply a license:

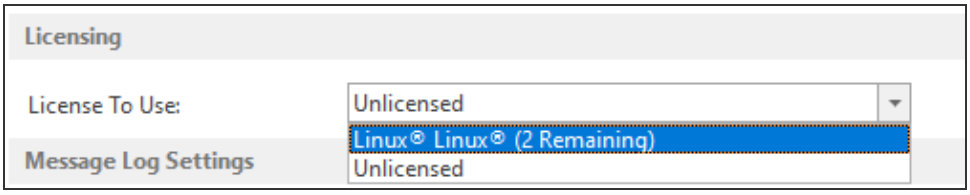
> **NOTE:** Spare licenses must be available for the Operating System to which the unlicensed system belongs to be able to assign a new license.

1. Select the **Systems** tab from the left-hand navigation panel of the Central Configuration Manager. Unlicensed systems are displayed with **No License Assigned**.



The **System Details** panel is displayed showing the current configuration, licensing, message log settings and connection check status for this system. In the **Licensing** section of this panel, the **License to Use** field currently displays **Unlicensed Systems**.

2. From the **License To Use** field, use the drop-down menu to select the Operating System license applicable to this system (only licenses that can be applied to this system are displayed in the drop-down). Once selected, the number of remaining licenses for the Operating System is reduced by one.



The **License To Use** field changes to reflect the assignation of the license, with the number of licenses available being reduced by one, and the monitors are enabled under the system ready for use.

3. From the **Central Configuration Manager** | **Home** menu ribbon select **Save** .

   The settings are saved and the system is now licensed for use within Network Server Suite.

Removing a License from a System

There may be occasions where you need to remove a license or re-assign a license from one system to another.

To remove a license from a system

1. From within the **Systems** tab of **Central Configuration Manager**, select the licensed system. The **License To Use** field within the **Systems** panel currently shows the Operating System license applicable to this system.
2. From the **License To Use** field, use the drop-down menu to select **Unlicensed Systems**. Once selected, the number of remaining licenses for the Operating System is increased by one. The system is now displayed as having **No license Assigned**.
3. From the **Central Configuration Manager** | Home menu ribbon select **Save**.

The settings are saved and the license is removed from the system so it can no longer be used within Network Server Suite. The license can now be re-assigned by applying an individual license.

> **NOTE:** The unlicensed system continues to be displayed within the **Systems** tab of the Central Configuration Manager until it is deleted using ✖ **Delete System**.

Automatic License Assignment

Network Server Suite has in-built automatic license allocation capability.

When you edit the Network Server Suite license you are prompted whether or not to auto-allocate licenses.

- If you select **No** then all licenses are removed from the Devices within the Central Configuration Manager and must be manually re-applied (see Applying Individual Licenses).
- If you select **Yes** then a relevant platform license is automatically assigned to each Device defined within the Central Configuration Manager. However, you should check this assignment is correct before proceeding.

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

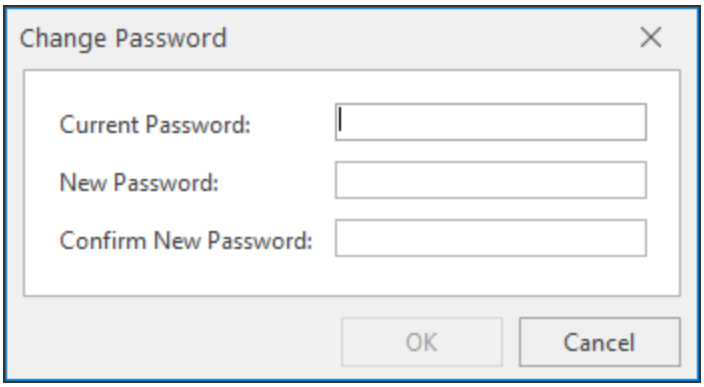
Passwords are changed from within the User Status option of Enterprise Console.

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.

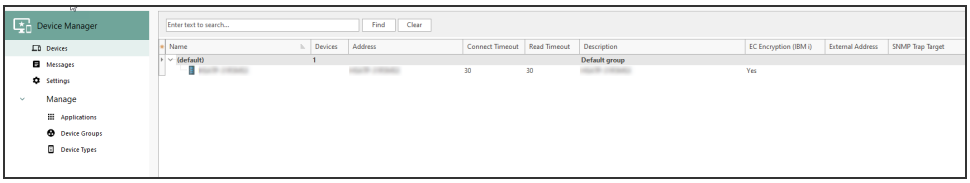
Recorded device information can be restricted to just **Name**, **Description** and **IP Address**, or can be fully comprehensive, incorporating time zones, support information and SNMP capability if available.

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.

Device Manager Appearance

Use the options in the Appearance tab to change the look of Device Manager.

From the Device Manager menu ribbon, click **Appearance**.

Display Vertical Grid Lines In Tree List Views

The default display within Device Manager shows information in a column by column view.

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

> TIP: This can make the viewing of information on the display easier to interpret when there is a large amount of data to view.

Dark Mode

Use the toggle switch to change the display mode from light (default setting) to dark.

> IMPORTANT: Dark Mode is saved per user and not by the application.
>
> Setting Dark Mode in any one of the UI ribbons applies it across all of the Network Server Suite applications, even those not currently loaded, which will then use the theme once opened.

Click the toggle switch again to return to the default light mode setting across all Network Server Suite applications.

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.

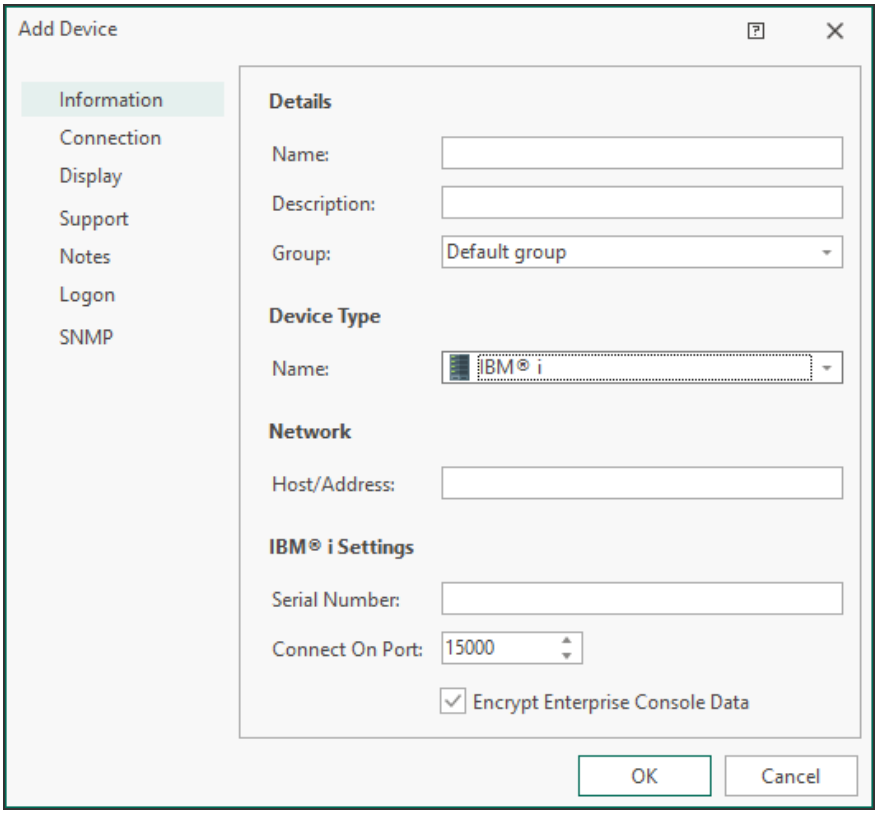
Adding a Device

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 Network 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

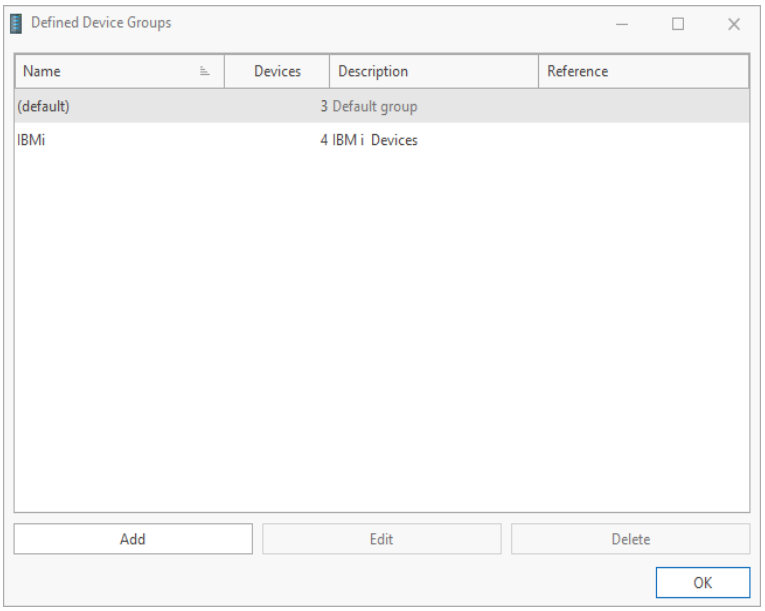
Once defined, devices can optionally be segregated into groups, for example, of similar devices, all devices belonging to a specific department, by location, or by whatever method required.

> **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.

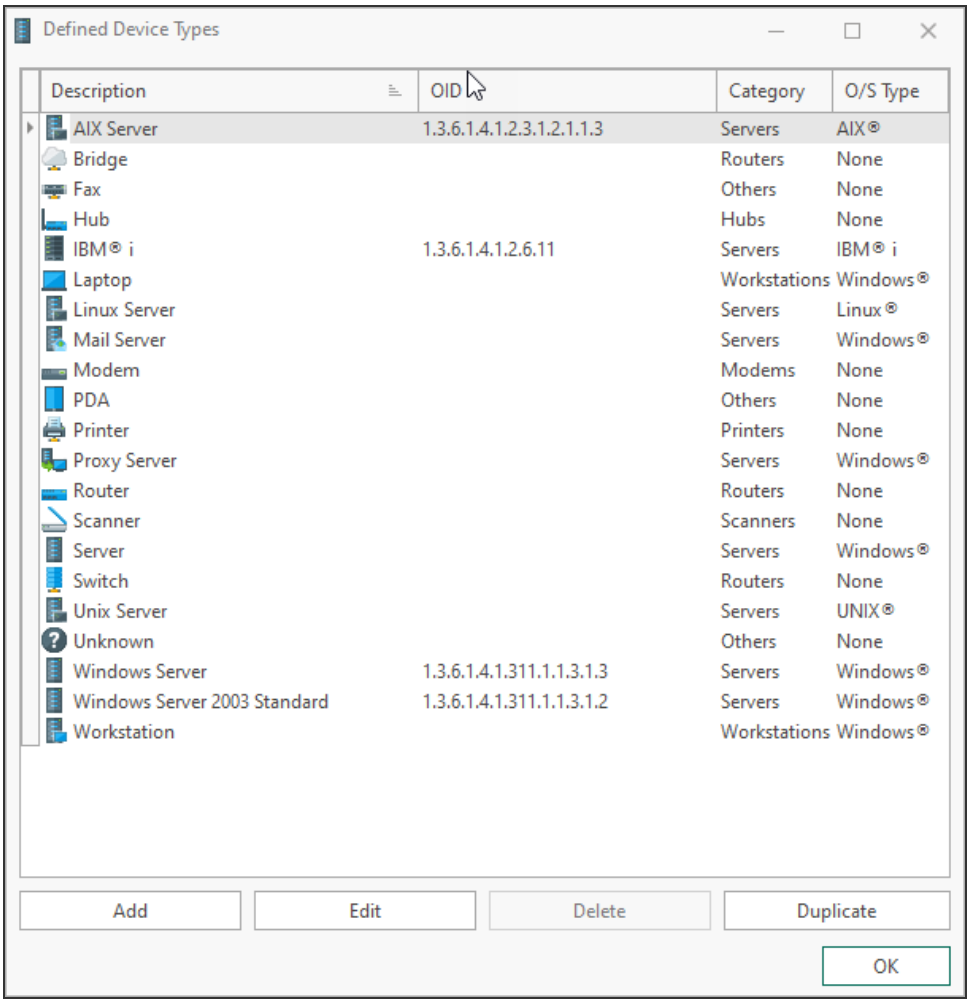
The full list of shipped device types is shown below:

- 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.

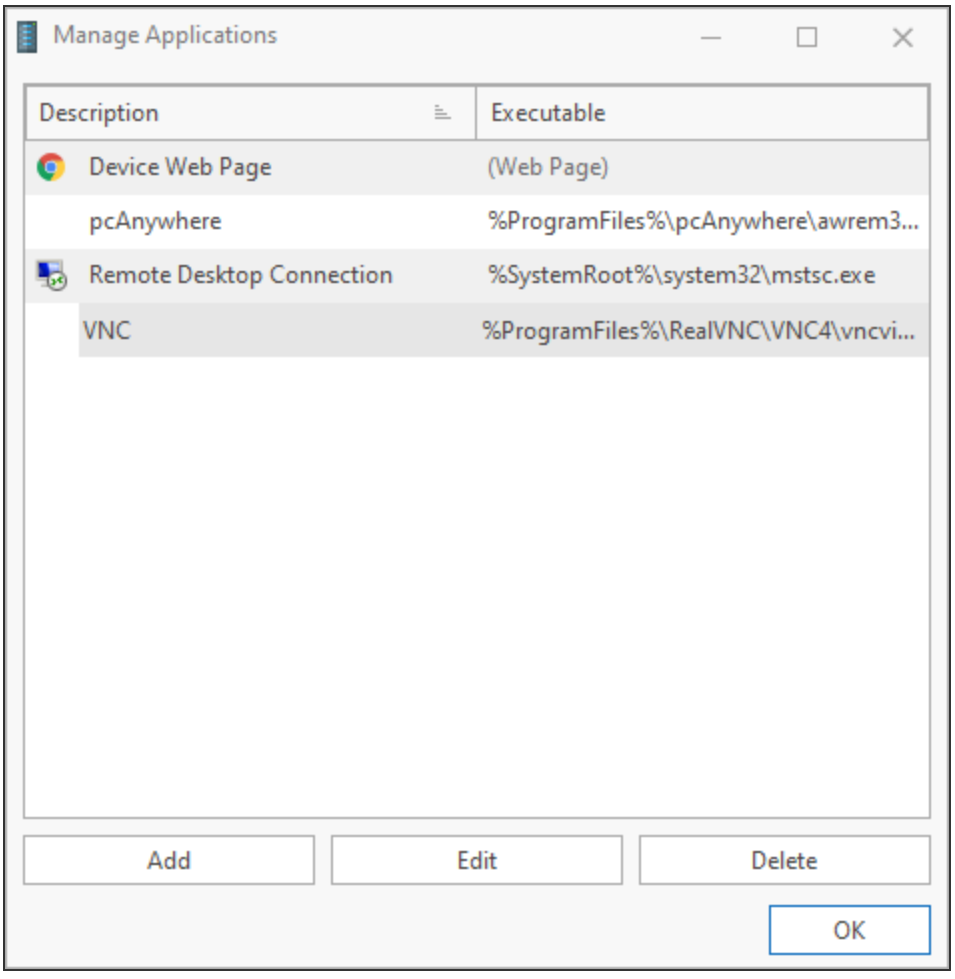
The device type can now be edited as required.

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.

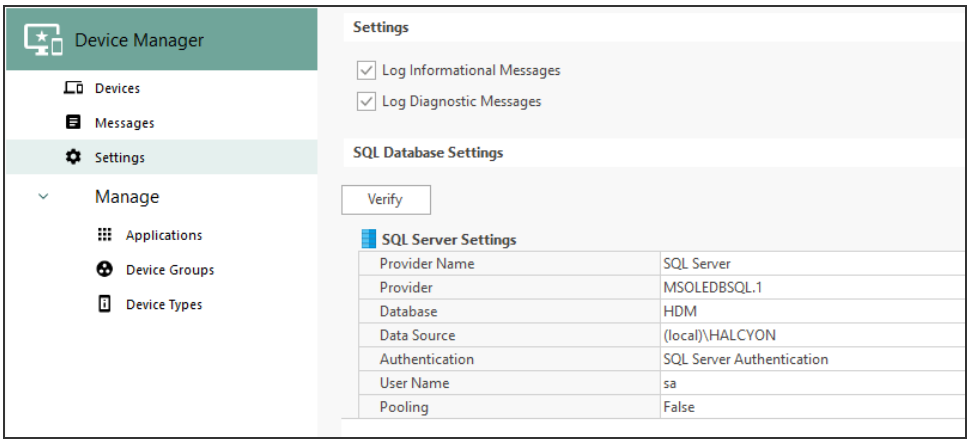
6. Click **OK** to confirm and add the client access application.

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.



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 Suite 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.

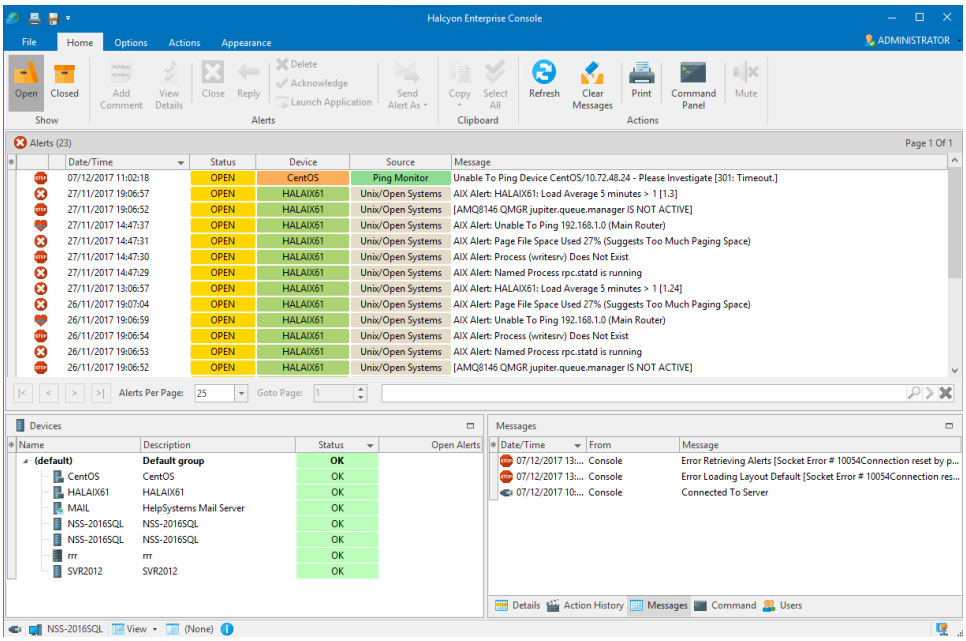
Enterprise Console is best used for monitoring and controlling multiple servers from a single location.

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.

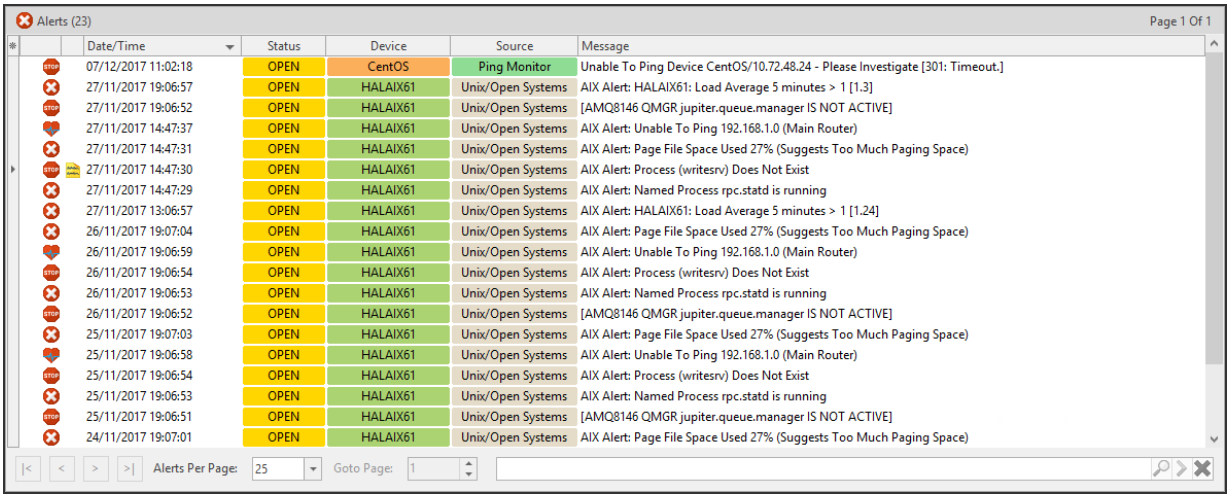
Alert panels

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.



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

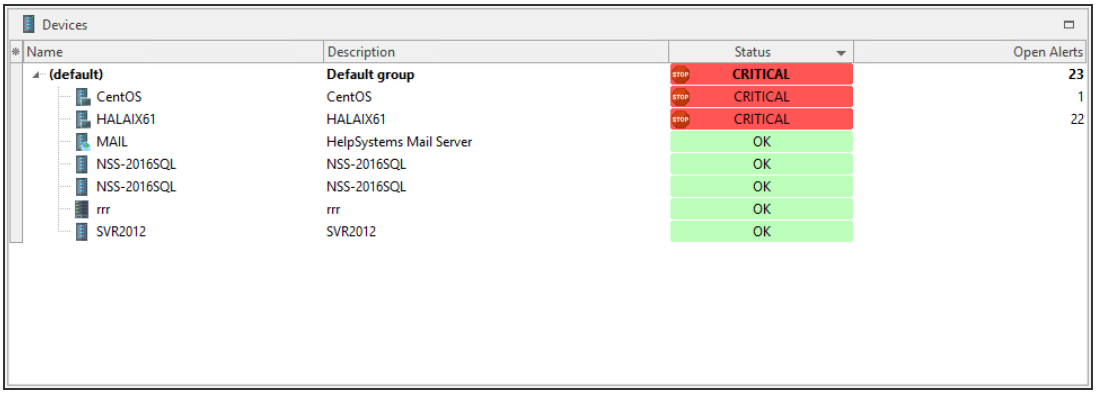
Displays the alert text as defined in the rule criteria that generated the alert. See Rule tab – Alert Message for more information.

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

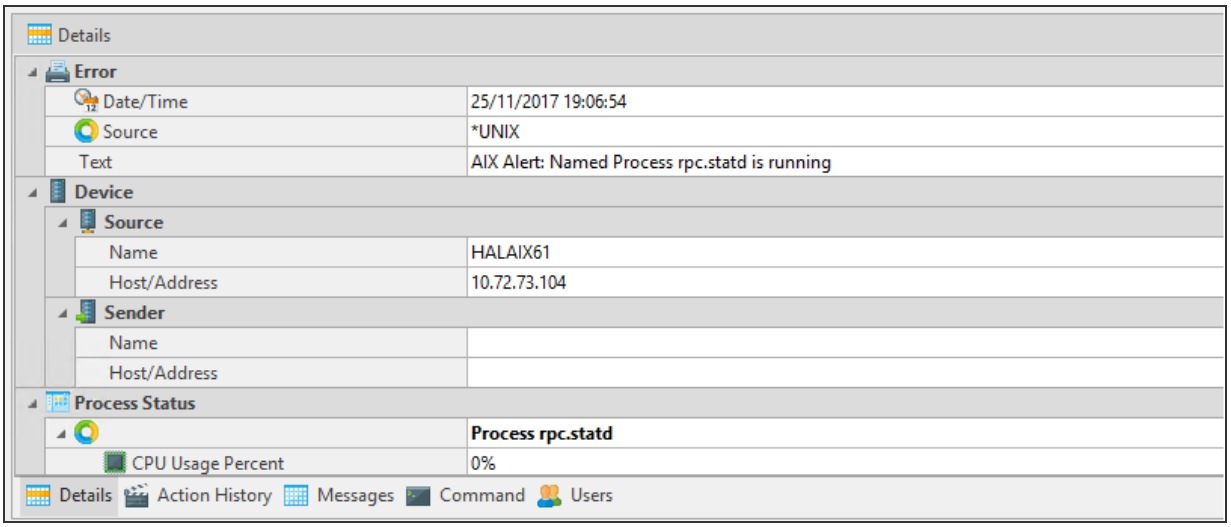
Displays the read timeout period for each device.

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.

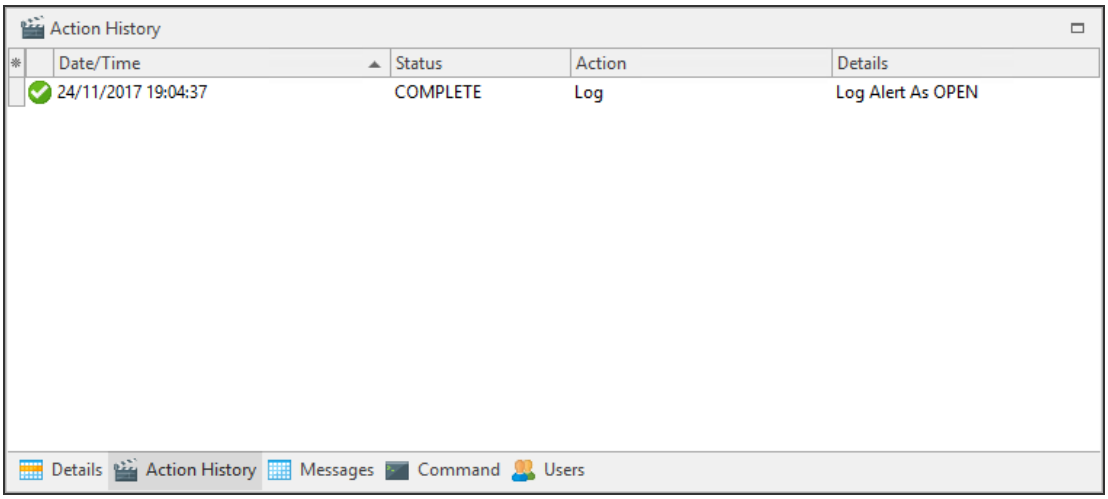
Console

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

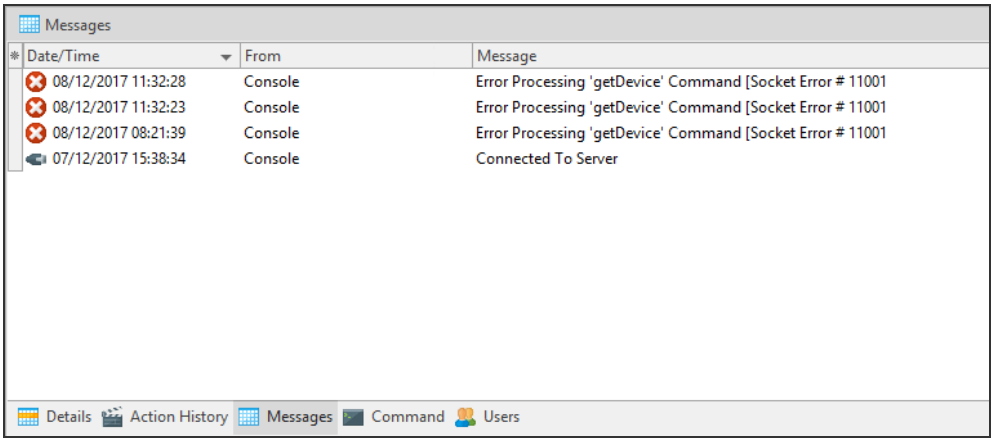
Displays the type of action that was performed.

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

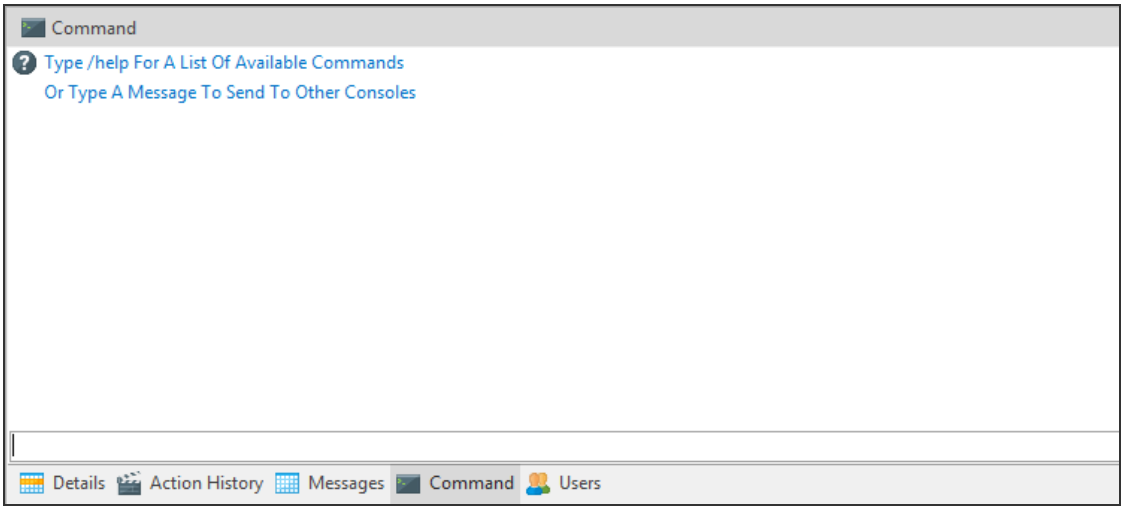
Displays full text of the message.

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):

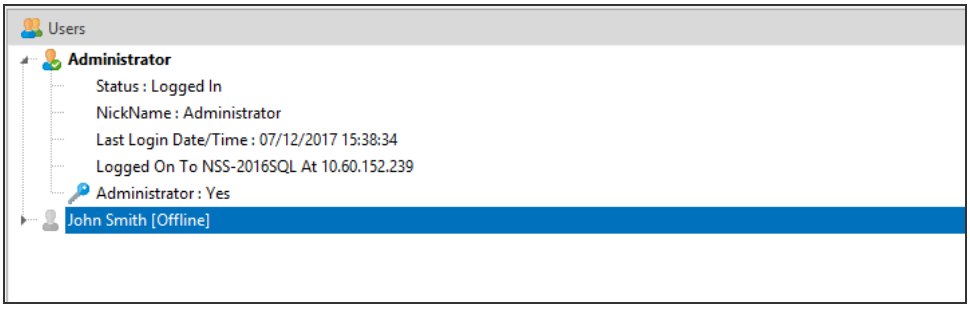
- **/AWAY**: without message
- **/AWAY AT LUNCH**: with a message, for example; 'At Lunch'
- **/CLS**: clears the command screen
- **/DATE**: returns the Enterprise Server date
- **/HELP**: displays a list of available commands
- **/LICENSE**: displays licensing information

- **/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

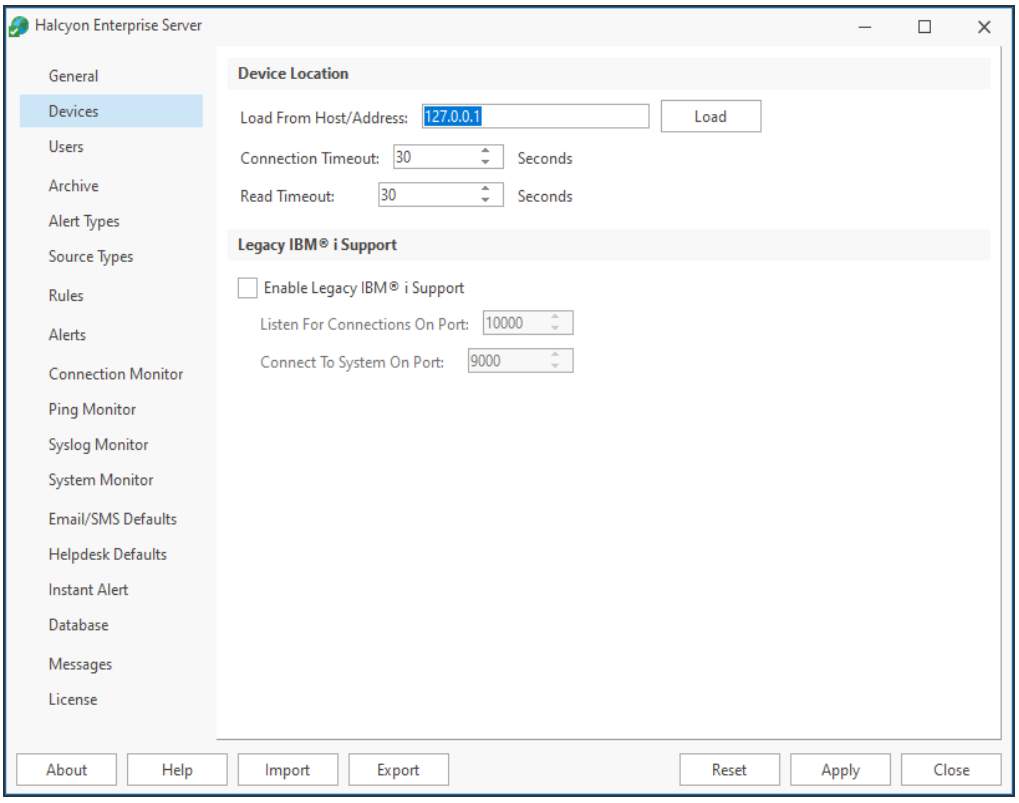
Enterprise Server Options

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

Alert Types

Source Types

Rules

Actions

Connection Monitor

Ping Monitor

Syslog Monitor

Email/SMS Defaults

Helpdesk Defaults

Instant Alert

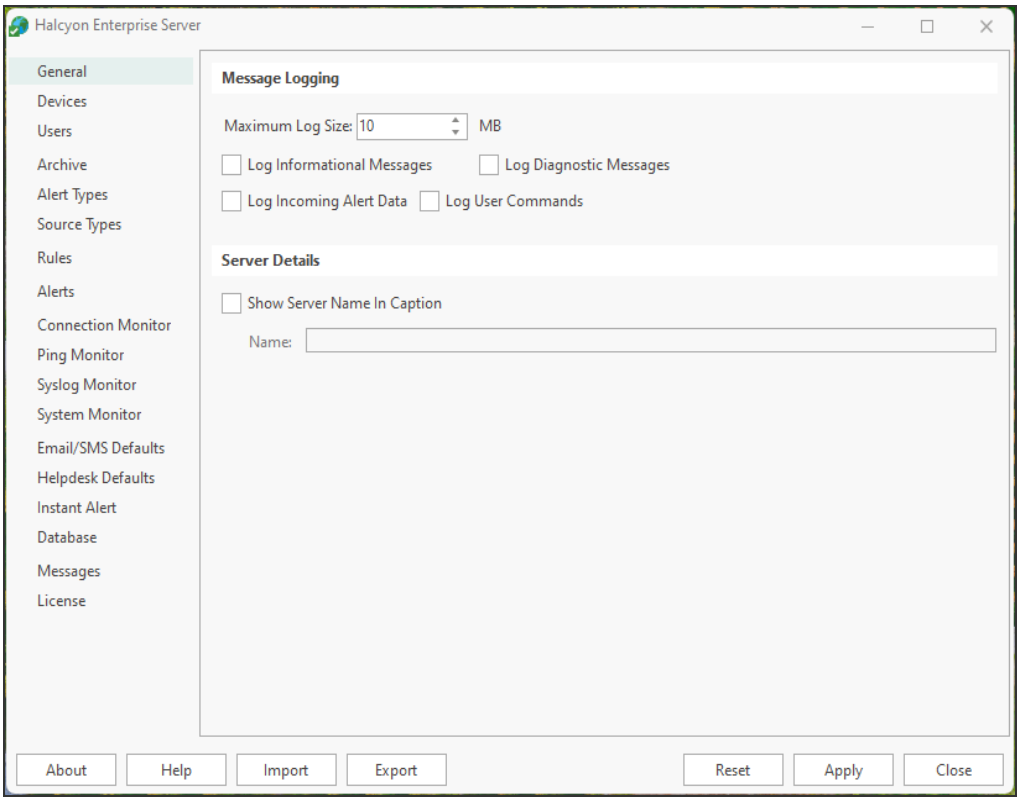
Database

Messages

License

> **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.

Maximum Log Size

Allows you to set the maximum size of any created log file from both the Enterprise Console Server and Client. The default setting is 100MB.

For Enterprise Console Server installations, the maximum permitted log size is 500MB.

For Enterprise Console Client installations the maximum setting is 100MB.

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.

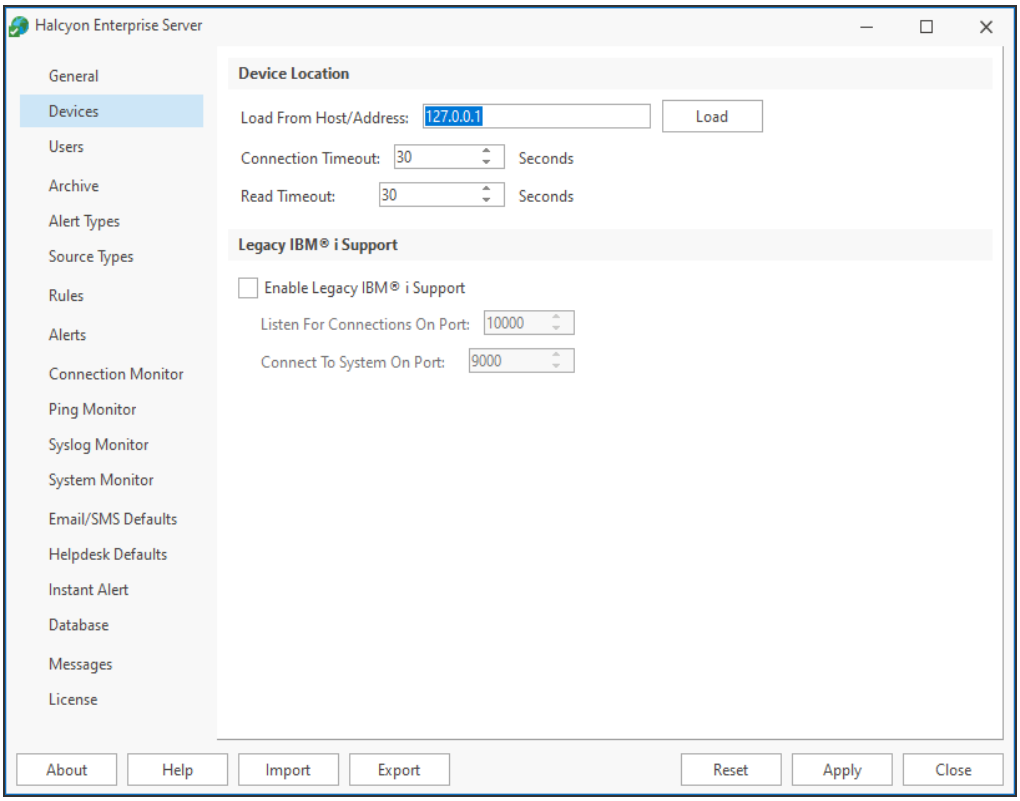
Show Server Name In Caption

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.

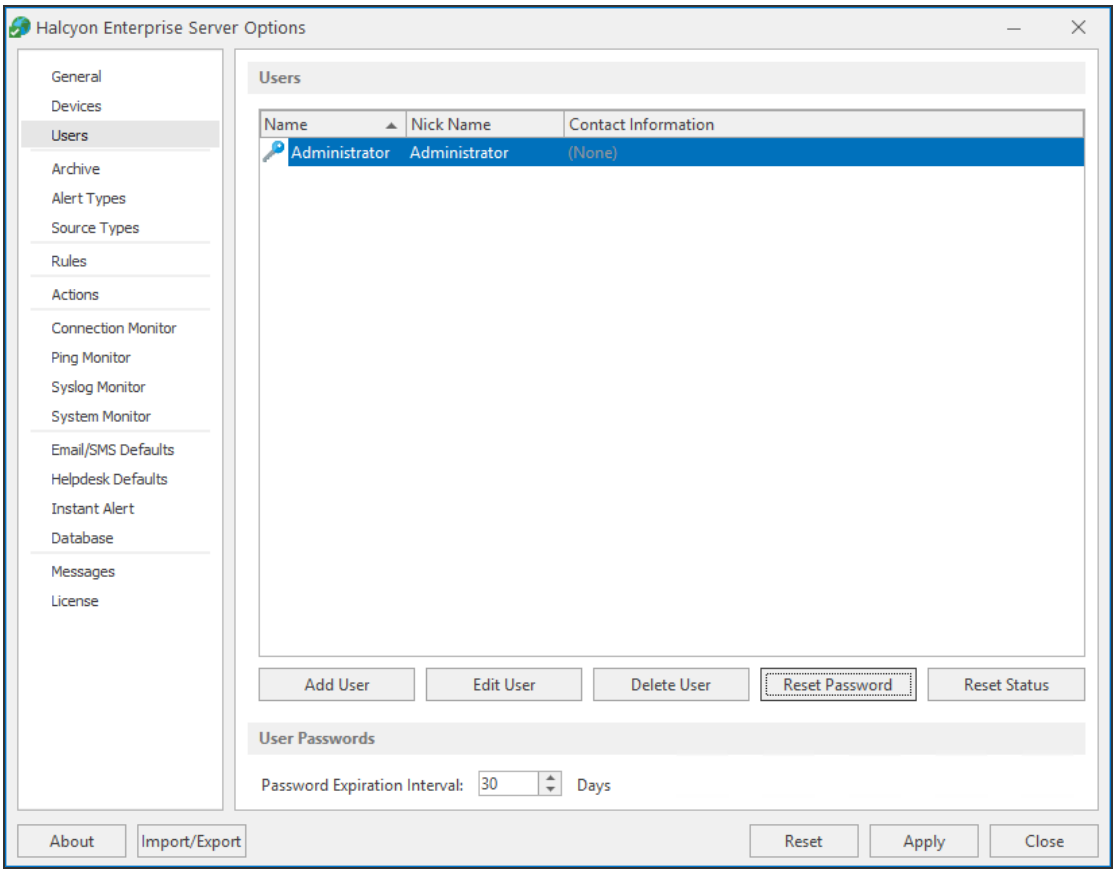
Listen for Connections on Port

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.

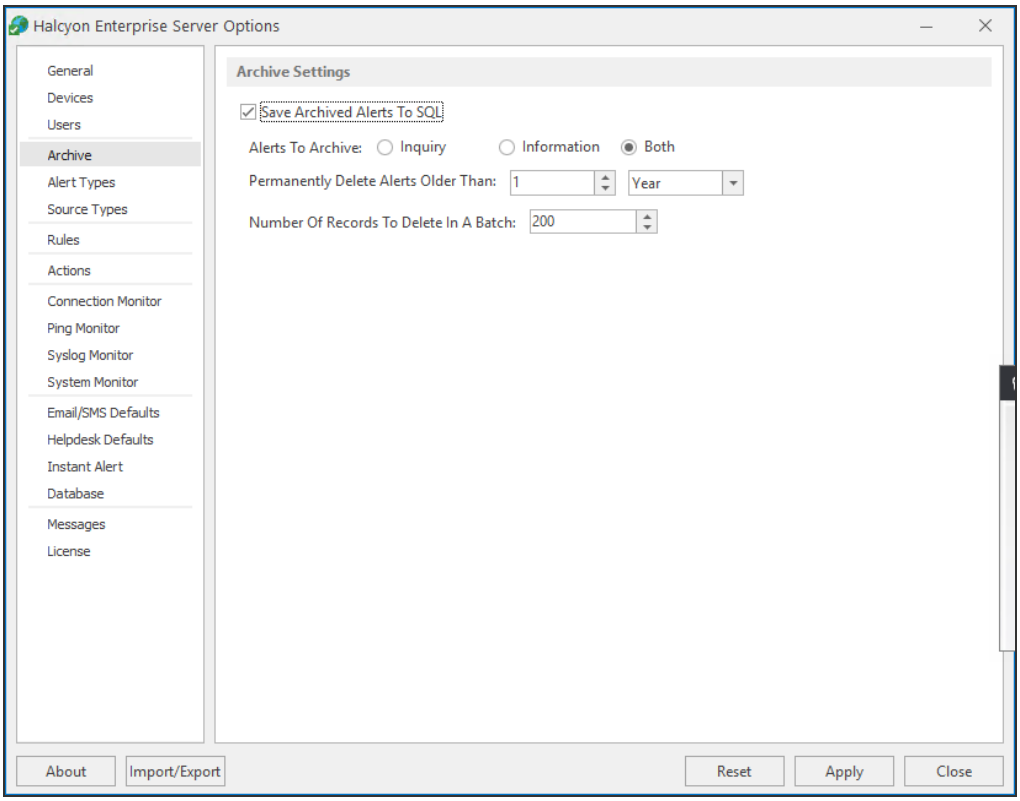
User Passwords section

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.

Enterprise Server Options- Archive settings



The options on this page are used to configure the archive and deletion settings for closed, replied to or purged alerts.

Archive Settings section

Save Archived Alerts To Database

Check this box to enable the saving of archived Enterprise Console alerts to the database. If this option is not checked, the closed alerts are automatically deleted after the period specified in the **Permanently Delete Alerts Older Than**... field and cannot be retrieved.

Alerts To Archive

This option defines the type of alerts that are archived. Select an option from:

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

Permanently Delete Alerts Older Than

Specify the time period after which any closed alerts are deleted from the system. Once deleted the alerts cannot be retrieved unless they have been archived.

Type the time period and use the drop-down menu to select whether the time is represented in Days, Months or Years.

Number of Alerts To Delete In A Batch

When deleting closed alerts, use this option to specify the number that should be deleted in a single action.

For example. if there are 600 alerts that are older than the specified time period to be deleted and this field is set to 200, the system will delete the alerts in 3 batches of 200. This is to prevent any performance issues arising between the database and the Enterprise Console, when large volumes of alerts are being deleted in a single process.

Reporting Archive Settings section

> **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.

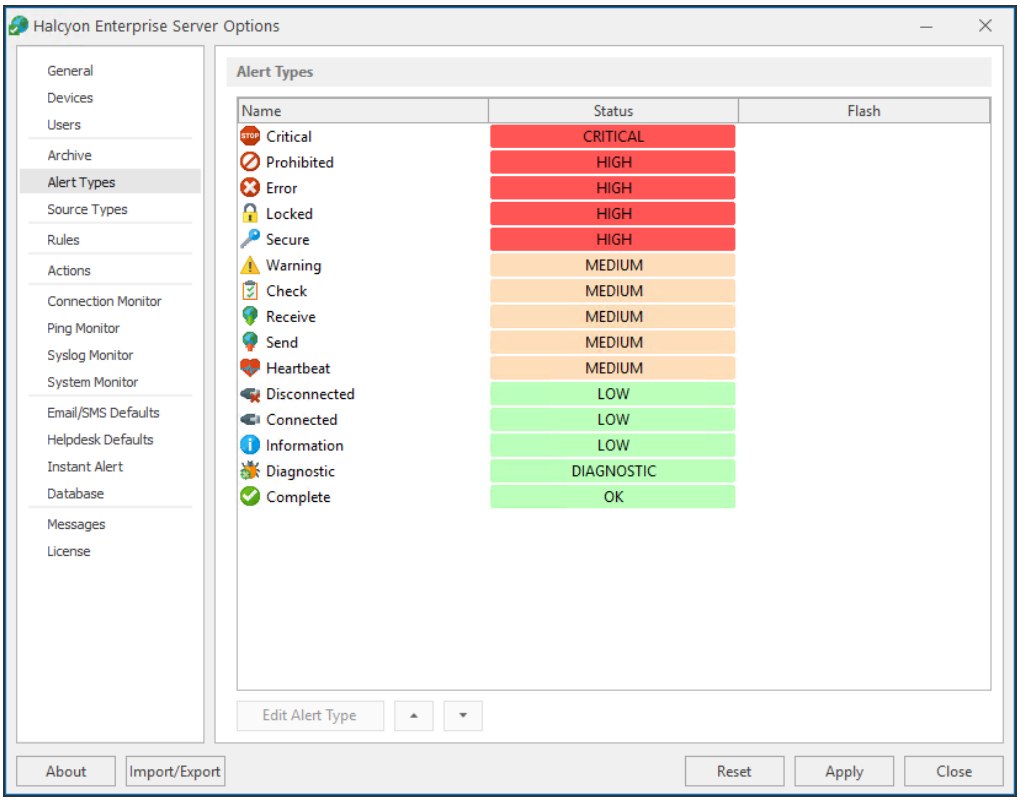
Amount Of Time To Keep Hourly Data Before Purging

Specify the amount of time, in Days, Months or Years to keep the collected hourly reporting data before purging. The default setting is 1 Day.

Number Of Records To Purge In A Batch

Specify the maximum number of records to purge in each batch when the purge period specified is reached. The default setting is 500.

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:

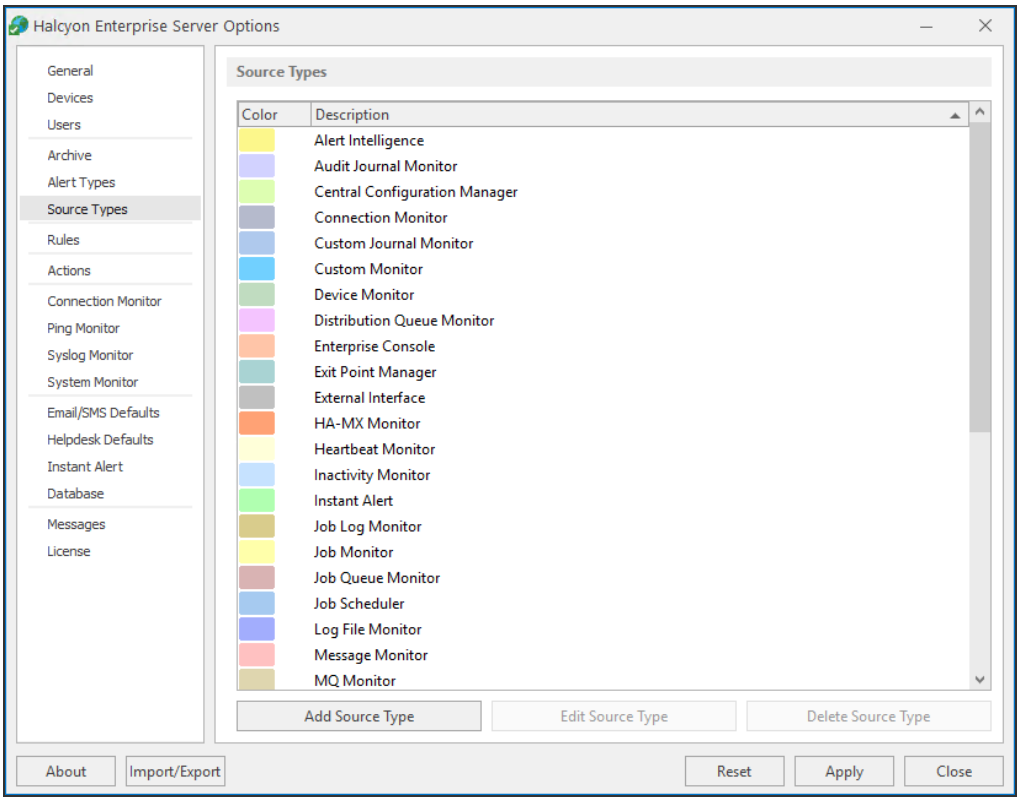
> **NOTE:** It is not possible to change either the Alert Type name or Alert Type icon.

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

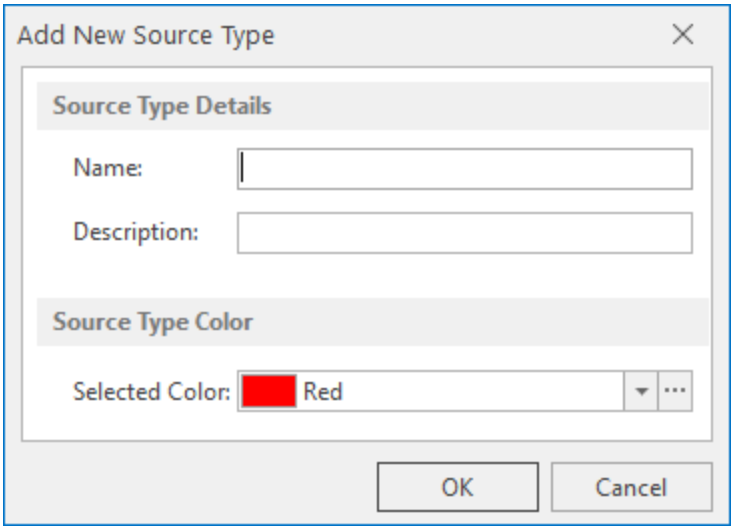
Working with Source Types

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.

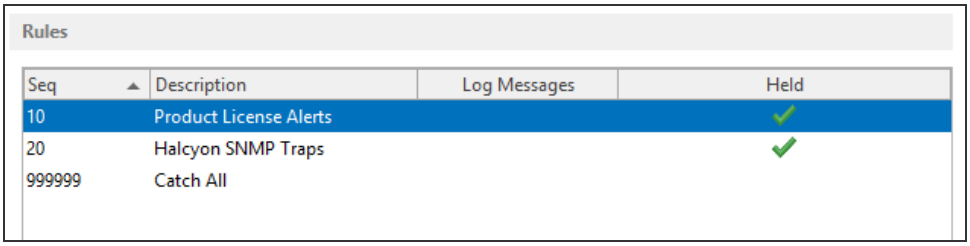
Rules monitor for messages or events across the network and specify what action to take should any specific message or event occur.

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

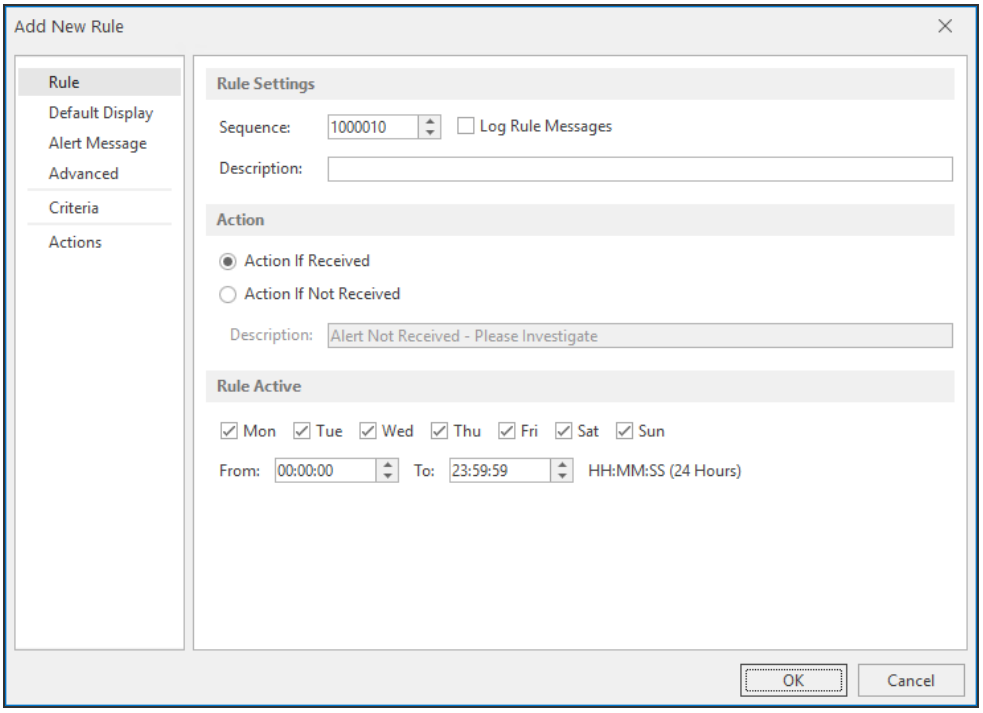
Adding or Editing Rules provides access to a series of dialogs and options used to capture any important events that do (or do not) occur. The dialogs are the same regardless of whether you are adding or editing a rule.

> **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.

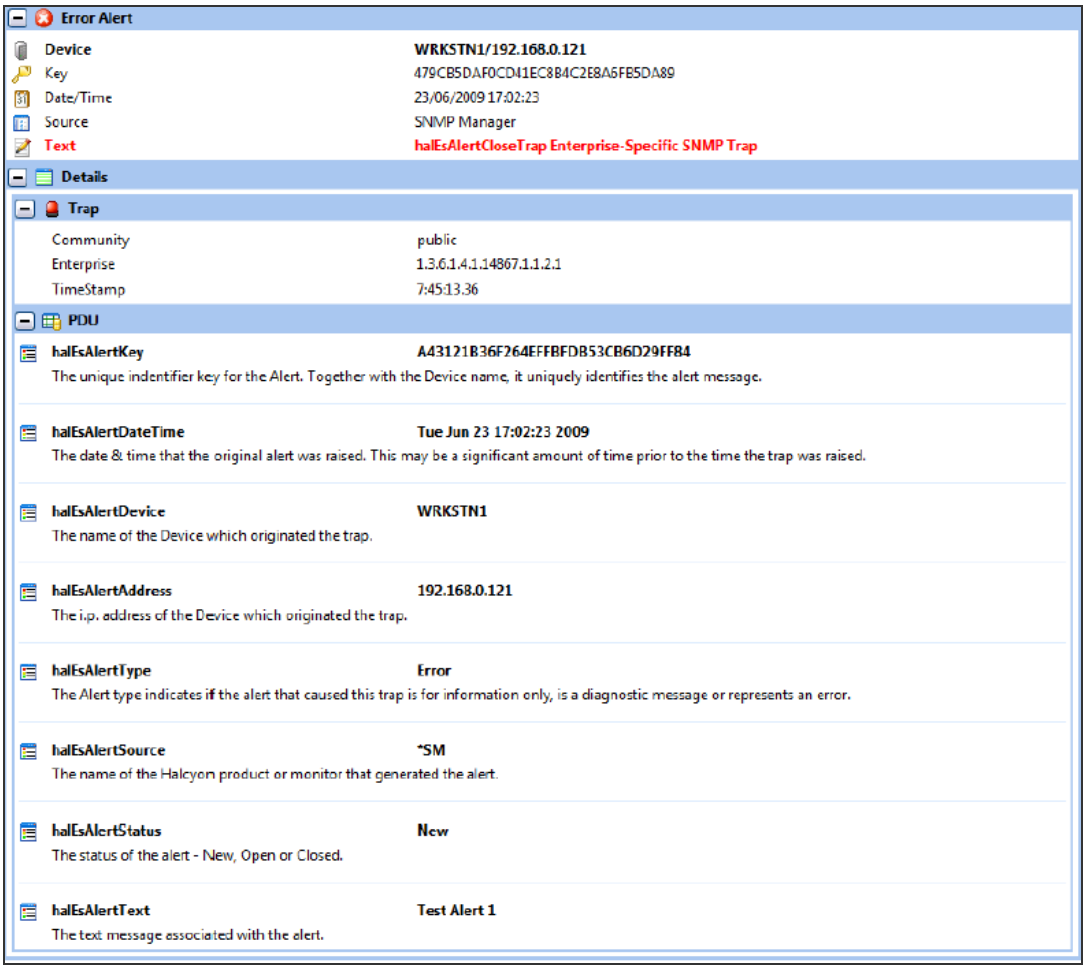
The Criteria and Actions pages are covered in their own sections.

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.

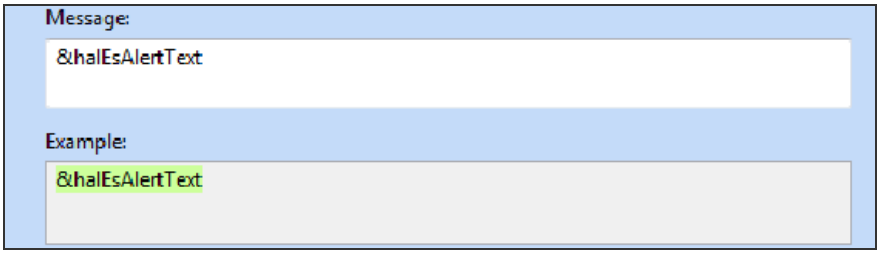
This feature is particularly useful when used for SNMP trap alerts as the Enterprise Console has no automatic way of recognizing which object in the trap payload actually represents the error message.

For example, in the SNMP Trap example below:

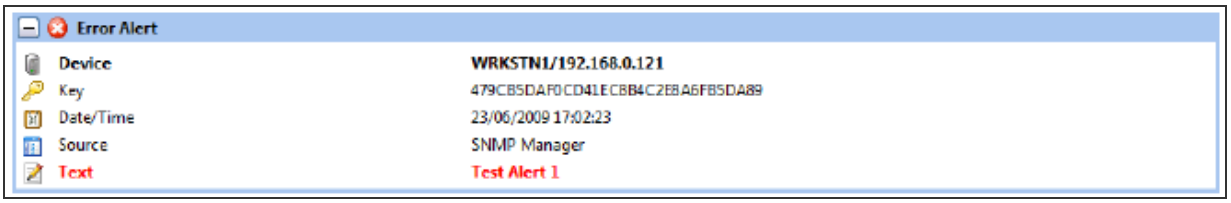


The trap payload is shown in the details section headed PDU. The payload contains a list of objects (left-hand side) and a corresponding value (right-hand side).

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’).

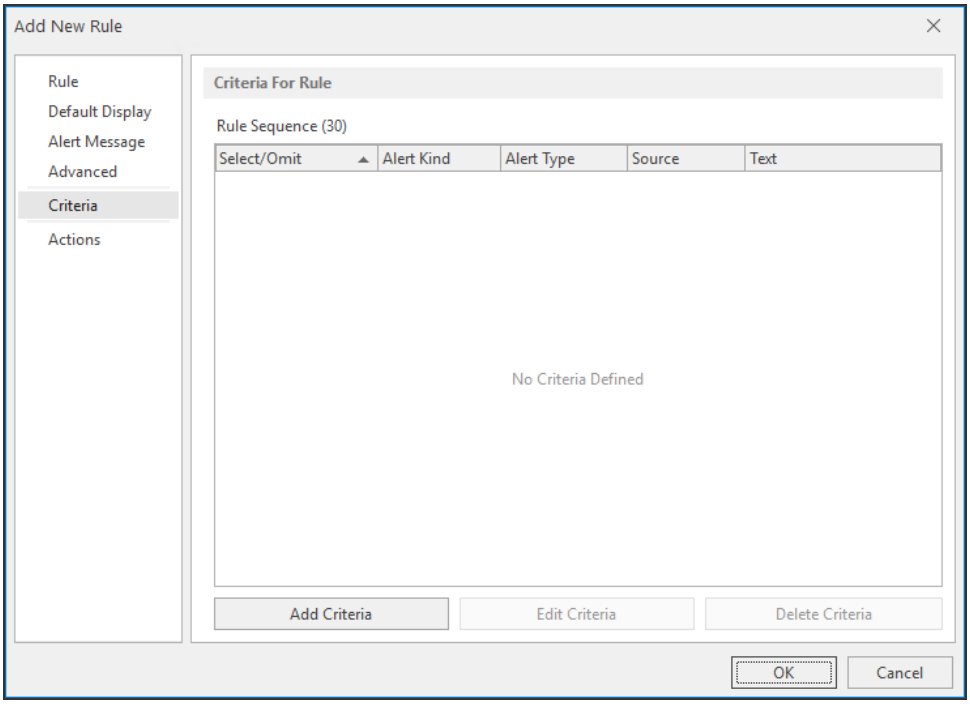


NOTE: If this option is used with common or frequently occurring message text, be sure to specify other criteria to ensure that the alert message generated is correct for the actual alert received.

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.

IMPORTANT: If you are using square brackets [ ] as part of a wildcard entry, they must be defined as a single character, so instead of using, for example, *[ABC]* as a wildcard entry the square brackets need to be separated so the entry would become *[[]ABC]*.

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

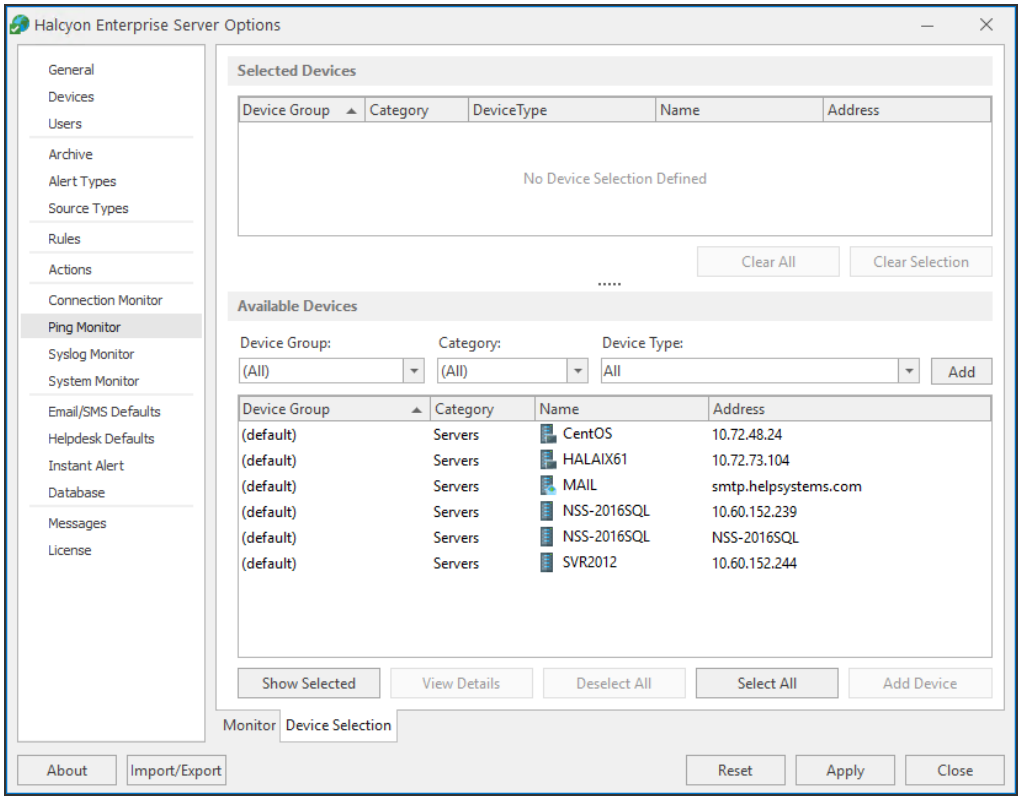
Enter the character to use as a substitute for this search span. '*' is defined as the default search span character.

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

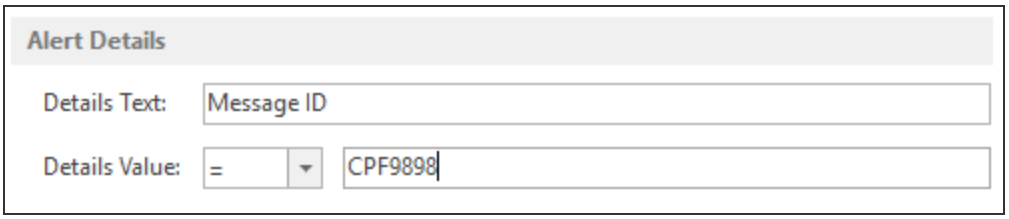
With string values, only operators '=' and '<>' are used. Other operators can be used, but note that unexpected results may be generated.

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

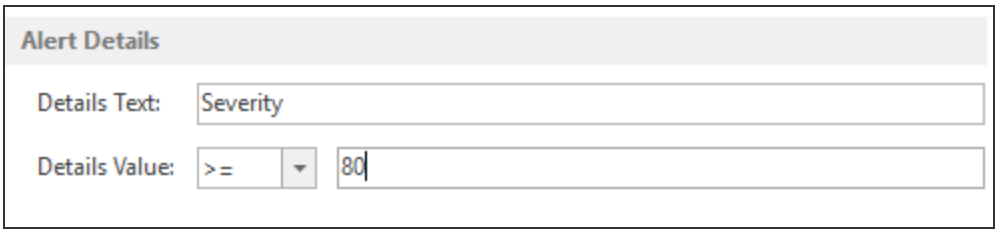
The following integer values are valid when entering Details Text for alerts originating from IBM i devices:

- 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.

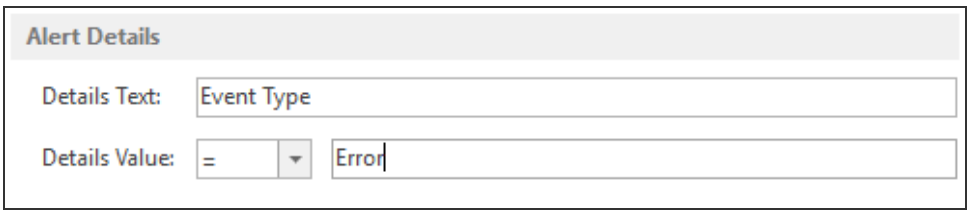
String Values

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 Syslog Messages

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

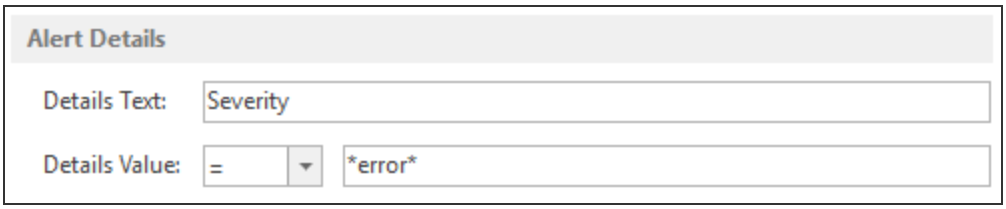
String Values

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*



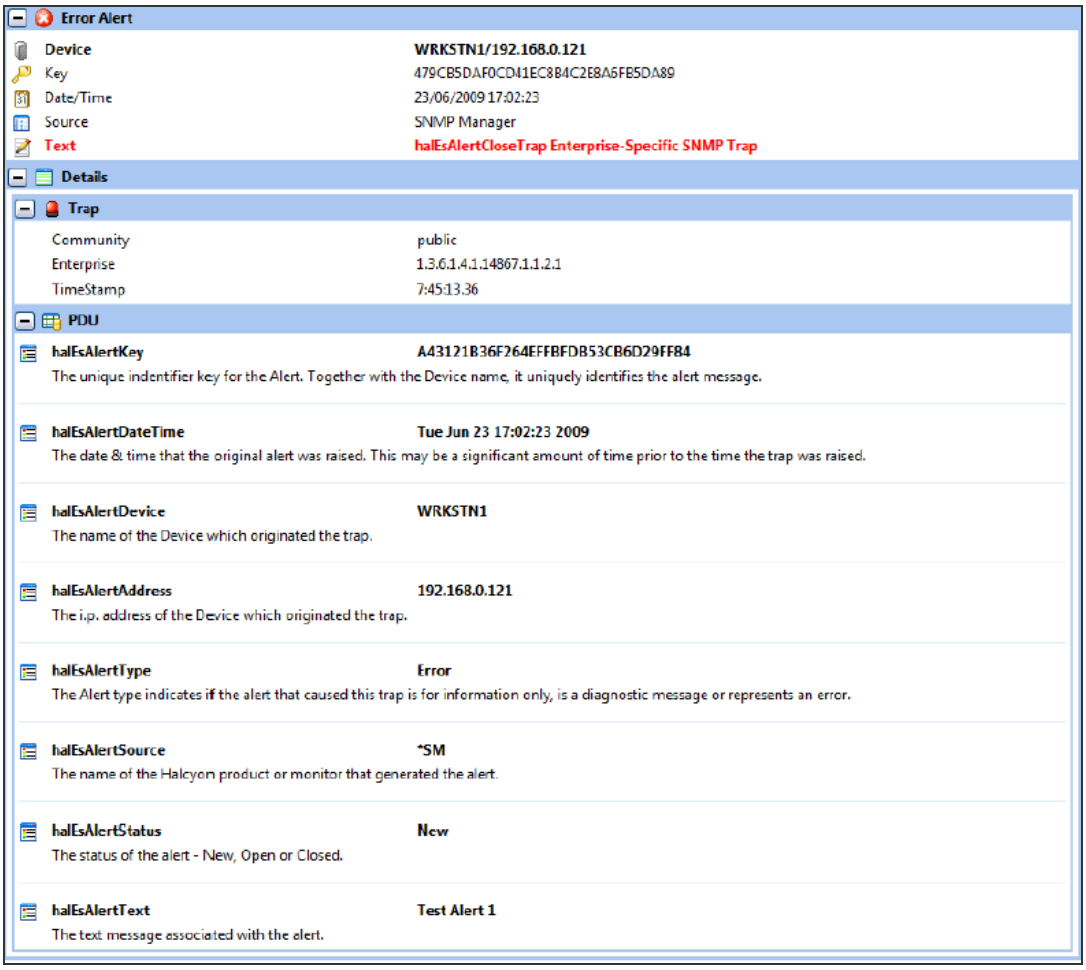
In the above example , an alert is generated for any Syslog Message Severity message with a value of *error*, that also meets other specified criteria.

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.

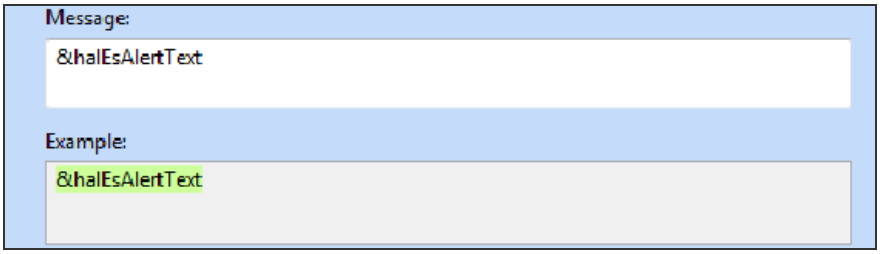
This feature is particularly useful when used for SNMP trap alerts as the Enterprise Console has no automatic way of recognizing which object in the trap payload actually represents the error message.

For example, in the SNMP Trap example below:

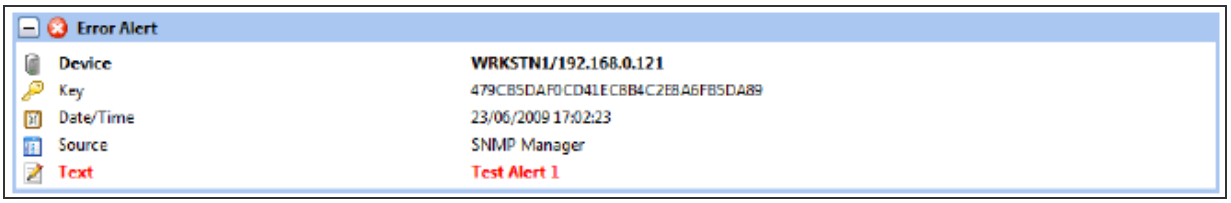


The trap payload is shown in the details section headed PDU. The payload contains a list of objects (left-hand side) and a corresponding value (right-hand side).

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 '='.

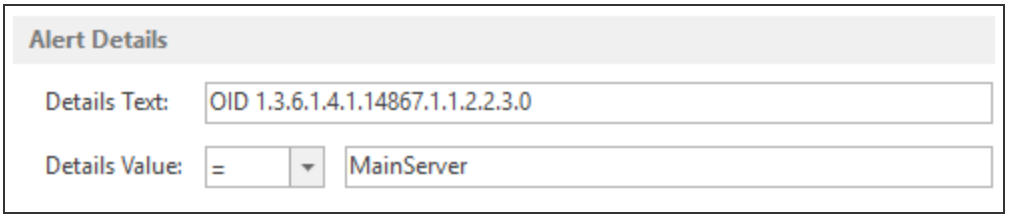
Therefore, the alert detail text for SNMP Trap alerts can be specified in a similar way as follows:

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



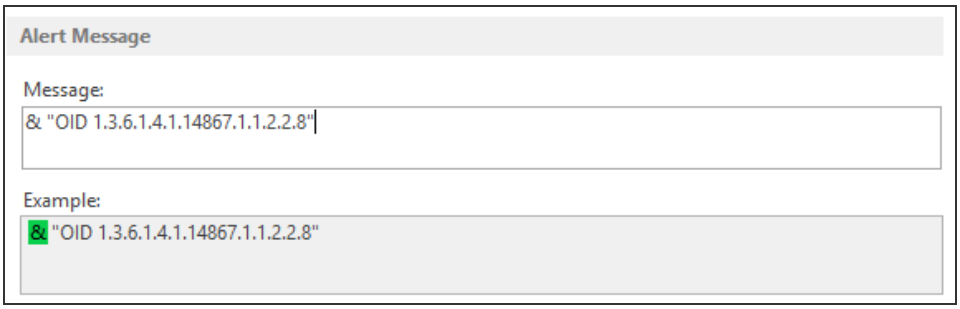
In the above example, an alert is generated for SNMP Trap OID 1.3.6.1.4.1.14867.1.1.2.2.3.0 with a value of MainServer, that also passes other specified criteria.

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:

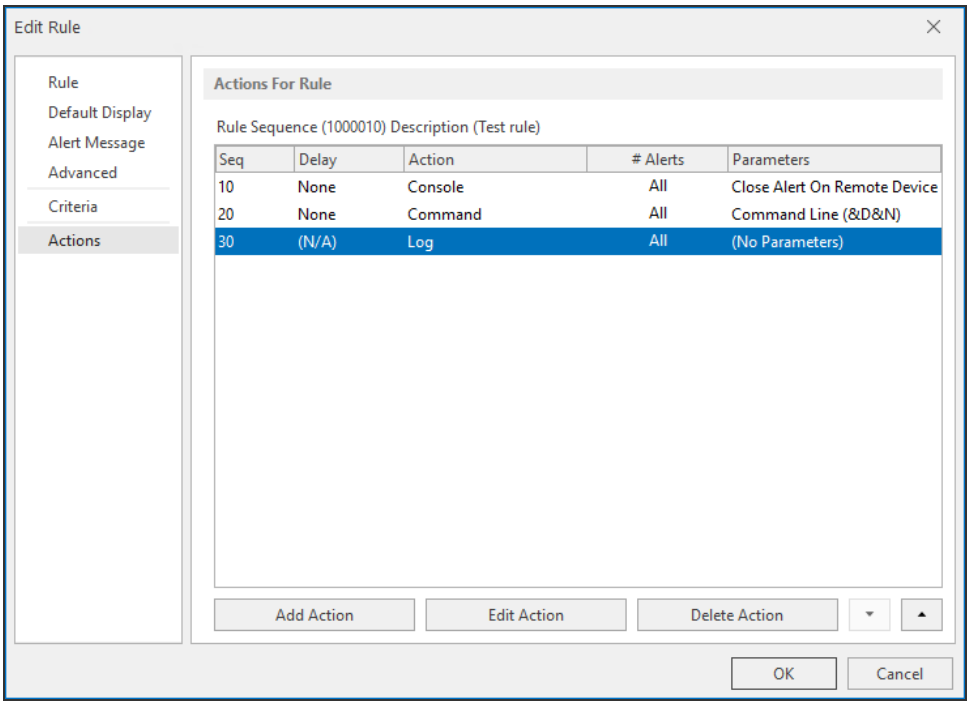
1. From Windows Start select **Programs** | **Halcyon** | Enterprise Server Options.
2. Select the **Rules** tab and click **Add Rule**.

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

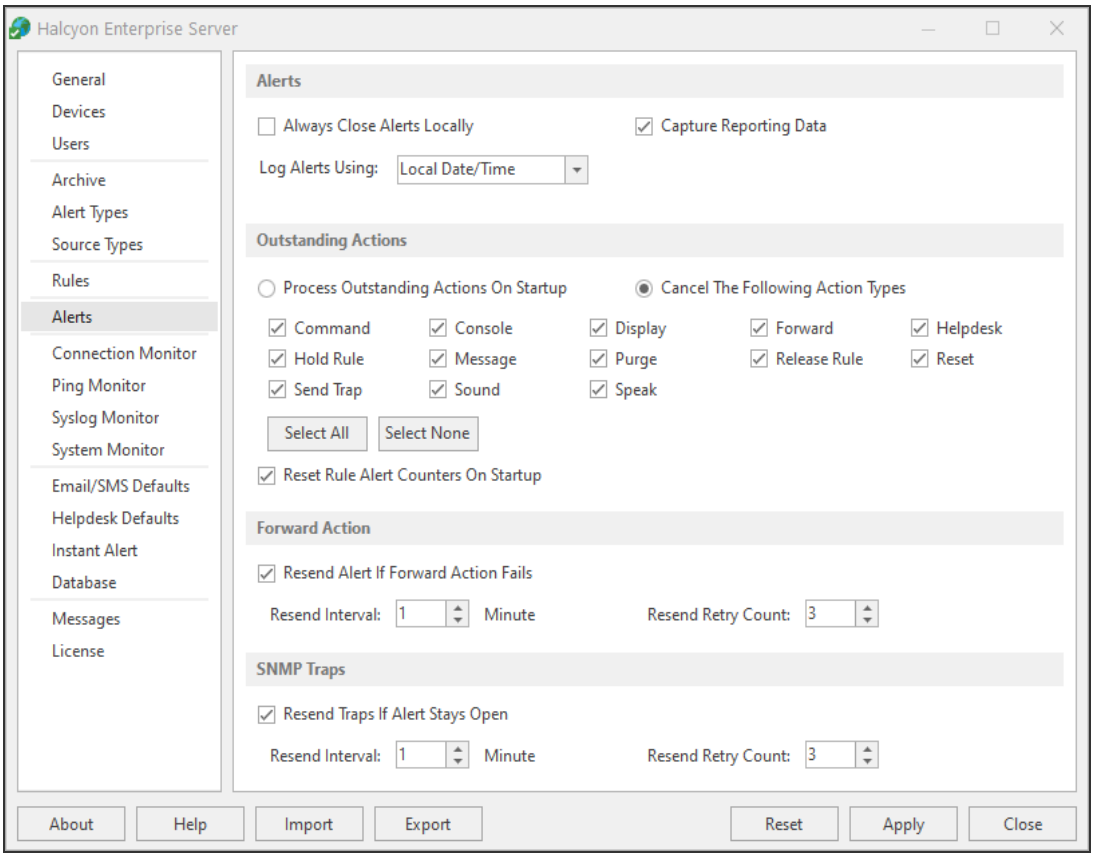
Add any comments you would like added to the status of this alert.

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.

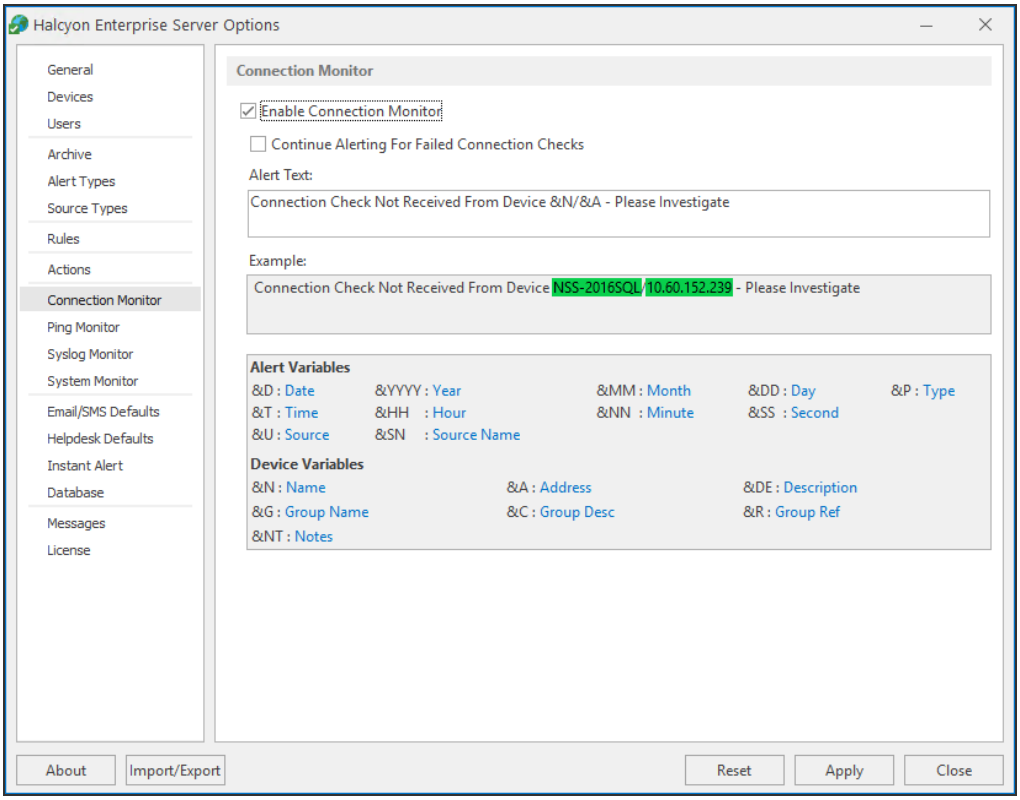
Enterprise Server Options - Connection Monitor

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

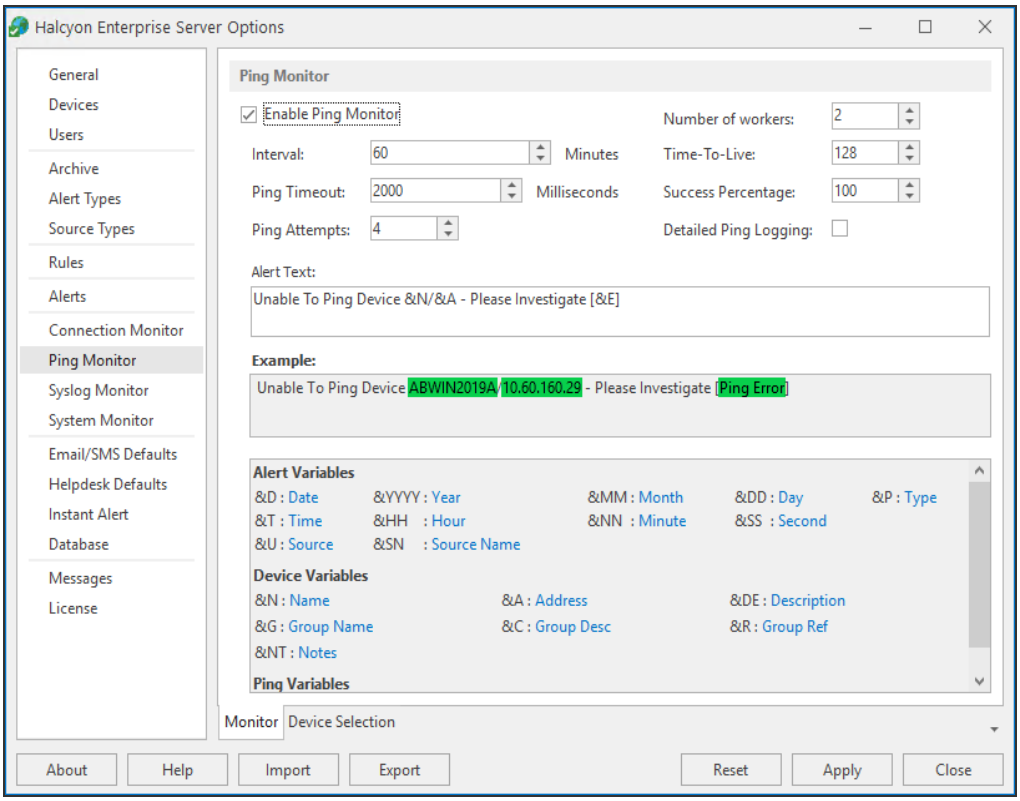
Connection Monitor substitution variables comprise:

- **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

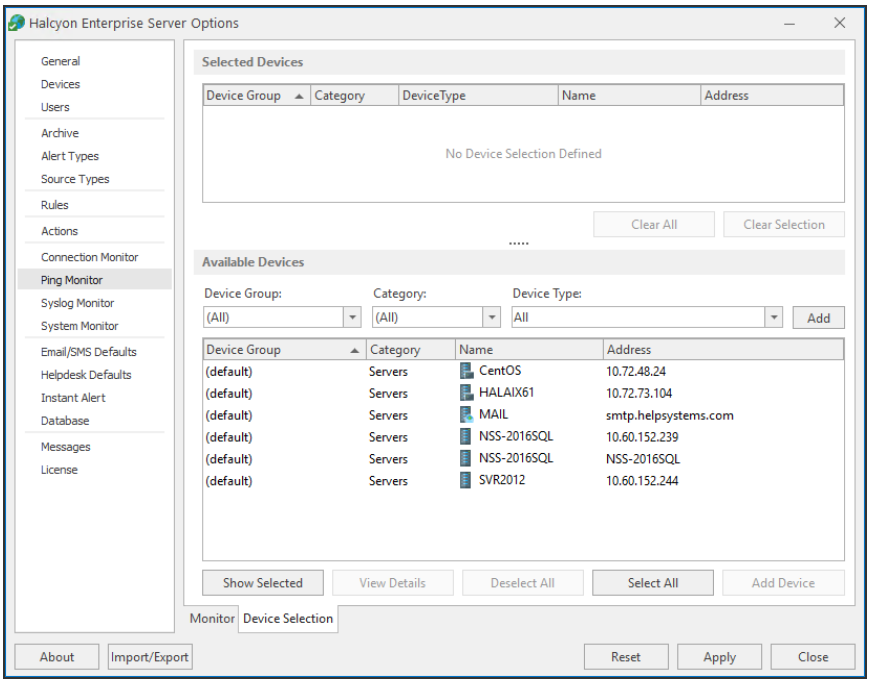
Ping Monitor substitution variables comprise:

- **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

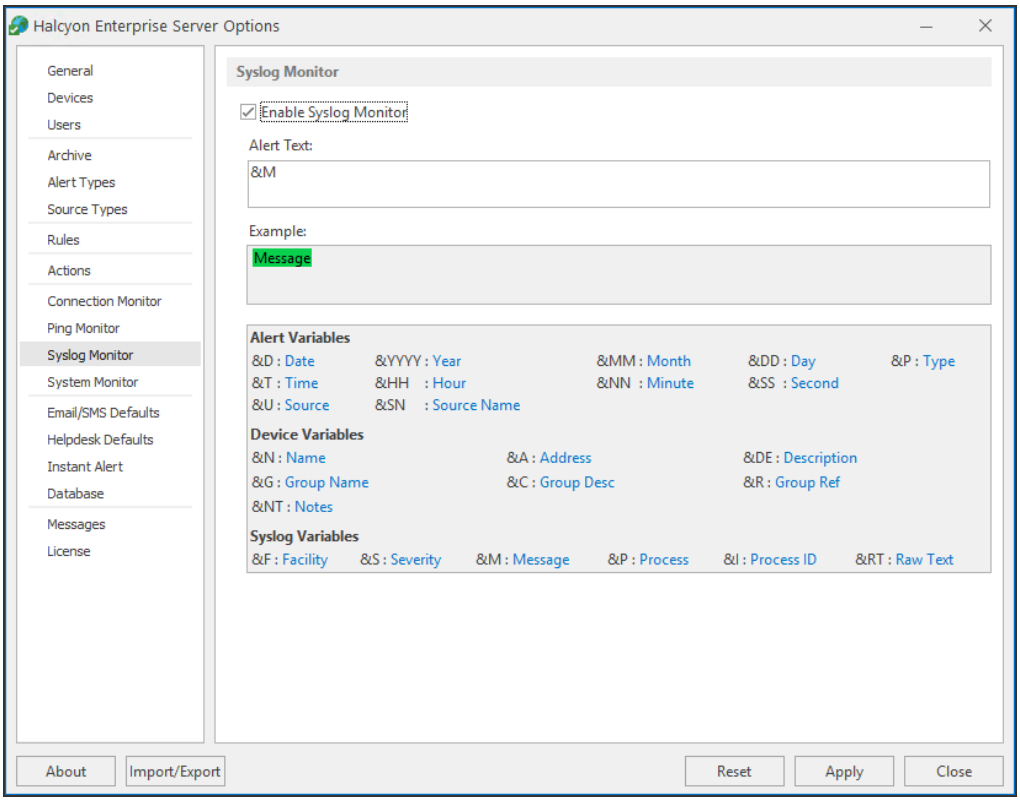
Click to deselect all of the currently selected devices in the **Available Devices** section.

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

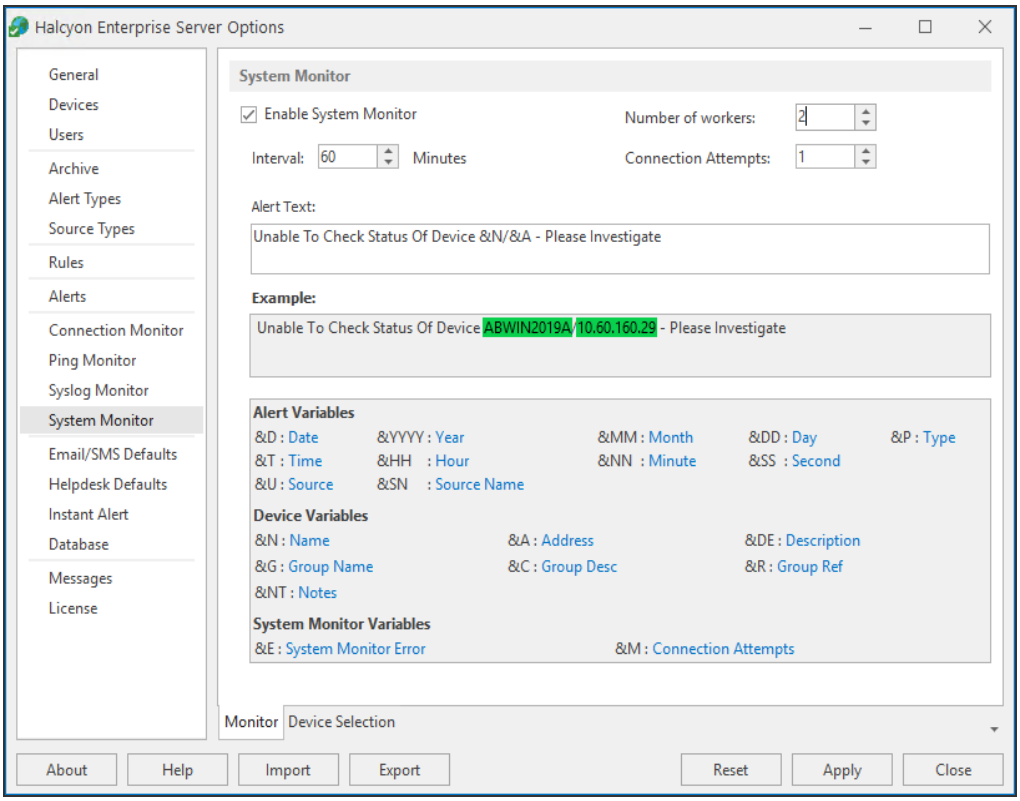
Forwarding Syslog Messages from a Linux Device

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

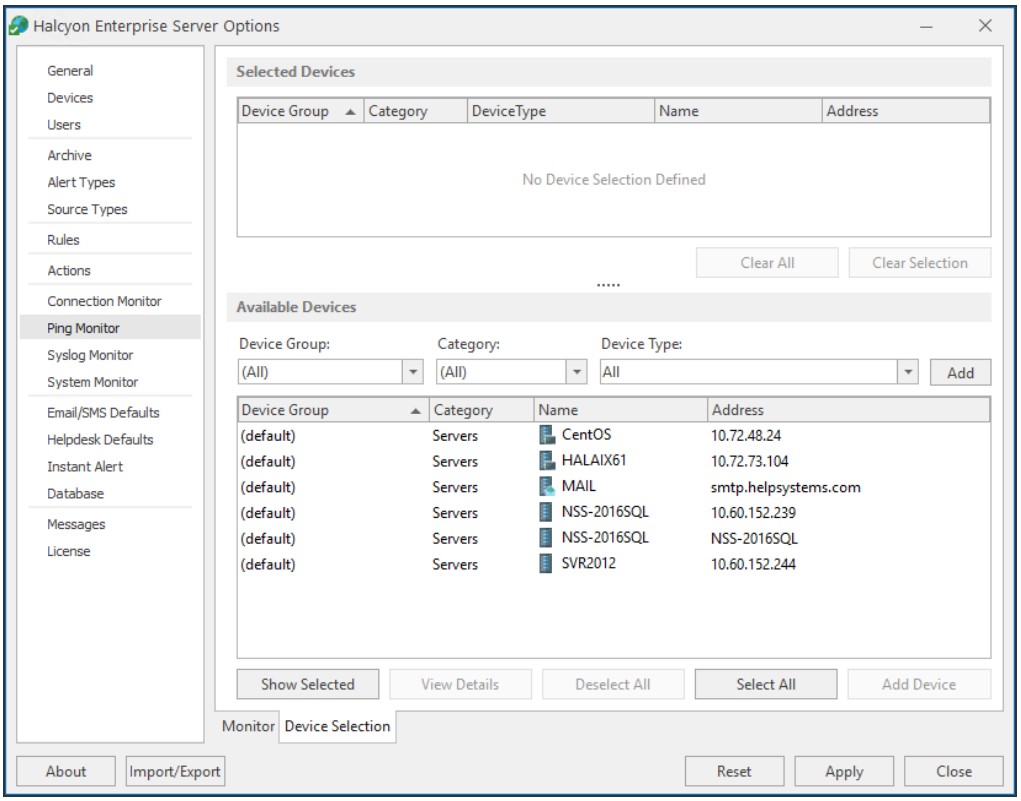
System Monitor variables comprise of:

- **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

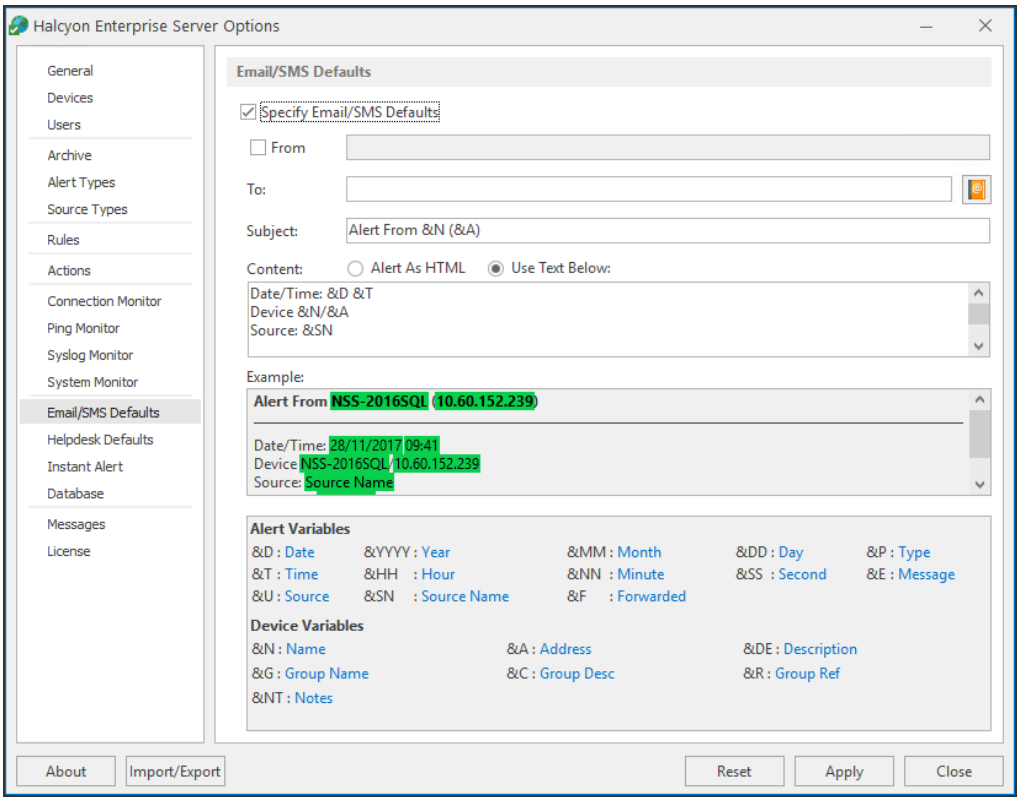
Click to deselect all of the currently selected devices in the **Available Devices** section.

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

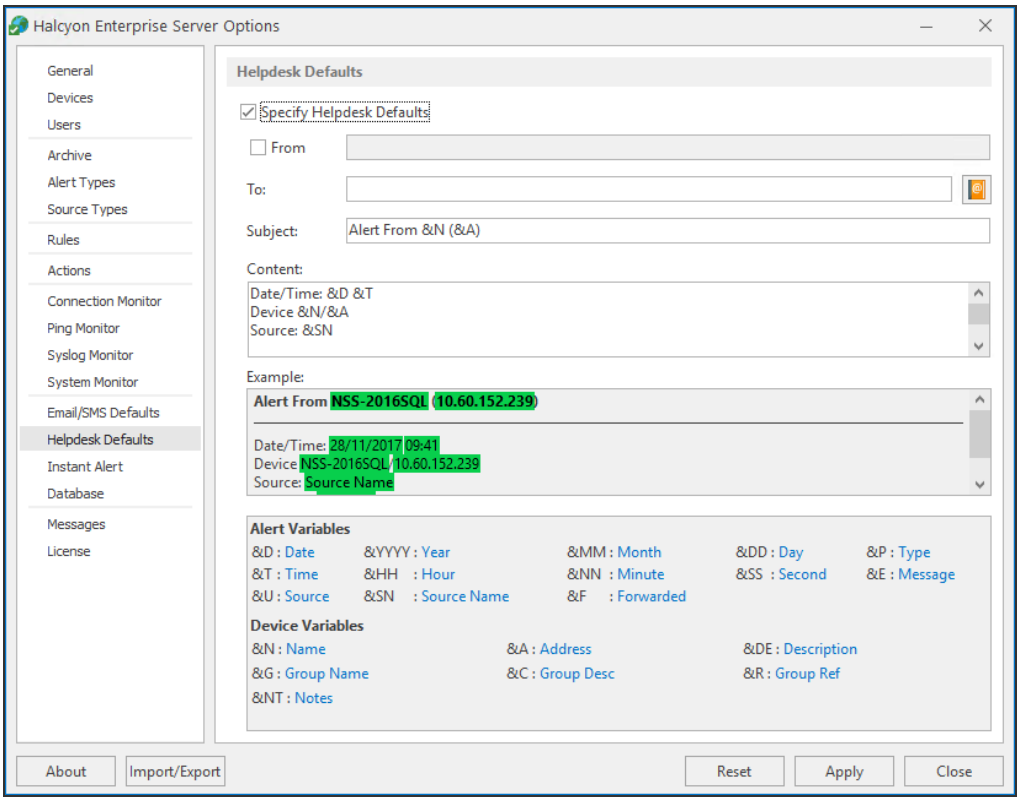
Use variables to assist in the building of the message content. Send Alert as Email/SMS substitution variables comprise:

- **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.

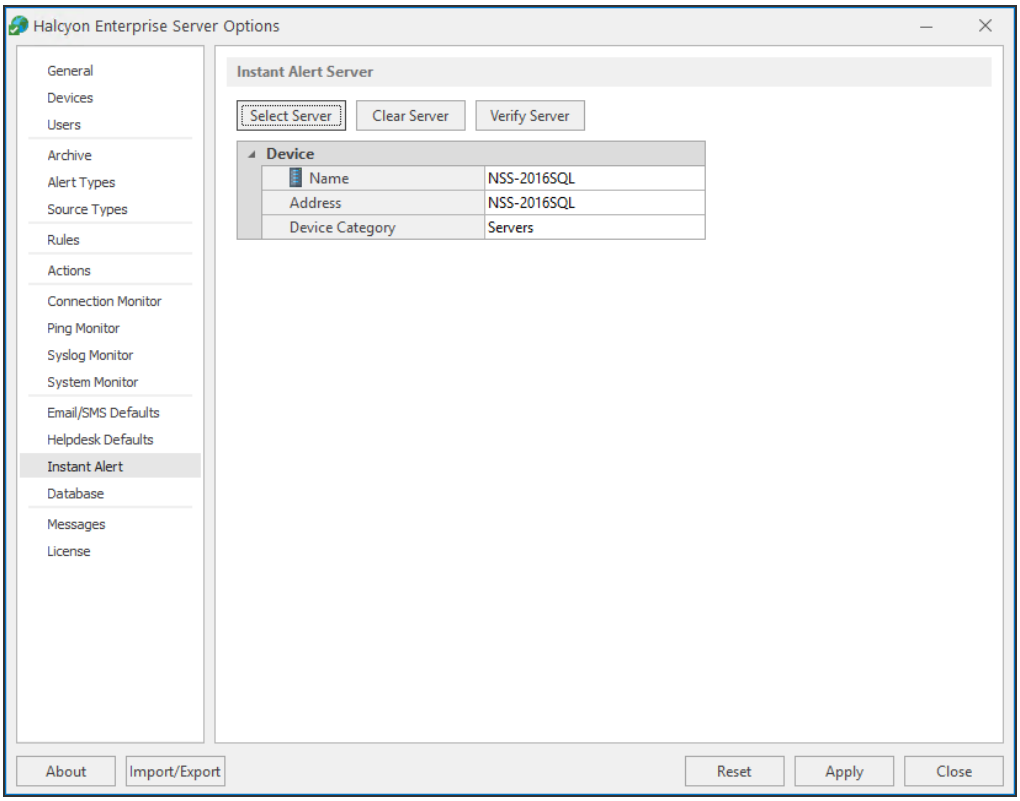
Variables

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

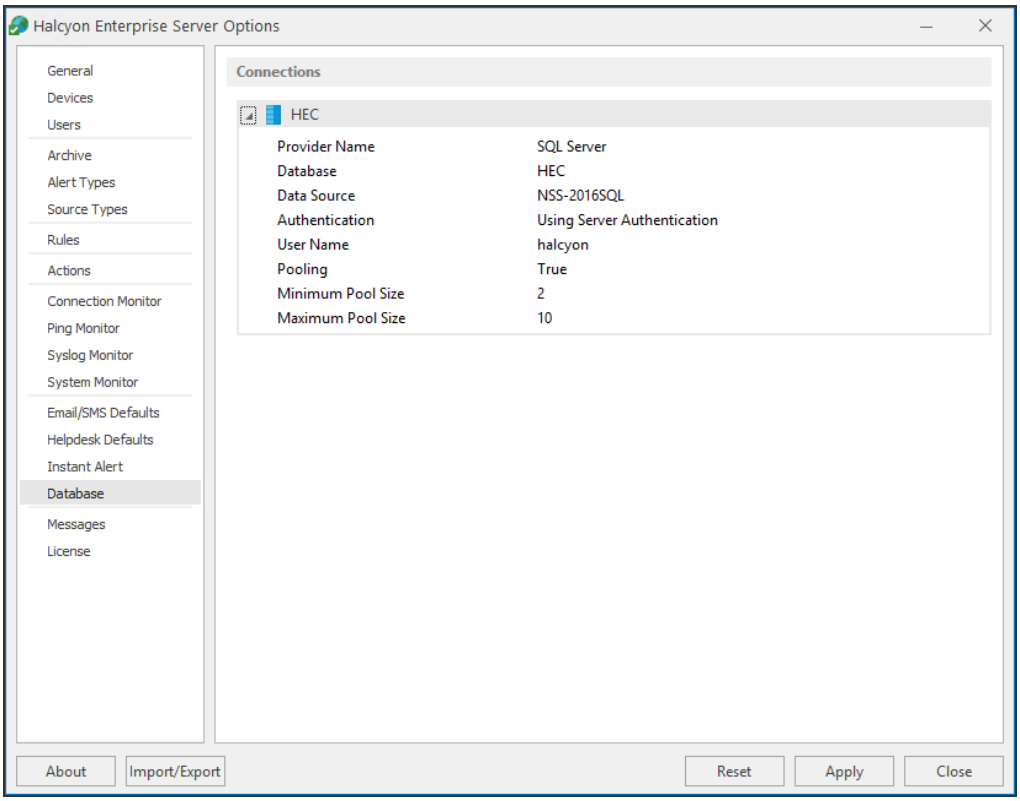
Click to remove the currently displayed device as the Instant Alert Server.

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.

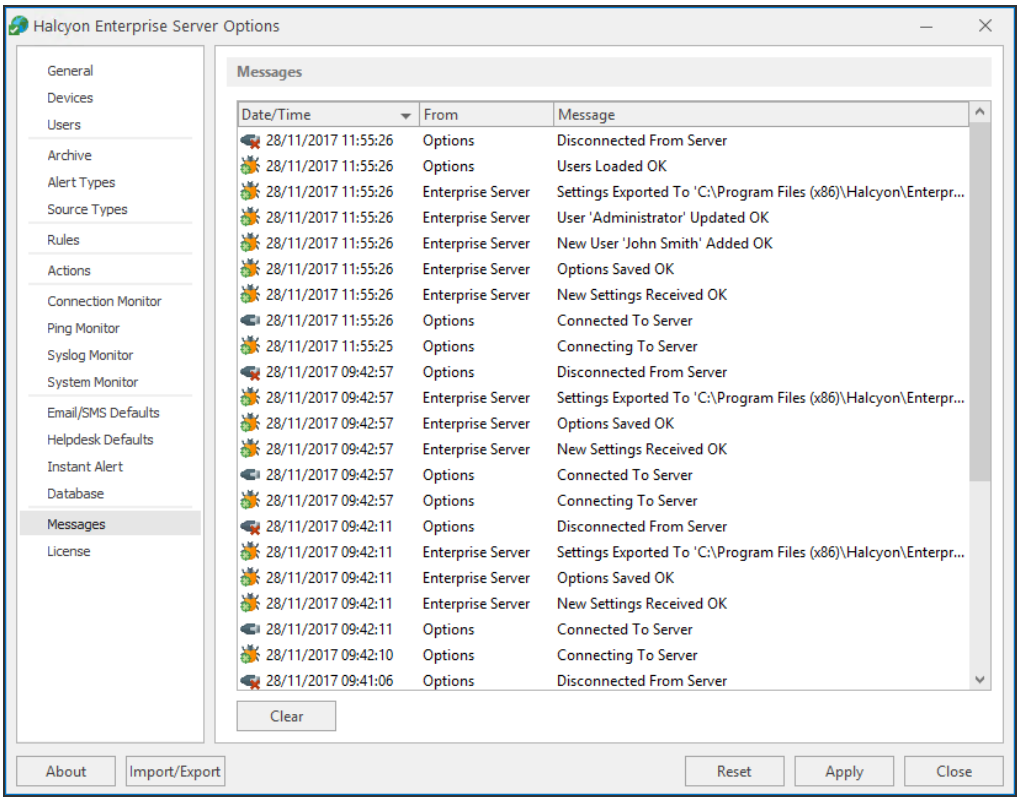
It is possible to view, but not amend, the details of the current instance.

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.

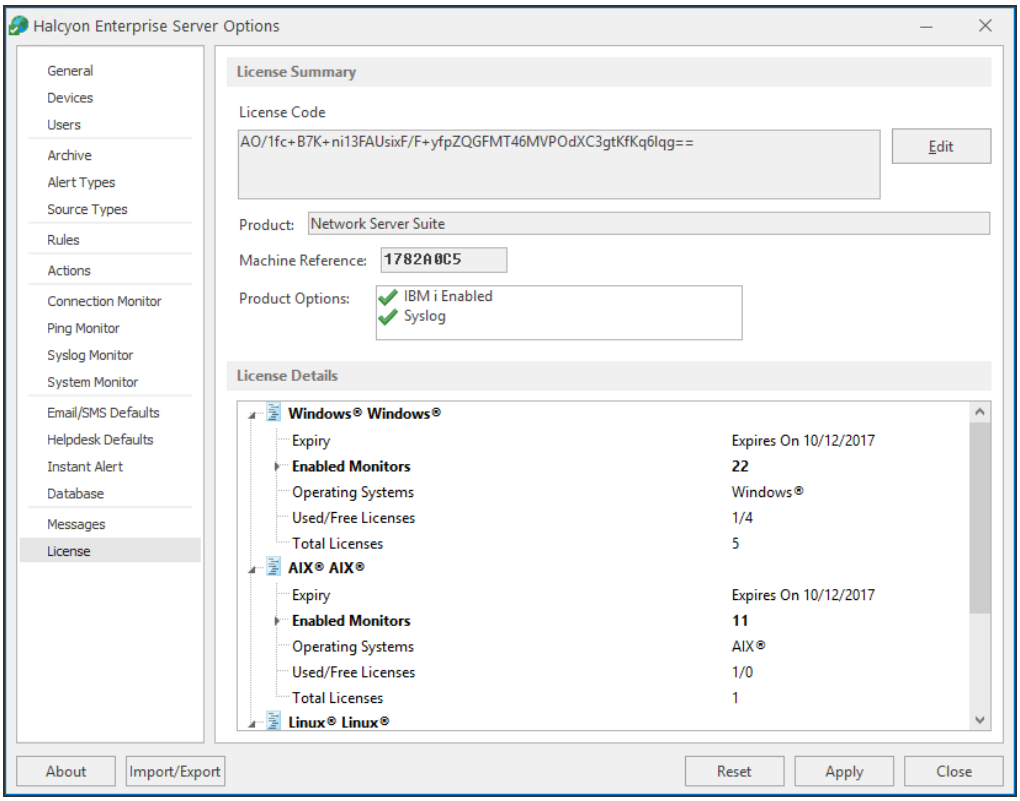
The messages in this display are generated regardless of the settings in the Message Logging Settings section of Enterprise Server Options- General page.



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

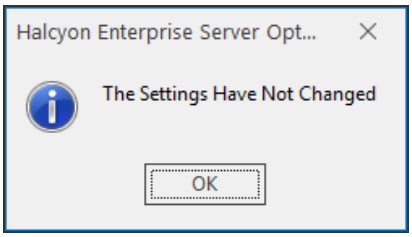
Click **Import/Export** to import or export current Enterprise Server Options settings from one device to another. See Exporting and Importing Data for more information.

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**.

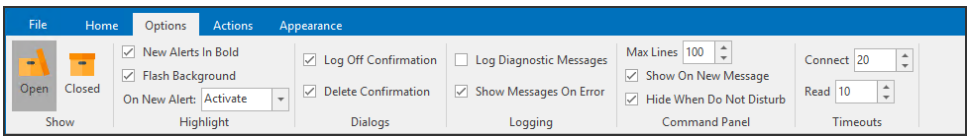
5. When prompted, click **Yes** to confirm the import and overwriting of the existing Enterprise Server Options data.

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.

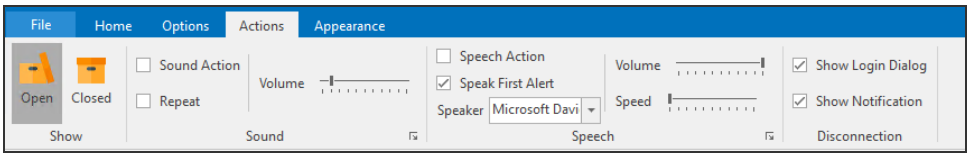
Read Timeout

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

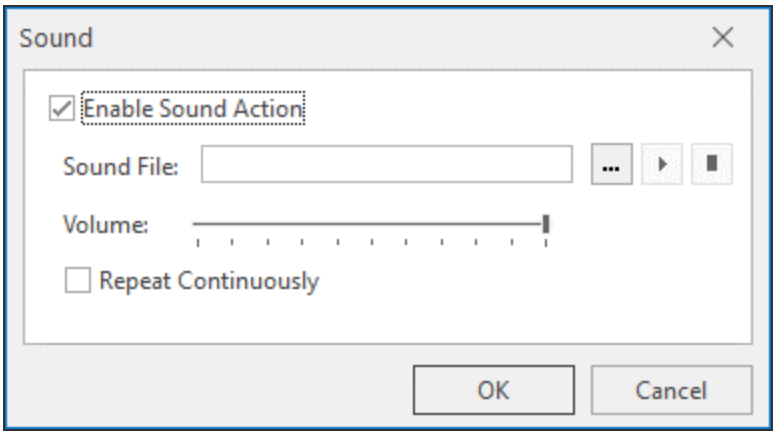
Check to have the sound played repeatedly until either **Mute Sound** or **F12** is pressed.

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

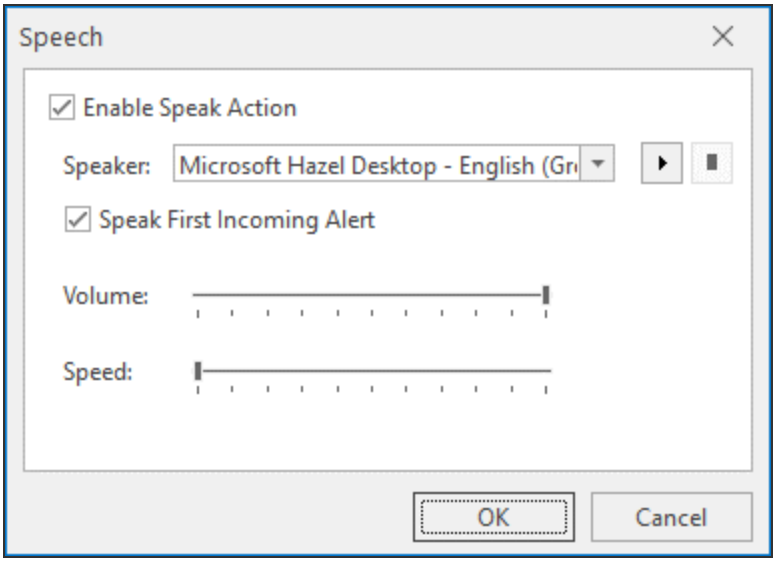
Use the slider bar to control the volume level of the speech.

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.

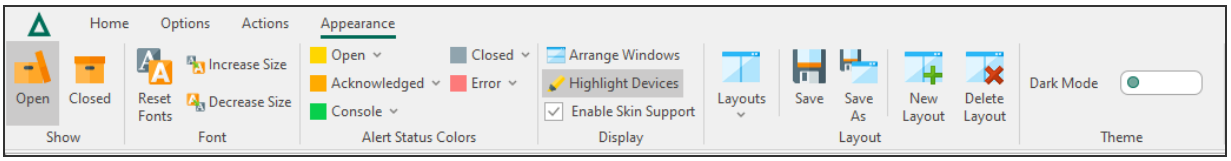
Show Notification

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**.

Theme

Dark Mode

Use the toggle switch to change the display mode from light (default setting) to dark.

> **IMPORTANT:** Dark Mode is saved per user and not by the application.
>
> Setting Dark Mode in any one of the UI ribbons applies it across all of the Network Server Suite applications, even those not currently loaded, which will then use the theme once opened.

Click the toggle switch again to return to the default light mode setting across all Network Server Suite applications.

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

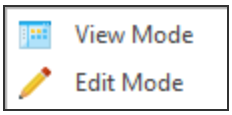
1. Open Enterprise Console.
2. From the top menu bar click and from the drop-down menu click **Import Layout**.
3. Use Windows Explorer to navigate to the location of the previously saved Enterprise Console Layout (.lyt) files.
4. Select the required .lyt files to be imported into Enterprise Console 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:

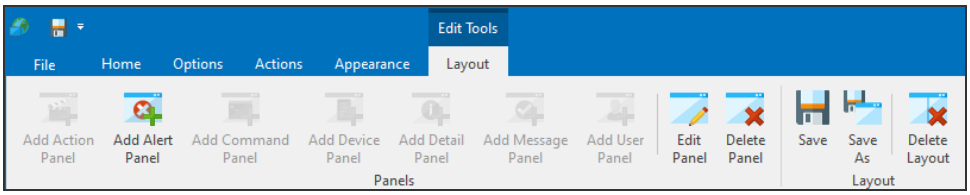
- **For View mode**: Ctrl+Alt+V
- **For Edit Mode**: Ctrl+Alt+E

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.

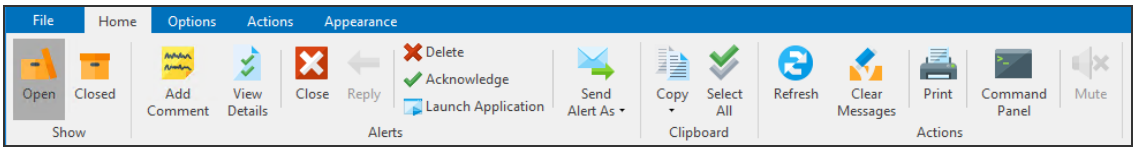
NOTE: **Edit Mode** is required in order to delete an existing panel. See Switching between View and Edit Mode for more information.

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

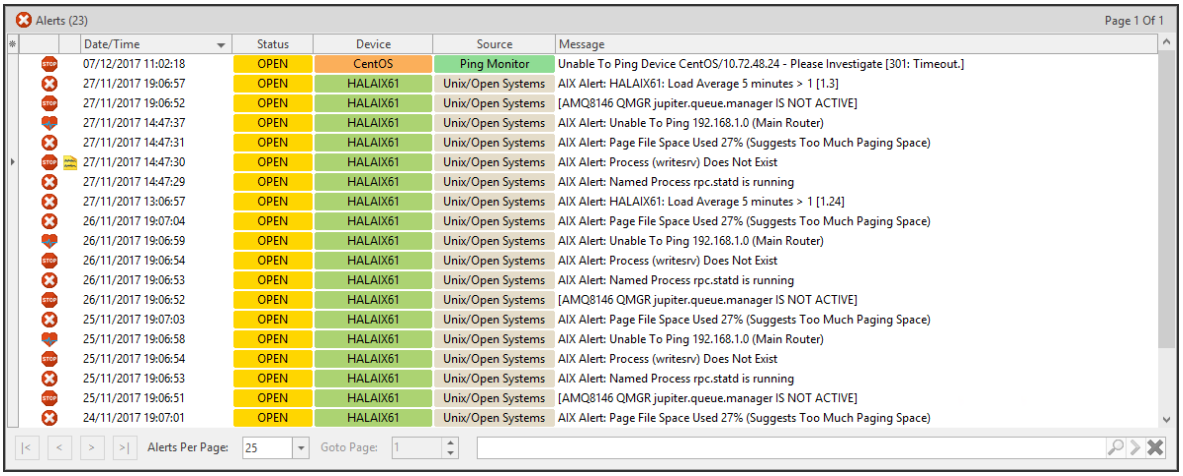
Alerts are generated as a result of rules that have been set up to monitor your network for any issues or problems. When alerts (that have an action of Send Console Action) are received they are displayed in the **Alerts** panel (by default) on the Enterprise Console.

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.

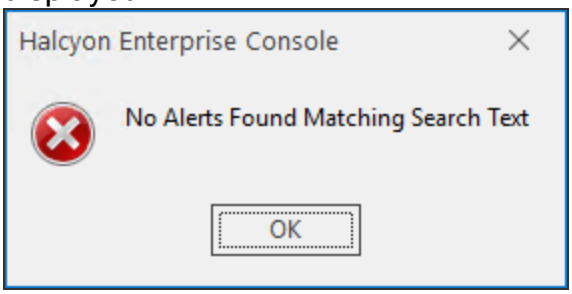
NOTE: The search option only operates on the current page of displayed alerts.

To search for specific alert text:

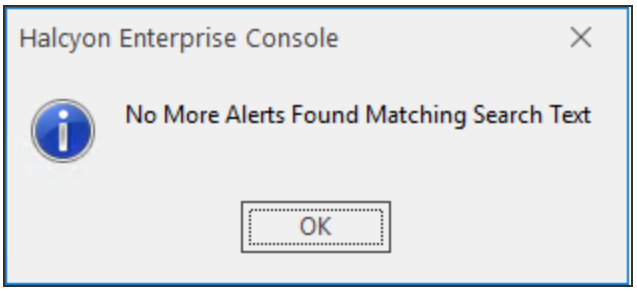
1. Type the text (either partial or full) of the alert message to be found on the current page and click **Search**.

   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.

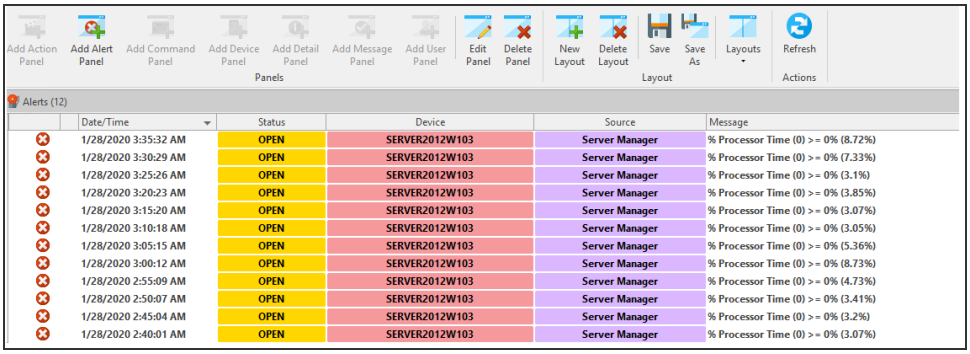
Setting up alert grouping

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.

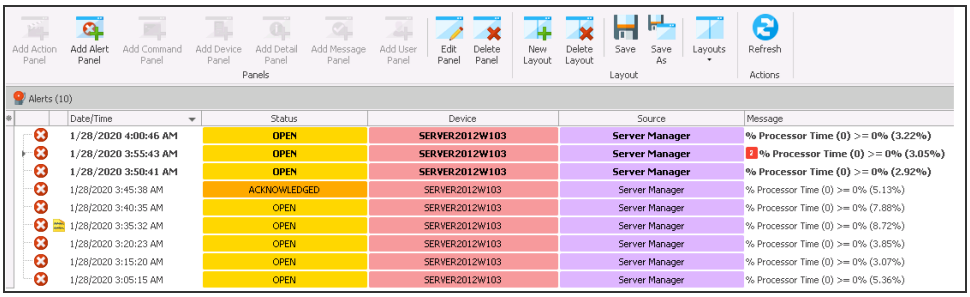
> **NOTE:** See Adding A New Layout - Grouping section for more information.

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

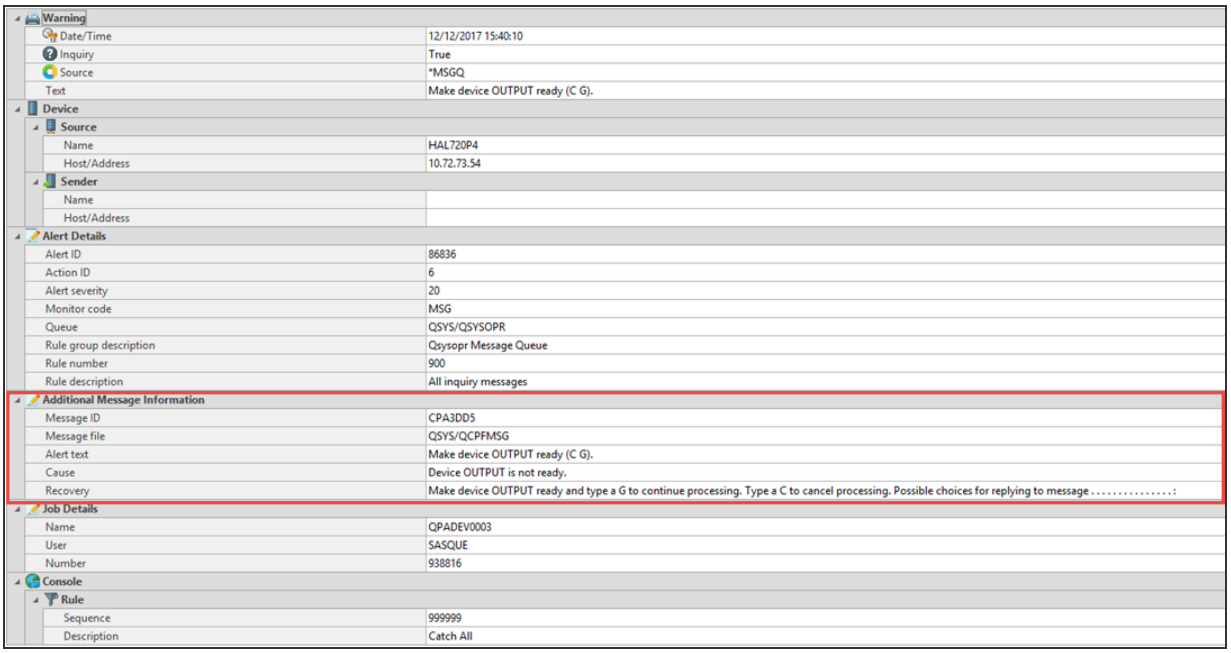
Four buttons along the bottom of the window allow you to navigate sequentially through alert details of all the alerts in the selected panel.

- 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.



Warning	
Date/Time	12/12/2017 15:40:10
Inquiry	True
Source	*MSGQ
Text	Make device OUTPUT ready (C G).
Device	
Source	
Name	HAL720P4
Host/Address	10.72.73.54
Sender	
Name	
Host/Address	
Alert Details	
Alert ID	86836
Action ID	6
Alert severity	20
Monitor code	MSG
Queue	QSYS/QSYSOPR
Rule group description	Qsysopr Message Queue
Rule number	900
Rule description	All inquiry messages
Additional Message Information	
Message ID	CPA3DD5
Message file	QSYS/QCPFMSG
Alert text	Make device OUTPUT ready (C G).
Cause	Device OUTPUT is not ready.
Recovery	Make device OUTPUT ready and type a G to continue processing. Type a C to cancel processing. Possible choices for replying to message . . . . . :
Job Details	
Name	QPADEV0003
User	SASQUE
Number	938816
Console	
Rule	
Sequence	999999
Description	Catch All

Closing the Alert Details dialog

Click **Close** in the navigation bar to exit the **Alert Details** dialog.

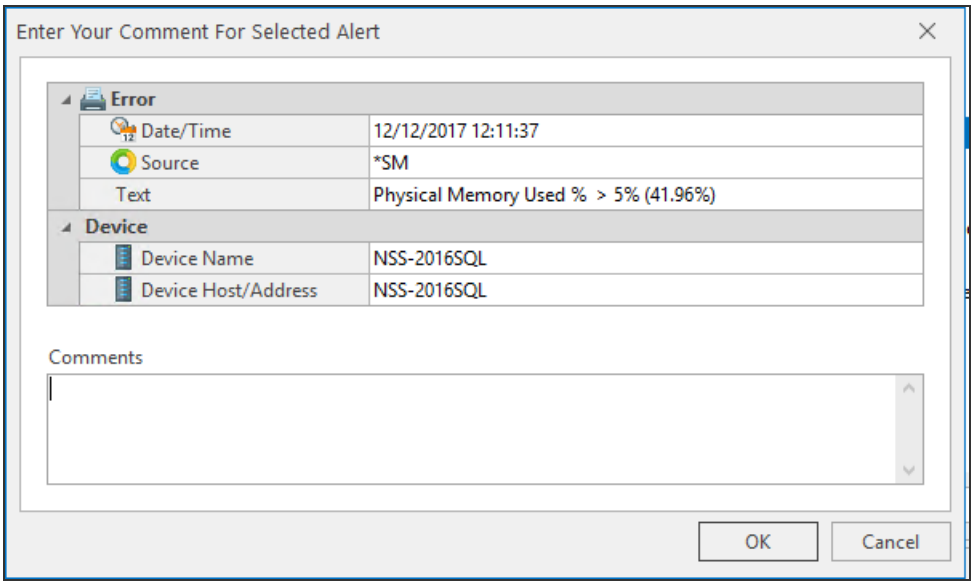
Adding Alert Comments

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

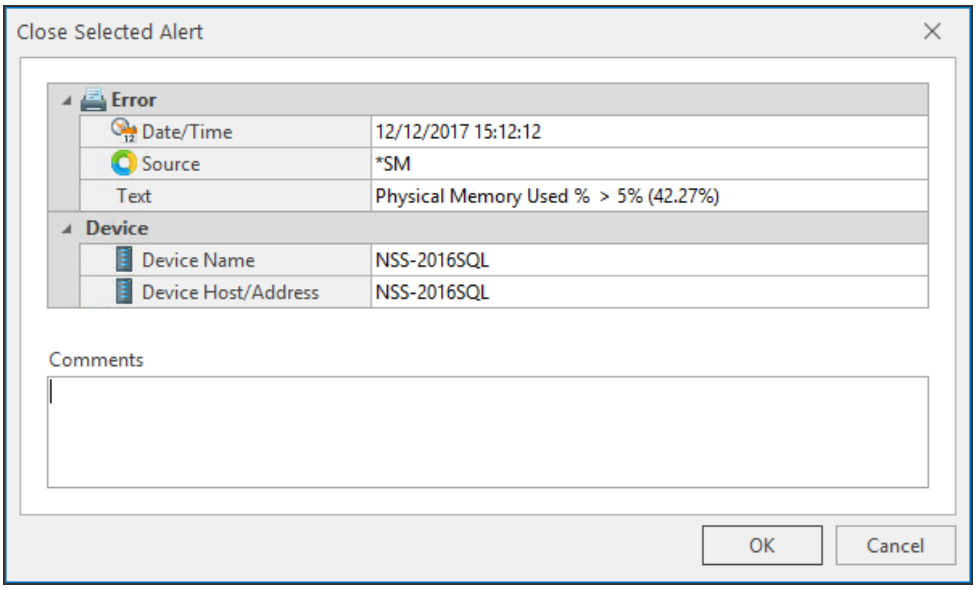
Alerts remain on the **Enterprise Console Open** alerts page, until they are closed at which point they disappear from the live console but can still be viewed using the Closed Alerts option. Multiple selections of alerts in a single Close operation are permitted.

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.

Closed Alerts

Once an alert has been closed, it can be viewed through the **Closed Alerts** view, available from the **Enterprise Console** | **Home** menu ribbon.

Closed Alerts are available to view via this option until they are purged from the database.

Closed Alerts

The number of closed alerts currently held in the database is shown in brackets in the header of this panel.

Closed alerts are displayed with the same information as that available in the Open alerts panels.

By default this page shows alerts that have been closed from midnight on the first day of the current month up to one minute to midnight on today's date.

Filtering options

Filtering options can be used to specify which closed alerts are displayed in the **Closed Alerts** panel. Filtering options are chosen from the **Filter** panel to the left of the **Closed Alerts** panel in the default layout.

By Date Range

Closed alerts are filtered by date and time range by default.

To set a Date and Time Filter:

1. From the Filter panel, select the **Date Range** tab, then do one of the following:

- Over-type the current entries with new dates and times in the correct format.
- Use the up/down arrows to the right of each option to select a new date and time

Click **Search** to retrieve any alerts closed within this range and display them in the **Closed Alerts** panel.

By Device

Filtering by device allows the retrieval and display of closed alerts from a group of devices, multiple devices within the same or different groups or by single device. The Default group, and all the devices contained within is selected by default when this filtering option is selected.

To Filter by Device:

1. From the Filter panel, select the **Devices** tab. Then:

- To filter by the pre-selected default group click **Search**.
- Click on other groups listed in this section to enable the search on these groups and the devices they contain. Click **Search**.
- Click on the arrow to the left of the group name to expand the group and select individual devices. Click **Search**.

By Source

Filtering by Source type allows the retrieval and display of closed alerts from all, multiple or single sources from where the alert originated.

To Filter By Source:

1. From the Filter panel, select the **Source** tab. Then:

- To filter by any source type, click **Search**.
- Click **Any Source** to remove this selection and enable the selection of individual or multiple sources. Click **Search**.

TIP: With the **Any Source** options deselected use **Select All** to reselect all source types or **Select None** to remove the selection from all source types.

By Alert Types

Filtering by Alert Type allows the retrieval and display of closed alerts from all, multiple or single alert types from which the alert originated.

1. From the Filter panel, select the **Alert Type** tab. Then:

- To filter by any alert type, click **Search**.
- Click **Any Alert Type** to remove this selection and enable the selection of individual or multiple alert types. Click **Search**.

TIP: With the **Any Alert Type** options deselected use **Select All** to reselect all alert types or **Select None** to remove the selection from all source types.

By Text

Filtering by Text allows the retrieval and display of closed alerts based upon the contents of the alert message text. Single, or multiple criteria can be specified to make the search as generic or as specific as required.

Options in this panel defines the alert text based on conditional parameters (equal to or not equal to) when used in combination with entry in the Details Text field. This can be generic or free text and can also use detail data values (alphanumeric, numeric and date/time) to retrieve alerts that match the selection criteria. User-definable wildcard characters can be used when defining this text.

Once the text selection criteria have been entered, click **Search**.

Specifying the number of alerts displayed per page

Alerts are displayed in sequential pages within the **Closed Alerts** panel. The default setting is to display 25 alerts per page.

To change the number of closed 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 **Closed 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.

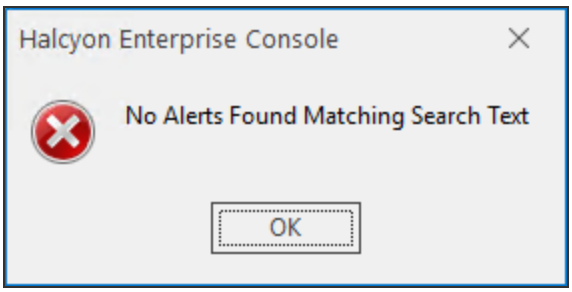
NOTE: The search option only operates on the current page of displayed alerts.

To search for specific alert text:

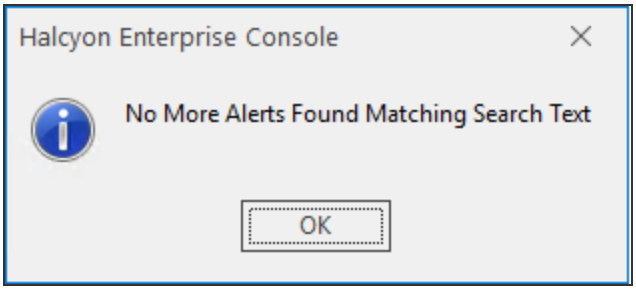
1. Type the text (either partial or full) of the alert message to be found on the current page and click .

If the text is found, the first alert containing the full or partial text on this page is highlighted in the alert panel. Click the **Next** arrow 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 the **Next** arrow is clicked, the following message is displayed.



2. Use **Delete** to remove the message text search criteria from the **Search** bar.

Options available with working with Closed Alerts

When working with closed alerts, the following options are available from the **Enterprise Console** | **Home** menu ribbon.

Add Comment

Select a group or individual alert and click **Add Comment** to add a comment to the selection.

View Details

Select a group or individual alert and click **View Detials** to open the Alert Details dialog providing comprehensive information regarding the selection.

Copy

Select an individual closed alert, click **Copy** and select whether to copy the alert summary, detail or detail as text or XML.

Select All

Click **Select All** to select all the alerts that are currently not selected.

Select None

Click **Select None** to remove the selection from all the alerts that are currently selected.

Invert Selection

Click **Invert Selection** to display the alert, or group of alerts with an inverted background.

Print

Select an individual or multiple alerts and click **Print** to open the **Print Preview** dialog from where various print options can be invoked.

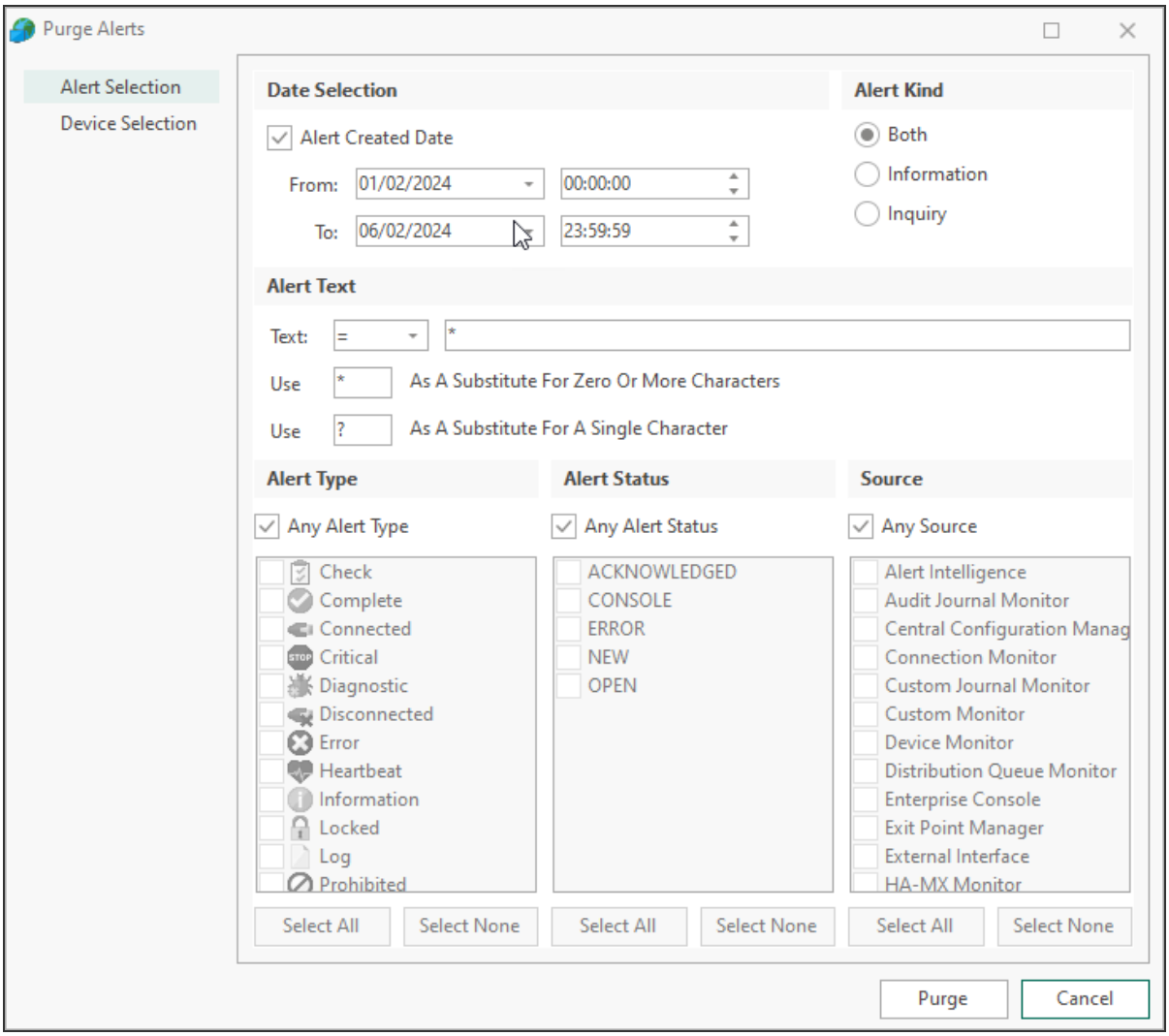
Purging Alerts

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.

Central Configuration Manager

Overview

The Central Configuration Manager (CCM) component of Network Server Suite is used to host the Server Manager elements for Windows, AIX and Linux operating systems.

The Server Manager is used to configure monitors and rules, apply templates and setup generic performance reporting criteria.

Once a device has been defined within Device Manager it can be added as a system within the Network Server Suite, although only servers and workstations can be monitored through functionality within the CCM.

> **NOTE:** Printers, hubs, routers and the like can be monitored by the use of SNMP Traps in Enterprise Server Options, if you have the appropriate license.

Once added as a system, various monitors become available that you can then apply to constantly check this system for common causes of errors and issues that may affect stability and performance on your network enterprise. Pre-defined templates can be used to speed up the process of applying key monitors across the network. A reporting template can be applied at system level to provide information on generic performance data to ensure that systems can be maintained at optimum performance levels.

> **NOTE:** See the sections Working with Monitors, Templates and Reporting for more details on how to use these functions.

CCM Server

The CCM Server is a background service associated with the Central Configuration Manager that allows communication between devices in a similar way to that used by the Enterprise Server.

A default CCM Server can be specified that is then applied to all devices added as systems within the Central Configuration Manager. See Central Configuration Manager - Options - Servers panel for more details.

Specifying an alternative CCM Server

You may need to change the CCM Server device should you have another device situated behind a firewall with which you need to communicate.

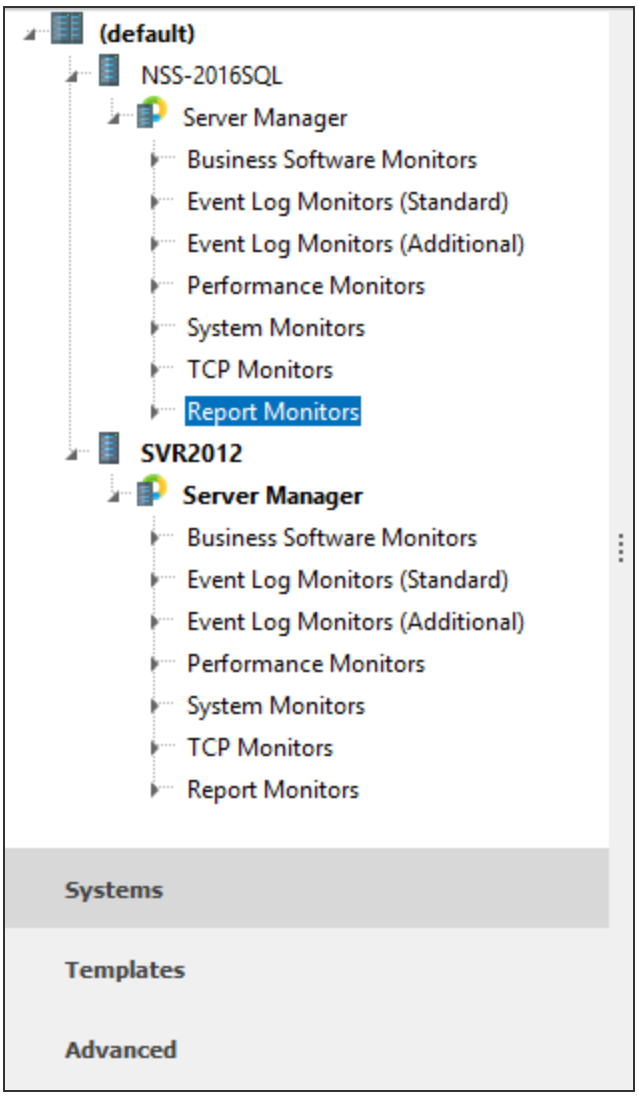
In these instances, change the CCM Server to the Network Address Translation (NAT) Address that your remote server uses to talk back to your Enterprise Server.

Systems

A system is a single device in the network that has a Network Server Suite license applied to it. Systems can be running any one of Windows, AIX or Linux operating systems. All licensed systems are displayed, within the Device Group to which they are assigned, in the Central Configuration Manager- **Systems** tab.

> **NOTE:** Non-server devices such as Printers, Routers and Modems are not shown in this panel even though they may exist in Device Manager.

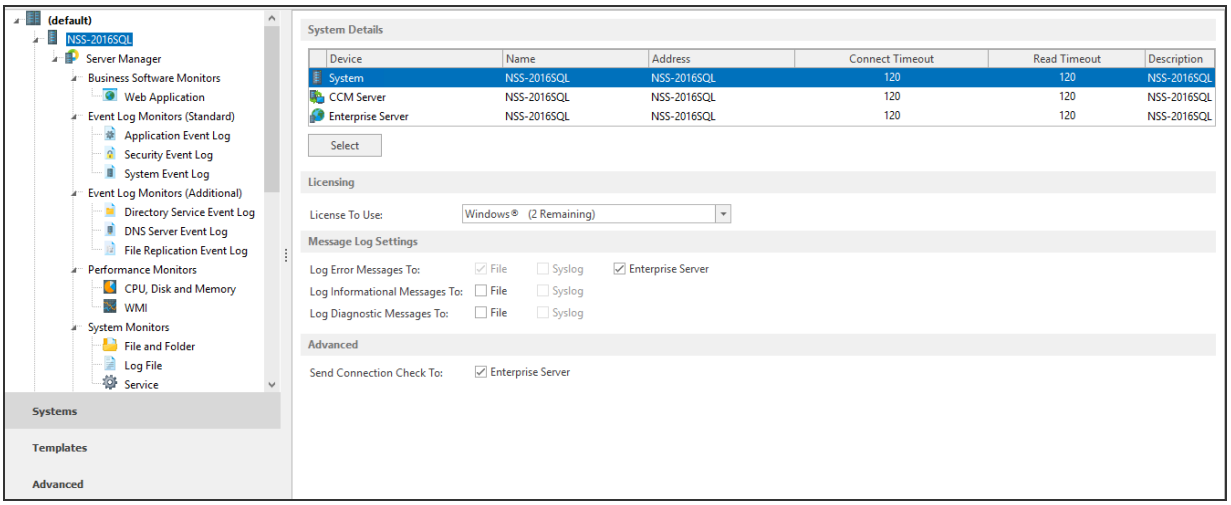
Click the **Systems** tab in the left-hand navigation panel of the Central Configuration Manager to display a tree view of currently managed systems.



Beneath each system is a list of available monitors. This list is dependent on the license assigned to each monitor.

The monitor name is shown in **bold** typeface if a rule, template or reporting structure has been applied.

When at System level in the Systems panel (the system name is highlighted), the System details are shown in the main panel of the Central Configuration Manager.



System Details section

Shows the details of both the system and the associated Enterprise Server and CCM Server devices. In most instances these will be installed on the same system.

Click on a device to select it. Click **Select** to view or amend the details of the device that is currently highlighted.

See Selecting CCM Server and Selecting Enterprise Server for more information.

Licensing section

The license settings show the current number of licenses available for the operating system to which the selected system belongs. The entry displayed in this field changes as you change between systems on different operating systems.

> **NOTE:** If you only have systems using a single operating platform, then the name of that operating system is the only one displayed in this field.

See Applying Individual Licenses for more information on how to license systems within Central Configuration Manager.

Message Log settings

Use the following options to set the log settings for the selected system.

On AIX and Linux systems, the default setting is to log messages (except Diagnostic Messages which are File and Syslog only) to the Syslog, and additionally to a file and the Enterprise Server device.

> **NOTE:** All log files are saved with an extension of .hlf.

Log Error Message To

On non-AIX and Linux systems, error messages are automatically logged to the error message log file. See Logging Panel for more information. Error messages can also be logged to the Enterprise Server device if required.

Log Informational Messages

Check to ensure that any generated Informational Messages are logged to file.

Log Diagnostic Messages

Check to ensure that any generated Diagnostic Messages are logged to file.

Advanced section

Send Connection Check To

Automatically defaults to ensure that a connection check is periodically sent to the Enterprise Server to ensure constant connection between the two devices. It is recommended that this setting is left unchanged.

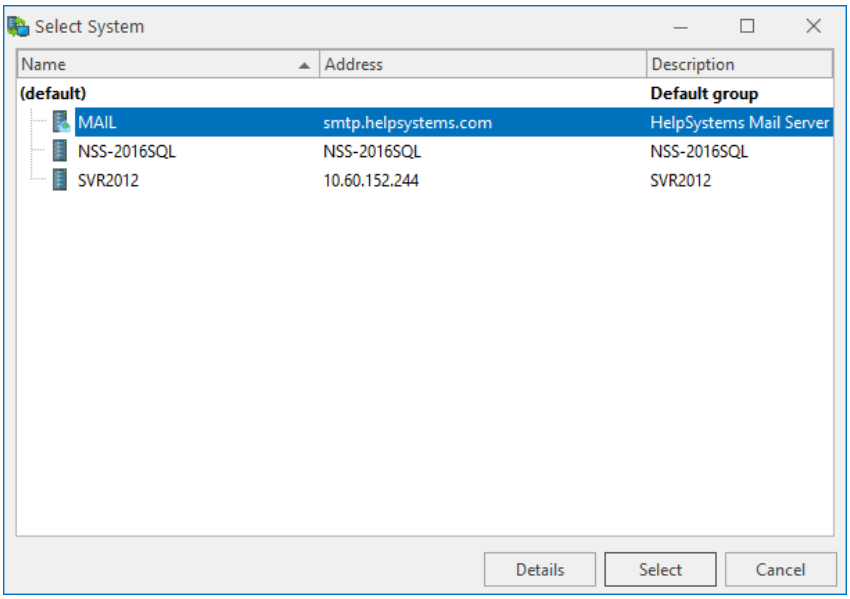
Adding a System to Central Configuration Manager

To add a system (which must first be defined in Device Manager (see Adding a Device) to the Central Configuration Manager:

1. Click **Add System** from the Central Configuration Manager toolbar ribbon.

   The **Select System** dialog is displayed.

> **NOTE:** This action can only be undertaken from the top level (**default or Device Group name**) of the system tree in the **Select Systems** navigation panel.



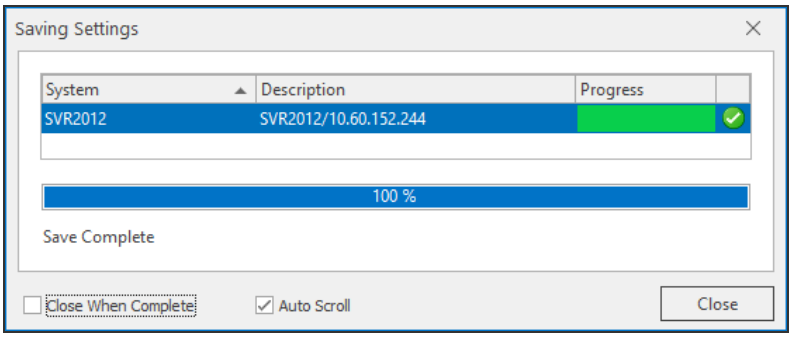
2. Highlight the required system and click **Select**. The **Add System** dialog is displayed.
3. Select the system to be added to Central Configuration Manager.

NOTE: The **Install Software On System** option is activated as a default on all systems except AIX and Linux Devices. This option remotely installs the Server Manager software onto the system being added. See also: Central Configuration Manager Options: Installation Panel

If required, an alternative Enterprise Server and/or CCM Server device can be specified by highlighting the respective device in the **Add System** dialog and clicking **Select**. The **Select System** dialog is re-displayed from where an alternative device can be chosen.

4. Click **OK** to add the system to the Central Configuration Manager and if chosen, install the Server Manager software.
5. Click **Save** to save the current settings.

   The **Saving Settings** dialog is displayed.



6. If the default setting of **Install Software on System** has been retained and the system is running Windows, valid log-in details for the system are required. This can either be

the current **Active User** or a **Specific User**. Select the required option and complete any prompts for additional information as necessary.

NOTE: This feature requires the Windows ADMIN share to be enabled and the selected user must have administrative account authority on the remote system.

7. Click **OK** to remotely install the software onto the system and continue saving settings.

TIP: On the **Save Settings** dialog, check the **Close When Complete** option to automatically shut the dialog when Save Settings is completed.

Deleting Systems

Systems can also be deleted from the Central Configuration Manager if they are no longer required.

To delete a system from Central Configuration Manager:

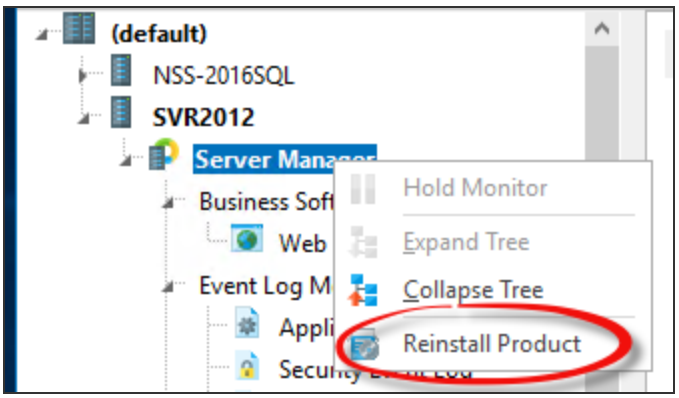
1. Select the required system in the left-hand navigation pane of the systems tab.
2. Click **Delete System** from the Central Configuration Manager toolbar ribbon. The **Delete System** dialog is displayed.
3. To remove the installed software at the same time as removing the system, click **Delete Software From System**.
4. Click **OK** to delete the system from Central Configuration Manager. The system remains as a selectable device from with Device Manager.
5. Click **Save** to save the changes.

Once deleted, the license previously applied to this system becomes available for assignment to an unlicensed system. The unlicensed system must be using the same Operating System.

WARNING: A Windows license cannot be applied to an unlicensed system running AIX or Linux and vice versa.

Re-installing Software Remotely

Windows Server Manager software can be re-installed remotely on a Windows system at any time by right-clicking on the relevant **Server Manager** (listed beneath the System Name) in the Systems navigation panel and selecting **Reinstall Product** from the pop-up menu.



TIP: A remote install of Network Server Suite requires the ADMIN share to be available.

Alternatively, software can be remotely re-installed on existing systems by clicking  | **Reinstall Product** from the menu bar.

NOTE: **Required Authority**: The user must have administrative account authority on the remote system. See Central Configuration Manager Options - Installation Panel for more information.

Upgrade Systems

Use the Upgrade Systems feature to install the latest version of the Network Server Suite onto remote systems.

From the Central Configuration Manager menu bar, click | **Upgrade Systems**.

TIP: Click **Get Versions** to display the current version of the software running on each system.

WARNING: A remote upgrade of Network Server Suite requires the ADMIN share to be available.

All available systems are listed by default and the **Check All** option enabled, meaning all systems are automatically selected for upgrade. If all the systems are not immediately visible, the dialog can be resized.

Agent systems are listed by the group under which they are defined in Device Manager. All the machines within a group or just selected devices can be upgraded.

Click next to any systems (or Group) that you **DO NOT**want to upgrade so that the tick mark is removed.

Click **OK** to start the upgrade process.

Depending on the settings that are in the Installation Panel of Central Configuration Manager Options, a user log in and password may be requested. Enter a valid user ID and password which must have administrative account rights on the remote system.

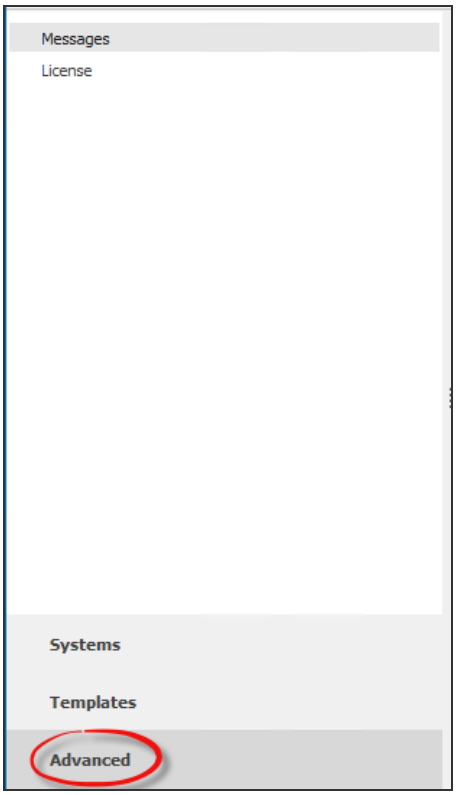
The upgrade process continues. Check the **Close When Complete** option to automatically close this dialog once the upgrade is complete. If the upgrade process fails on one or more of the agent machines, this dialog remains open and the systems that have not upgraded correctly are identified by a red cross icon. Hover the mouse pointer over the icon to display a screen tip showing the reason for the failure.

Once complete, save the settings using **Home** | **Save**.

Central Configuration Manager - Advanced Settings

Advanced settings of the Central Configuration Manager allow the viewing of connectivity messages and license information.

From the left-hand navigation panel select **Advanced**.

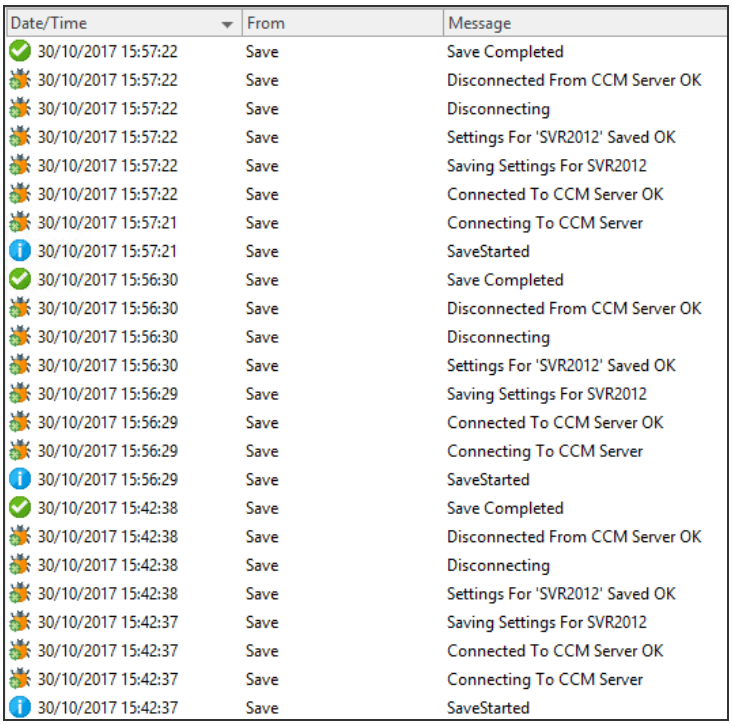


The **Advanced** tab contains two pages of configuration information.

Messages page

The **Advanced** | **Messages** page shows details of any system messages that are sent between the Central Configuration Manager and Remote Servers.

The Messages panel is used to display Informational and/or Diagnostic messages depending on the Logging settings specified in the Central Configuration Manager Options.



Date/Time	From	Message
30/10/2017 15:57:22	Save	Save Completed
30/10/2017 15:57:22	Save	Disconnected From CCM Server OK
30/10/2017 15:57:22	Save	Disconnecting
30/10/2017 15:57:22	Save	Settings For 'SVR2012' Saved OK
30/10/2017 15:57:22	Save	Saving Settings For SVR2012
30/10/2017 15:57:22	Save	Connected To CCM Server OK
30/10/2017 15:57:21	Save	Connecting To CCM Server
30/10/2017 15:57:21	Save	SaveStarted
30/10/2017 15:56:30	Save	Save Completed
30/10/2017 15:56:30	Save	Disconnected From CCM Server OK
30/10/2017 15:56:30	Save	Disconnecting
30/10/2017 15:56:30	Save	Settings For 'SVR2012' Saved OK
30/10/2017 15:56:29	Save	Saving Settings For SVR2012
30/10/2017 15:56:29	Save	Connected To CCM Server OK
30/10/2017 15:56:29	Save	Connecting To CCM Server
30/10/2017 15:56:29	Save	SaveStarted
30/10/2017 15:42:38	Save	Save Completed
30/10/2017 15:42:38	Save	Disconnected From CCM Server OK
30/10/2017 15:42:38	Save	Disconnecting
30/10/2017 15:42:38	Save	Settings For 'SVR2012' Saved OK
30/10/2017 15:42:37	Save	Saving Settings For SVR2012
30/10/2017 15:42:37	Save	Connected To CCM Server OK
30/10/2017 15:42:37	Save	Connecting To CCM Server
30/10/2017 15:42:37	Save	SaveStarted

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.

Clearing Messages

From the **Home** menu ribbon, click  **Clear Messages** to remove the messages from this display.

Alternatively, right-click on an individual message (or select multiple messages) in the Messages panel and select **Clear** from the pop-up menu.

License page

The **Advanced** | **License** page of the Central Configuration Manager contains information relating to the current licensing of Network Server Suite.

This is covered in detail in the Enterprise Server Options - Licenses page.

Saving Central Configuration Manager settings

Any changes made within the Central Configuration Manager must be saved prior to exiting the program otherwise the changes are canceled.

When any changes have been made to a system configuration within the Central Configuration Manager, the top level system name in which the changes were made is highlighted within the left-hand navigation panel.

> TIP: Settings need to be saved when **Save** becomes available on the Central Configuration Manager **Home** and **Options** menu ribbon.

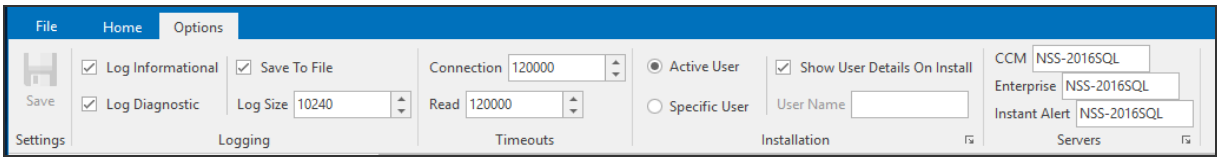
A progress bar for each agent machine is displayed when saving settings. The disk icon changes to a tick mark encased in a green circle to indicate that the settings have been successfully saved.

The **Saving Settings** dialog remains open until **Close** is selected, unless the **Close When Complete** option is checked.

Central Configuration Manager Options

Options are used to set specific configuration options regarding the operation of Central Configuration Manager.

Central Configuration Manager Options are opened by selecting **Options** from the menu bar.



TIP: Any changes made directly in the **Options** panel are saved immediately and do not require the **Save** option from the **Settings** panel.

There are four separate panels that can be used to change configuration options:

CCM Logging panel

This panel provides options to log both Informational and Diagnostic messages. These files may be required by our technical team in the event of a system issue.

Log Informational

Click to log all informational messages relating to the operation of Device Manager. These are displayed in the Messages panel of the Advanced tab within Central Configuration Manager. If the Save To File option is checked, the messages are logged to the default log file.

Log Diagnostic

Click to log all diagnostic messages relating to the operation of Device Manager. These are displayed in the Messages panel of the Advanced tab within Central Configuration Manager. If the Save To File option is checked, the messages are logged to the default log file.

Save To File

Click **Save to File** to log all Informational and/or Diagnostic messages to the default log file:

%Program Files%\ProgramData\Halcyon\CCMConsole\Logs\CCMConsole.hlf.

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.

Timeouts panel

This panel is used to specify maximum timeout settings between the Central Configuration Manager and the systems with which it interacts.

Connection Timeout

Specify a time (in milliseconds) in which the connection to a system must be made before the session is deemed unsuccessful. The default setting is 12000 (12 seconds).

Read Timeout

Specify a time (in milliseconds) in which the data must be read from a system before the session is deemed unsuccessful. The default setting is 12000 (12 seconds).

> IMPORTANT: Windows, AIX and Linux Agents, provided they are licensed and authorized, have a monitoring grace period of 48 hours should there be any issues connecting to the Central Configuration Manager.

Installation panel

This panel provides details of the user and password requirements needed when installing software remotely on Windows servers.

> NOTE: This feature requires the Windows ADMIN share to be enabled and the selected user must have administrative account authority on the remote system.

The panel in the **Options** menu ribbon provides the facility to view the current settings. See **Amending the current installation settings** (below) to change any of the information in this panel.

Active User

Uses the current user for log-in purposes when using the remote software installation option.

Specific User

Uses the details of a specific user whose log-in details are used when using the remote software installation option.

Show User Details Prompt on Installation

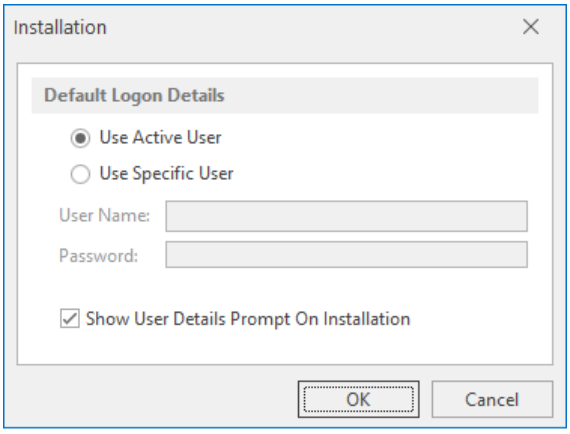
Enable this setting to have the entered User Details requested at the point of installation.

User Name

If a specific user has been identified, this field displays the name of the User.

Amending the current installation settings:

1. From the **Installation** panel, click the arrow in the bottom right-hand corner. The **Installation** dialog is displayed.



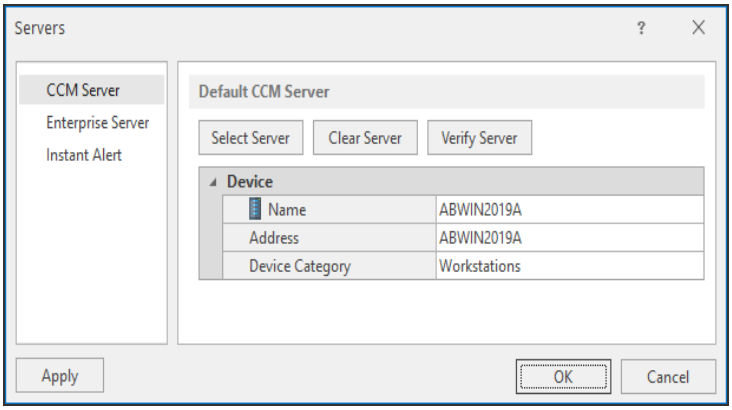
2. Change the settings as required. Note that if a **Specific User** is requested, both the **User Name** and **Password** fields must be completed.
3. Click **OK** to confirm and save the changes.

Servers panel

The **Servers** panel displays the current systems used to host the CCM, Enterprise Server and Instant Alert server software. These are usually the same system on which the installation of Network Server Suite was completed.

Amending the current server settings

1. From the **Servers** panel, click the arrow in the bottom right-hand corner.
   The **Servers** dialog is displayed.



This page is used to define the default devices that are then used for CCM, Enterprise Server and Instant Alert connections for other devices that are subsequently added to the Central Configuration Manager.

> **NOTE:** It is recommended that the default CCM server is the same device selected as the Enterprise Server. This setting can be overridden if required at both default and system level.

Servers

From the left-navigation panel of the **Servers** dialog, select the type of Server:

- CCM Server
- Enterprise Server
- Instant Alert

to which the following options are applied:

Select Server

Click **Select Server** to display the **Select Device** dialog from which the Server device can be selected. This must have been loaded via the Device Manager prior to the device being available for selection in this dialog.

Clear Server

Click **Clear Server** to clear the details of the current Server device.

Verify Server

Click **Verify Server** to verify the connection between the device on which this configuration is being undertaken and the selected Server device.

Apply

When selecting the server for CCM and Enterprise Server, the **Apply** button becomes visible.

With the CCM server selected, click **Apply** to assign the selected server to **all** devices running CCM across your enterprise. The same applies when selecting the Enterprise Server. Following the use of the Apply button, click **OK** to confirm and save the changes.

> **NOTE:** The Instant Alert Server is still selected by clicking **OK**.

Central Configuration Manager Appearance

Use the options in the Appearance tab to change the look of Central Configuration Manager.

From the Central Configuration Manager menu ribbon, click **Appearance**.

Dark Mode

Use the toggle switch to change the display mode from light (default setting) to dark.

> **IMPORTANT:** Dark Mode is saved per user and not by the application.
>
> Setting Dark Mode in any one of the UI ribbons applies it across all of the Network Server Suite applications, even those not currently loaded, which will then use the theme once opened.

Click the toggle switch again to return to the default light mode setting across all Network Server Suite applications.

Additional Central Configuration Manager Features

Synchronizing Settings

Synchronize Settings is used to ensure that system settings remain constant between use of the **Save** command.

This option is available by:

- From the **Home** menu ribbon | **Actions** panel, click **Synchronize Settings**.
- Using the keyboard shortcut Shift+Ctrl+Y.

A progress bar for each agent machine is displayed when synchronizing settings. The disk icon changes to a tick mark encased in a green circle to indicate that the settings have been successfully synchronized.

The **Synchronizing Settings** dialog remains open until **Close** is selected, unless the **Close When Complete** option is checked.

Once a change has been made to the system, such as a rule being edited, then this option is unavailable and is replaced by the Save Settings option.

Multiple Access

A pop-up window is displayed when multiple users are attempting to use Central Configuration Manager at the same time and when attempting to save settings. This to warn other users that there may be a potential conflict with the synchronizing and saving of settings.

Auto Collapse

Central Configuration Manager uses a feature called Auto Collapse (set to On as default) when viewing systems in the **System** panel.

This feature automatically closes the previous tree view so that the navigation area remains as accessible as possible, which is beneficial if there are many different systems to view and maintain.

To turn this option off and prevent the tree view from automatically collapsing:

1. From the **Home** menu ribbon | **View** panel, click Auto Collapse. The icon changes to Auto Collapse to indicate that this option is now inactive.

Manual System Tree View

If Auto Collapse is inactive, manually use the Expand Tree **Expand Tree** and Collapse Tree **Collapse Tree** options directly from the **Home** menu ribbon | **View** panel, or by selecting the system

from the **Systems** panel, right-clicking and selecting the **Expand Tree** or **Collapse Tree** option from the pop-up menu.

Holding and Releasing Systems

Holding a system prevents any of the monitors on that system from raising alerts generated by the rule criteria. It is a quick and efficient way of stopping a system from generating alerts without holding each monitor or deleting information and then having to re-instate it later.

It may be necessary to hold a system if it is temporarily unavailable due to technical issues or environmental influences.

Releasing a held system re-enables the monitoring.

To hold a system:

1. From the systems panel, right-click on the name of the system to be held.
2. From the pop-up menu, select **Hold System**. The system is now in Held status.

To release a system

1. From the systems panel, right-click on the system that is in Held Status.
2. From the pop-up menu, select **Release System**. The system is now active again.

Importing and Exporting Central Configuration Manager settings

Because the Central Configuration Manager is the hub on which Network Server Suite operates, it is wise to take a backup so that should the device on which it is running fails, settings can be easily and quickly restored to a new machine.

Likewise, if multiple installations of Central Configuration Manager are running on the network it is possible to save time by exporting and then importing settings between these installations.

> **NOTE:** Any existing settings are overwritten when Central Configuration Manager settings are imported.

Exporting Settings from Central Configuration Manager

Settings exported from Central Configuration Manager include:

- All systems
- Defined Rules
- Defined Templates
- Defined Reporting activities

The file generated is saved as an comma separated file (.csf) document with an automatically generated file name identifying the Component – Date (yyyy-mm-dd) – Time (hh:mm:ss). You can override this file name if desired.

The generated file is saved to:

%Program Files%\Halcyon\Central Configuration Manager\Console\Backup

by default, although this setting can also be overridden if required.

> **NOTE:** When importing settings, the Central Configuration Manager defaults to the backup directory as the initial location when searching for compatible files.

To export Central Configuration Manager settings:

1. From the Central Configuration Manager quick access options in the top-left corner of Central Configuration Manager, click **Export Settings**. The **Save As** dialog is displayed.
2. Select the directory path to which the Central Configuration Manager settings export file is saved.
3. Enter a file name by which to identify the export file. The default entry for this field is in the format of: 'CCMServer-YYYY-MM-DD-HHMMSS-Ms.csf.' It is recommended that this setting is retained unless internal practices require a specific entry format.
4. Retain the setting of '.csf' in the **Save as** type field and click **Save** to create the named Central Configuration Manager settings file in the specified directory.

Importing Settings into Central Configuration Manager

WARNING: By importing settings from another instance of Central Configuration Manager, you overwrite any existing data. This action cannot be undone.

To import Central Configuration Manager settings:

1. From the Central Configuration Manager quick access options in the top-left corner of Central Configuration Manager click **Import Settings**. A prompt is displayed to confirm the import action all existing systems and templates are overwritten on completion.
2. Click **Yes** to confirm the import of device settings and display the **Import Settings** dialog.
3. From within the **Look In** field, navigate to the network directory path where the Central Configuration Manager settings file (.csf) is stored. Click on the file to be imported so that it is highlighted and then click **Open** to start the import process.
4. When the import process is complete, a system message is displayed confirming the successful import of the settings. Click **OK** to close this message and display the list of imported systems in the Systems tab of the Central Configuration Manager left-hand navigation panel.

Template settings can also be exported and imported. See Exporting and Importing Templates.

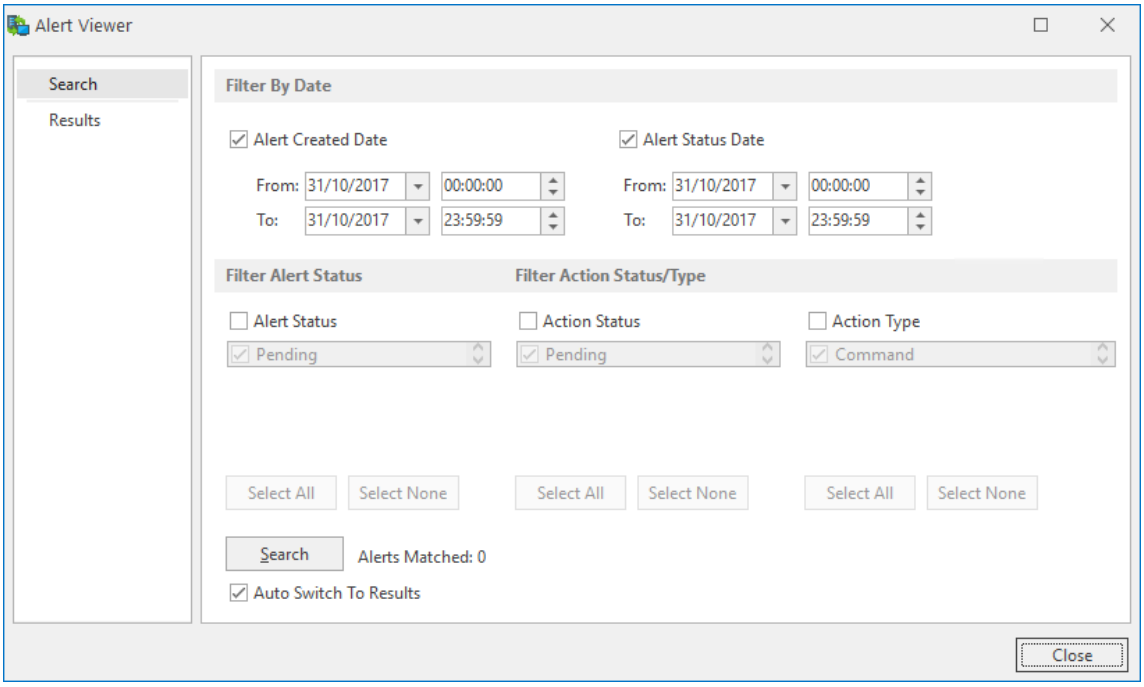
Alert Log

The Alert Log provides information on all alerts raised on a server-by-server basis for a ten-day rolling time period. This setting is not user-configurable and is only available for alerts received from Windows agents.

> **NOTE:** This option is not available for alerts received from AIX, AIX VIOS or Linux agents.

To access the Alert Log:

1. From the **Home** menu ribbon | **View** panel, click **Alert Log**. The **Alert Viewer** dialog is displayed.



The Alert Viewer is split into two pages:

- Search
- Results

Search page

The fields on this page are used to specify the criteria used to retrieve alerts from the alert log.

Filter By Date section

Alert Created Date

The **From** and **To** fields allow you to select specific date and time criteria ranges between which the search is conducted for alerts created.

Alert Status Date

The **From** and **To** fields allow you to select specific date and time criteria ranges between which the search is conducted for alerts with a changed status.

Filter Alert Status section

Choose at least one option from which alerts will be retrieved.

Alert Status

1. Click **Alert Status** to enable the search by **Alert Status**.
2. Use the up and down scroll buttons to select which Alert Status types are required for the search parameters. A tick mark indicates that the status type is selected.

   Pending
   Canceled
   Error
   Closed
3. Click **Select All** to add all Alert Status Types to the search parameters.

Filter Action Status/Type section

Action Status

1. Click **Action Status** to enable the search by **Action Status**.
2. Use the up and down scroll buttons to select which Action Status types are required for the search parameters. A tick mark indicates that the status type is selected.

   Pending
   Canceled
   Error
   Closed
3. Click **Select All** to add all Action Status Types to the search parameters.

Action Type

1. Click **Action Type** to enable the search by **Action Type**.
2. Use the up and down scroll buttons to select which Action Types are required for the search parameters. A tick mark indicates that the action type is selected.

   Control Service
   Execute Command
   Hold Rule
   Log Only (No Action)
   Release Rule
   Send Enterprise Console Alert
   Send Message
   Send Network Message
   Send SNMP Trap
3. Click **Select All** to add all Action Types to the search parameters.

Search

Click **Search** to initiate the search for alerts that meet the selected criteria within the specified date and time range.

> TIP: The number of alerts that will be found using the current search criteria is displayed next to the **Search** button.

Auto Switch to Results

Enable this setting to automatically switch to the Results page once the search has been completed.

Results page

The options on this page are used to view the details of the alerts (and any associated actions) from the alerts that retrieved from the criteria entered on the Search page.

Viewing Alert Details

Select the alert from those listed and click **Details**. The **Alert Details** dialog is displayed from where the full details of the alert can be viewed (no amendments can be made on this screen).

Viewing Action Details

Select the alert from those listed and click **Details**. The **Action** dialog is displayed from where the full details of the action can be viewed (no amendments can be made on this screen).

Refresh Alert

Click **Refresh Alert** to refresh any highlighted alerts with updated information.

Working with Monitors

Within Network Server Suite Central Configuration Manager, monitors are used to apply rules against different operating aspects of the network.

These rules keep a constant check on the essential routines and processes that your business uses and relies on during and outside of working hours. If any issues are found, according to the criteria specified in the rule, an alert is raised and various actions can be taken to notify the appropriate personnel of a potential problem.

Monitors are available for **Windows**, **AIX** and **Linux** operating systems. A Business Software Monitor is also available to monitor applications running on a website.*

*An additional license purchase is required to access this option.

In the **Systems** panel of Central Configuration Manager, monitors are shown beneath each system to which a valid license has been applied.

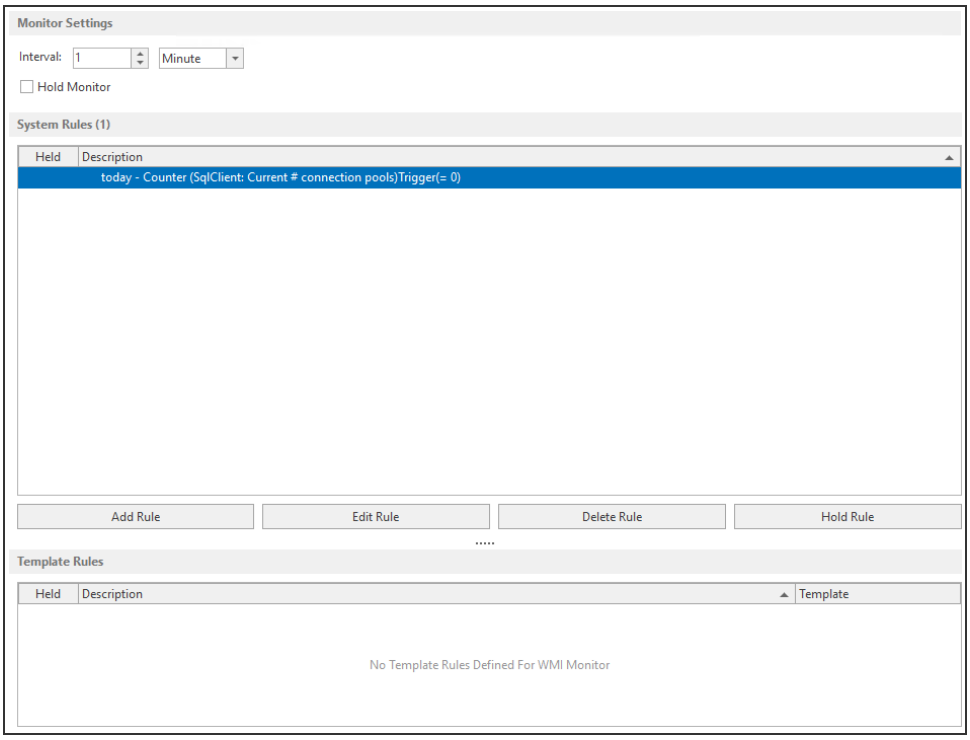
To view the available monitors for each system, ensure that the **Systems** view is selected and then expand the **Group Name**, **System Name** and **Server Manager**folders.

Once at least one rule has been created within a monitor, the description of the monitor in the **Systems** panel of the Central Configuration Manager is shown in **bold** text.

Monitor Summary Details Panel

From the **Server Manager** view of the available monitors, all monitors use the same panel layout which contains the summary detail of the applied Settings, Rules and Template Rules. With the exception of the Event Log Monitors, all fields and options within these sections are identical.

Click on any monitor from within the left-hand navigation panel to display the associated summary details.



Monitor Settings section

The fields contained within this section allow you to specify global settings for this monitor.

> WARNING: Settings applied in these fields override any settings specified at rule level.

Interval/Time Period

These settings specify how frequently the monitor runs. Unless held, all rules within this monitor are checked at this interval. The time period can be defined in seconds, minutes, hours or days.

This option is only available for the following monitors:

- **Application Event Log**: Default setting of 30 seconds
- **Security Event Log**: Default setting of 30 seconds
- **System Event Log**: Default setting of 30 seconds
- **Directory Service Event Log**: Default setting of 30 seconds
- **DNS Server Event Log**: Default setting of 30 seconds
- **File Replication Event Log**: Default setting of 30 seconds
- **CPU, Disk & Memory**: Default setting of 1 minute
- **WMI**: Default setting of 1 minute
- **Service**: Default setting of 1 minute

All other monitors set the check interval at Rule level and so this field is unavailable.

Hold Monitor

If checked (indicated by a tick mark), the monitor, and any of the rules contained within, does not run, until the monitor is released.

To hold a monitor

Either:

1. Click in the **Hold Monitor** check box in this panel.
   or
2. Right-click on the monitor from within the system list and select **Hold Monitor** from the pop-up menu.

To release a Held monitor

Either:

1. Click in the **Hold Monitor** check box to remove the tick mark.
   or
2. Right-click on the monitor in the system list and select **Release Monitor** from the pop-up menu.

Startup options (For Event Log Monitors only) section

When Windows restarts, Network Server Suite either ignores or processes any events since shutdown, depending on the selection made in these options.

Ignore events since monitor was last stopped

Any events logged since shutdown are ignored by the Event Log Monitors.

Process events since monitor was last stopped

Any event logged since shutdown are processed by the Event Log Monitors.

Rules section

Displays the **Status** and **Description** of any rules set up for the selected monitor. You can add, edit, delete and hold and release rules from within this panel.

Held

A ✅ green tick mark is displayed in the held column to indicate that the rule is held.

Description

The Rule Description is taken from the individual rule criteria. If a rule has more than one criteria defined, the Description changes to '(**Multiple Criteria Defined**)'.

Template Rules section

Displays the summary details of any template rules currently applied to this monitor.

Network Server Suite Monitors

Monitors are used in Network Server Suite to run rules against specific system elements. Different monitors are available depending on the operating system which they are monitoring (Windows, AIX and Linux). Monitors are sub-divided into groups according to the type of processes and events that they are designed to monitor.

A monitor group can contain one or more monitors.

Windows Monitors

The following monitors are available for the monitoring of devices running the Windows operating system.

Event Log Monitors Group (Standard)

This group contains the following monitors:

- Application Event Log Monitor
- Security Event Log Monitor
- System Event Log Monitor

Event Log Monitors Group (Additional)

This group contains the following monitors:

- Directory Service Event Log Monitor
- DNS Server Log Monitor
- File Replication Service Log Monitor

Performance Monitors Group

This group contains the following monitors:

- CPU, Disk and Memory Monitor
- Windows Management Instrumentation Monitor

System Monitors Group

This group contains the following monitors:

- File & Folder Monitor
- Log File Monitor
- Services Monitor

TCP Monitors Group

This group contains the following monitors:

- TCP FTP Monitor
- TCP HTTP Monitor
- TCP NNTP Monitor
- TCP Ping Monitor
- TCP POP3 Monitor
- TCP SMTP Monitor
- TCP Telnet Monitor
- TCP/UDP Generic Monitor

AIX Monitors

The following monitors are available for the monitoring of devices running the AIX operating system.

- AIX Error Report Monitor
- Subsystem Monitor
- Logical Volume Monitor
- Script Monitor
- File & Folder Monitor
- Log File Monitor
- CPU, Filesystem & Memory Monitor
- System Monitor
- Process Monitor
- Ping Monitor

Linux Monitors

The following monitors are available for the monitoring of devices running the Linux operating system.

- Linux Logical Volume Monitor
- Script Monitor
- File & Folder Monitor
- Log File Monitor

- CPU, Filesystem & Memory Monitor
- System Monitor
- Process Monitor
- Ping Monitor

Business Application Monitors

These monitors are not included in the standard release of Network Server Suite but are fully compatible with the software. These monitors can be purchased for an additional license fee.

> **NOTE:** If you have not purchased an additional license, the Business Software Monitors are not displayed in the Systems view of Central Configuration Manager.

- Web Application Monitor

> **NOTE:** Separate documentation is available for the Web Application Monitor.

Windows Event Log Monitors

Event Log Monitors are used to monitor the standard Windows Application, Security and System event logs. New events which are sent to the logs can be monitored and alerts raised accordingly. Most standard ‘server’ based products such as Exchange and SQL post events into the standard logs. In some instances, you may want to monitor if an event has not been received during a specified time.

You can also use Event Log Monitors to monitor the contents of any text-based log file (including fixed-format and delimited) for any new entries, raising alerts accordingly.

Standard Event Log Monitors

The standard Event Log (Application, Security and System) Monitors provide two key features:

- Monitoring of standard Windows event logs
- New events in the log can be filtered and alerts raised accordingly. Most standard ‘server’ type products (such as Exchange and SQL) post events into the standard logs.

Additional Event Log Monitors

There are also three additional Event Log Monitors:

Directory Service Event Log Monitor

This can be used, for example, to log connection problems between the server and the global catalog.

DNS Server Event Log Monitor

Events associated with resolving DNS names to Internet Protocol (IP) addresses are recorded in this log.

File Replication Event Log Monitor

File replication failures and events that occur while domain controllers are being updated with information about System Volume (Sysvol) changes are recorded in the file replication log. Sysvol is a shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain.

Event Log Monitors - Examples of Use

The following are all examples of where an Event Log Monitor can be used to determine successful (or unsuccessful) occurrence of system events:

- Failed backups
- SMTP protocol errors
- Specific event sources, categories, event IDs, event user or text
- Service status monitoring
- Security violations

Creating an Event Log Monitor Rule

The following section provides instructions on how to create an typical Event Log Monitor Rule. The general instructions apply to all the monitors that run within the Event Log group.

Event Log Monitor Rules specific criteria fields

When adding rule criteria the following pages and fields are specific are specific to Event Log Monitors.

Criteria Page

Event Log Parameters section

Fields in this section define the characteristics of the event as found in the Event Log.

> WARNING: Keeping the default settings in these fields greatly increase the chance of the rule criteria triggering as they are set to 'catch-all' events.

Criteria Type

Use the radio buttons to select whether matching events are included or excluded from the rule criteria. Exclusions can be used to filter out commonly occurring events.

Event Type

Select the type of event for which this rule applies. The following event types can be selected and multiple selections are allowed. At least one event type must be selected.

- **Error**: All error log messages are selected.
- **Information**: All information log messages are selected.
- **Warning**: All warning log messages are selected.
- **Audit Failure**: All audit failure log messages are selected.
- **Audit Success**: All audit success log messages are selected.

Event Source

Enter a specific source to identify the origin of the event log message. Use the **Comparison** field to determine whether the origin should be equal to or different from the entry in the **Value** field.

Event Category

Enter a specific category to determine the group in which the event log message originated. Use the **Comparison** field to determine whether the origin should be equal to or different from the entry in the **Value** field.

Event ID

Enter a unique Event ID that is used to select the event log message. Use the **Comparison** field to determine whether the origin should be equal to, greater than, greater than or equal to, less than, less than or equal to or different from the entry in the **Value** field.

Event User

Enter the name of a user that is used to select an event log message that was created as a result of this user's activity. Use the **Comparison** field to determine whether the origin should be equal to or different from the entry in the **Value** field.

Event Message

Enter the specific event log message required. Use the **Comparison** field to determine whether the origin should be equal to or different from the entry in the **Value** field.

TIP: Use wildcards * and ? to specify extended criteria. For example, entering An* in the Event User field would find users; Andrew, Andrea, Andy, Andre, and so on.

NOTE: Comparison values are not case sensitive.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

Wildcard Characters section

Fields in this section determine alternative characters that can be used for multiple or single character substitution.

Use * As A Substitute For Zero Or More Characters

Specify a character, other than '*' that will be used as a wildcard substitution for none or multiple characters in this rule.

Use ? As A Substitute For A Single Character

Specify a character, other than '?', that will be used as a wildcard substitution of a single character in this rule.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** period if the criteria is still not triggering.

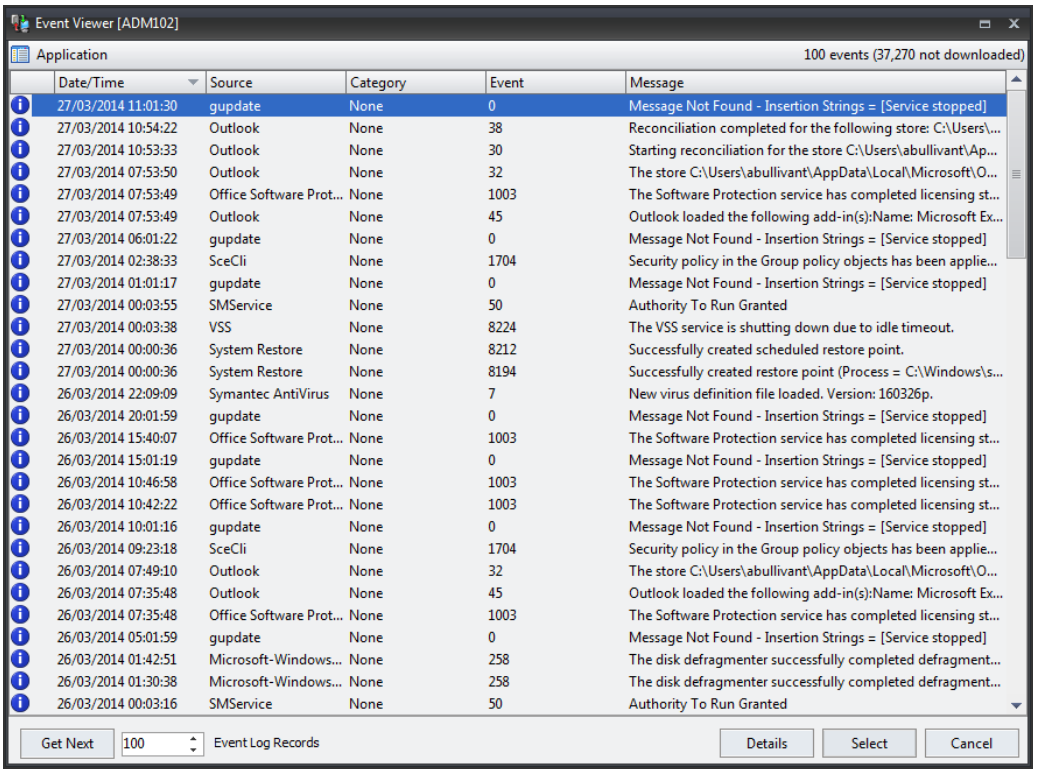
> **EXAMPLE:**
> • A CPU rule has criteria to alert if the CPU % Processor Time is above 75%.
> • It also has Auto-Close specified to Auto-Close Enterprise Console Alerts with a Delay period of 5 minutes.
>
> The rule criteria is checked and triggers as the CPU is above 75%. An alert is sent to the Enterprise 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Using the Browse utility

From the **Add Criteria** dialog, used when adding criteria for Event Log Monitor rules, a **Browse** facility provides both summary and detail information about existing entries in each of the three log types.



Get Next

By default, the 100 most recent entries are displayed. Click **Get Next** to retrieve the specified number of Event Log Records. This figure can be increased or decreased as required by either over-typing the existing entry or using the up and down arrows to amend the figure.

Details

Click **Details** to display the Event Properties dialog showing detailed information for the event log. From this dialog, move through further logs in the summary display by using the up and down arrows. After finishing viewing the detail information, click **OK** to return to the main Event Log Viewer display.

Select

Single-click on an event log on this display and then click **Select** to automatically populate the rule criteria fields with the detailed log information from the selected event log.

Example Application Event Log Monitor rule

This example rule checks that any events sent to the Windows Application Event Log do not contain the words: **Backup failed**.

This is useful if there is a device on which regular backups are performed as this rule can ensure that these are completing successfully. If the rule is triggered, an alert is sent to the Enterprise Console (although any action can be specified to suit a particular requirement).

1. From the **Systems** panel of the Central Configuration Manager, select the **system** to which the monitor rule is to be applied and expand the **Server Manager** > **Event Log Monitors (Standard)** view so that the monitors are displayed.
2. Select the **Application Event Log Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of **'Check for Backup Failures**'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.
5. In **Event Type Settings** clear the **Information**, **Warning**, **Audit Failure** and **Audit Success** settings.
6. Leave all comparison values as '**=**'. In the **Event Source Value** field, enter the name of the system. This name is used in the alert message.
7. Enter **'None**' as the **Event Category Value**.
8. Enter '**9999**' as the **Event ID Value**.
9. Enter '**System**' as the **Event User Value**.
10. Using wild cards to capture any instance of backup failure, enter '***Backup Failed***' as the **Event Message Value** and click **OK**.
11. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
12. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
13. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the System Rule panel for the Application Event Log Monitor.
14. From the **Central Configuration Manager** menu ribbon, click **Save**. The rule is now active within the monitor.

Windows Performance Monitors

These monitors allow you to check generic performance counters. Performance Monitors can report on installed applications, for example, if Microsoft Exchange Server is installed and diagnostics logging configured within Exchange, Network Server Suite can monitor and alert you as required. The Performance Monitors comprise of:

CPU, Disk & Memory Monitor

Gives administrators the ability to monitor the CPU, Disk and Memory statistical data. The disk option allows all drives recognized by Windows to be monitored in a single rule.

The CPU, Disk and Memory monitor is used to check common attributes of system performance.

Common examples of CPU, Disk and Memory Monitors

- **CPU Load** (%Processor Time, %Privilege Time, %User Time).
- **Disk Space** (%Available, %Used). All drives can be included in one rule.
- **Memory** (Page File Used/Available %, Physical Memory Used/Available %).

WMI (Windows Management Instrumentation) Monitor

Gives administrators the ability to select the performance indicators required to monitor and set up actions dependent upon user-defined thresholds.

WMI is a set of specifications from Microsoft for consolidating the management of devices and devices and applications in a network from Windows computing systems. WMI is installed on all computers with Windows ME or Server 2003 upwards installed. WMI provides users with information about the status of local or remote computer systems.

WMI also supports such actions as the configuration of security settings, setting and changing system properties, setting and changing permissions for authorized users and user groups, assigning and changing drive labels, scheduling processes to run at specific times, backing up the object repository and enabling or disabling error logging.

Alerts are raised if the specified instance exists, does not exist or if the criteria triggers at a pre-determined value. When applicable, for example, selecting Processes as a Non-Performance category, it is possible to use a generic value using wildcard '*' in the **Instance** parameter to raise an alert for all matching values.

> **NOTE:** When setting WMI rule criteria, if a Specified Instance is not identified, a wildcard query must be entered in order to be able to proceed.

WMI Reporting

The WMI Monitor is capable of generating reports based on seven pre-defined and 25 user-defined criteria.

See Reporting for more information on this functionality.

Creating CPU, Disk & Memory Rules

The following section provides instructions on how to create an typical CPU, Disk and Memory Rule.

CPU, Disk & Memory Monitor specific criteria fields

When adding criteria the following pages and fields are specific are specific to the CPU, Disk & Memory Monitor.

Criteria page

Performance Parameters section

The fields in this section determine the type and trigger value of the selected area of system performance.

Performance Group

From the drop-down menu select the area of performance for which the rule is created. Select from:

- CPU
- Disk
- Memory

> **NOTE:** Further fields on this page are dependent on the selection made in this field.

Instance (For Performance and Memory Performance Groups)

Select the instance on which this rule measures performance. Select **_Total** to measure performance across the total of all listed instances.

Drive (For Disk Performance Groups)

Select the Drive on which this rule measures performance. Select All Drives (*) to measure performance across all drives.

Performance Type

For CPU Performance, the following choices are available:

- **% Privileged Time**: % Privileged Time counter shows the percent of time that the processor is spent executing in Kernel mode. Most of the time a processor should be executing User mode operations, so a high % privileged time might indicate a poorly written device driver or a faulty piece of hardware.
- **% Processor Time**: % Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the percentage of time that the processor spends executing the idle thread and then subtracting that value from 100%.
- **% User Time**: % User Time is the percentage of elapsed time the processor spends in the user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems.

For Disk Performance, the following choices are available:

- **Disk Space Available %**: Measures the percentage of Disk Space Available on the selected drive.
- **Disk Space Used %**: Measures the percentage of Disk Space Used on the selected drive.

For Memory Performance, the following choices are available:

- **Page File Available %**: A pagefile is a reserved portion of a hard disk that is used as an extension of random access memory (RAM) for data in RAM that hasn't been used recently. This indicator measures the amount of pagefile memory still available for use and expresses it a percentage value.
- **Page File Used %**: This indicator measures the amount of pagefile memory used and expresses it a percentage value.
- **Physical Memory Available %**: Physical memory is the amount of RAM you have installed in the system. This indicator measures the amount of physical memory left available for use and express it as a percentage value.
- **Physical Memory Used %**: This indicator measures the amount of physical memory that has been used and express it as a percentage value.

Trigger Value

The trigger value is used to specify a percentage value threshold at which the Performance criteria is set. The following comparators can be used:

- **=** The trigger value is exactly equal to the percentage value entered.
- **>** The trigger value is greater than the percentage value entered.
- **>=** The trigger value is greater than or equal to the percentage value entered.
- **<** The trigger value is less then the percentage value entered.
- **<=** The trigger value is less than or equal to the percentage value entered.
- **<>** The trigger value is anything other than the percentage value entered.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click ? to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

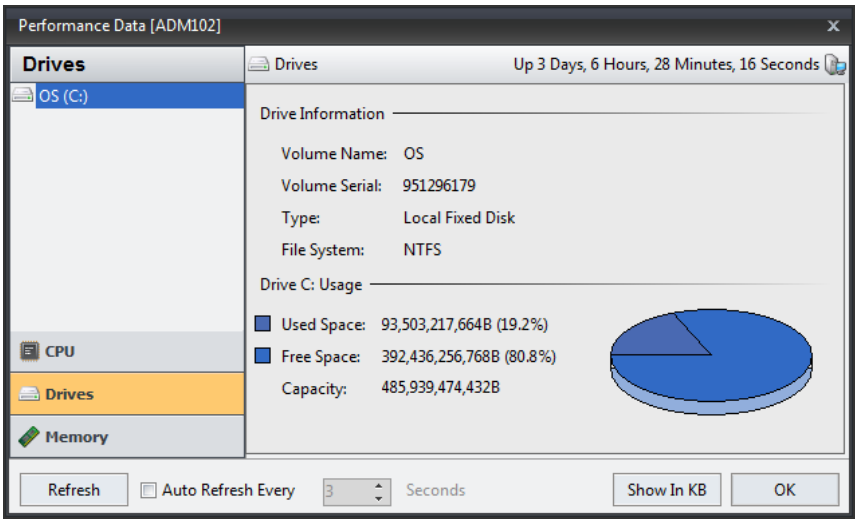
The rule criteria continues to be checked and if the CPU does not cause any further triggers, the existing alert is closed at the tagged auto-close time.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Using the Performance Data utility

Prior to setting any criteria for this monitor, it is advisable to use the **Performance Data** button, on the **Performance Criteria** dialog to display the current Performance Data for the chosen system.



Use the tabs in the left-hand navigation panel of this display to view the relevant performance data of each attribute of the selected system.

Refresh

Use **Refresh** to periodically update the display or set the **Auto Refresh** setting to automatically update the display every specified number of seconds.

Show in MB/KB

Data can be displayed in KB or MB. Click **Show in MB/KB** to toggle the display between size metrics.

When you have the required information, click **OK** to close the **Performance Data** dialog.

Creating an example CPU, Disk and Memory Rule

This example rule checks that the disk space available on the 'C:\' drive of a given system remains above 25%. If the rule is triggered, an alert is sent to the Enterprise Console (although you can specify any action that suits your circumstances).

1. From the **Systems** panel of the Central Configuration Manager, select the **system** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **CPU, Disk & Memory Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of '**C Drive Disk Space Available >25%**'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.
5. Choose the **Device** to which this rule applies and click **Select**.
6. From the **Performance Group** choice menu, select **Disk**. The entry in the **Drive** field automatically defaults to the 'C:\' Drive.
7. From the **Performance Type** choice menu, select **Drive Space Available %**.
8. Set the Trigger Value to **> 25%** and click **OK**.
9. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
10. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
11. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the CPU, Disk & Memory Monitor.
12. From the Central Configuration Manager menu ribbon, click  **Save**. The rule is now active within the monitor.

Creating WMI Rules

The following section provides instructions on how to create an typical Windows Management Instrumentation (WMI) Rule.

WMI Monitor specific criteria fields

When adding criteria the following pages and fields are specific are specific to the WMI Monitor.

Criteria page

Category section

Use the radio buttons in this section are used to determine whether the rule measures Performance or Non-Performance of a specific system property.

Performance

Click the **Performance** radio button and select a system property on which performance is measured from the drop-down menu.

Non-Performance

Click the **Non-Performance** radio button and select a system property on which non-performance is measured from the drop-down menu.

Instance section

The fields in this section determine when actions are performed, when the alert is generated and the instance which causes the criteria to trigger.

Perform Actions For

This is used to determine how alerts are raised when the selected instance causes a trigger. Certain options may be limited in this section dependent on the system property selected in the Category section.

- **Specified Instance**: Actions are only performed when the specified instance triggers.

- **First Triggered Instance**: Actions are performed on the first triggered instance. The alert raised contains a summary of the instances that breached the criteria threshold.
- **All triggered instances**: Actions are performed on all triggered instances. An alert is raised for each instance containing only details of that particular instance that breached the criteria threshold.

Alert If

If available, this field determines when the alert is raised.

- **Instance Exists**: An alert is raised if the named instance is found to exist.
- **Instance Does Not Exist**: An alert is raised if the named instance is found not to exist.
- **Criteria Triggers**: An alert is raised if the specified criteria trigger this instance.
- **Instance Count**: An alert is raised if a specific count of the instance is reached.

Instance

Use the drop-down menu to select the instance to which the rule applies. The selections in the menu are dependent on the choice made in the **Category** section.

Criteria section

This section is used to specify the criteria for the instance that if triggered, cause an alert to be generated.

Counter

Use the drop-down menu to select the counter method to which the rule applies. The selections in the menu are dependent on the choice made in the **Category** section.

Trigger Value

Use the Trigger Value fields to specify a comparator and value, which if breached, cause an alert to be generated.

Timestamp Trigger Value section

This section, if available based on selections made elsewhere on this dialog, allows the criteria to be specified as a Date or Age Timestamp on which an alert is generated if the criteria is met.

Date

Select the **Date** radio button to specify a **Date** and **Time** that the remaining criteria on this display must equal (or not equal) in order for an alert to be generated.

Age

Select the **Age** radio button to specify a time period that the remaining criteria on this display must equal (or not equal) in order for an alert to be generated.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Wildcard Characters section

Fields in this section determine alternative characters that can be used for multiple or single character substitution.

Use * As A Substitute For Zero Or More Characters

Specify a character, other than '*' that will be used as a wildcard substitution for none or multiple characters in this rule.

Use ? As A Substitute For A Single Character

Specify a character, other than '?', that will be used as a wildcard substitution of a single character in this rule.

Error If Instance Not Found

Click this option to raise an error if wildcards have been used to specify an instance and the instance is subsequently not found.

Ignore Instances section

Use this section to add, edit or delete any specific instances to be ignored by this rule.

Add

Click **Add** to add instances to be ignored by this rule. In the **Add Item** dialog enter the name of the **Instance** that you wish to be ignored if encountered. Click **OK**

Edit

Click **Edit** to amend a selected instance in this section.

Delete

Click **Delete** to remove a selected instance in this section.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

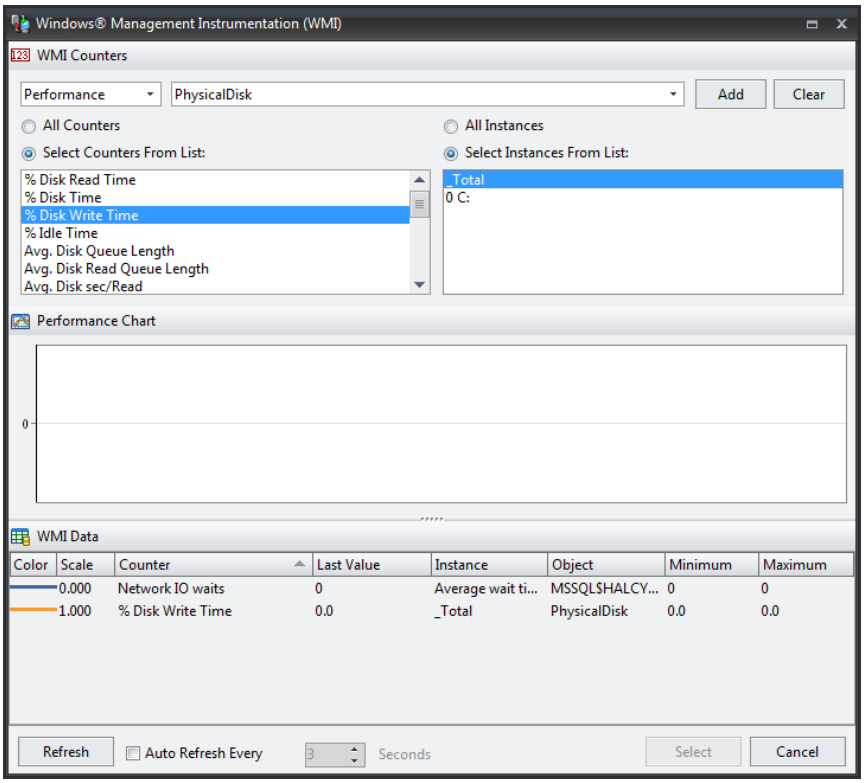
The rule criteria continues to be checked and if the CPU does not cause any further triggers, the existing alert is closed at the tagged auto-close time.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Using the WMI Browse Utility

When adding criteria for WMI monitor rules, a **Browse** facility lets you view both performance and non-performance information about various Windows system properties.



To browse for WMI data:

1. From the drop-down choice menus, select whether you wish to monitor for performance on non performance and then select the system property that you wish to monitor against.
2. Select specific counters and, if available, instances to drill-down into extra detail of the system property or select all counters and instances.
3. Click **Add** to display the WMI data for your selection in the bottom panel of this dialog together with a performance chart, showing the current data for your selection in real-time.
4. Click **Clear** to remove the current selection from the dialog ready for a new selection to be made.
5. Use **Refresh** to manually update the display or set the auto-refresh settings to automatically update the data.
6. When you are ready to make your selection, highlight the required detail line in the WMI Data panel of this dialog and click **Select**. The criteria is automatically added to the rule.
7. Click **Test** on the WMI Criteria dialog to check your criteria against either the local or a remote system.

Example WMI Monitor rule

This example rule checks that the number of inactive terminal service sessions is not equal to or greater than five. An alert is generated if the number of inactive terminal service sessions matches or exceeds this threshold.

1. From the **Systems** panel of the Central Configuration Manager, select the **system** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **WMI Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of '**Inactive Terminal Service Sessions >5**'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.
5. Click **Browse** to open the **Windows Management Instrumentation** dialog.
6. Using **Performance** as the mode, select **Terminal Services** from the parameters choice menu.
7. Ensure **Select Counters From List** is enabled and select **Inactive Sessions**. Click **Add**.
8. From the **WMI Data** panel, highlight the current line entry and click **Select**. The data is now transferred into the **WMI Criteria** dialog.
9. Change the **Trigger Value** from '**=**' to '**>=**' and change the associated value to **5**. Click **OK**.
10. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
11. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
12. On the Add Rule Detail dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the WMI monitor.
13. From the Central Configuration Manager menu ribbon, click  **Save**. The rule is now active within the monitor.

Windows System Monitors

These monitors allow the monitoring of system status. Advanced logical monitoring can be used within File & Folder Monitor to alert when specific actions external to Network Server Suite **do not** write to the application logs (have or have not taken place).

These monitors comprise:

File & Folder Monitor

Checks for changes in selected folders and/or files. For example, when a new file is created in a folder or when the size of a file changes. This is useful for tracking the creation of files sent via FTP and also ensuring that critical files are not deleted. In addition it can be used to check the date and time stamps of virus .dat files.

Example uses of the File & Folder Monitor

- Anti-virus definition downloads
- Existence based on date, time, size, etc.
- Search for wildcard files and folders

Log File Monitor

Monitors any Windows log file on any local or networked drive. New events appearing in the log can be filtered and alerts raised accordingly. Rule Criteria can include or exclude text or can use Regular Expressions to filter information. Regular Expressions allow the selection of specific strings from a set of character strings.

> **NOTE:** The Log File Monitor does not currently support files generated in Unicode.

Example uses of the Log File Monitor

- Application specific log files

Services Monitor

The status of services running on a server can already be monitored from the Windows Event Logs. However, this only informs the user if the service starts and stops correctly.

The Service Monitor periodically checks the status of selected services and trigger actions when an incorrect status is found. The actions include the ability to start, stop, pause and resume a service.

Additionally, it is possible to specify Services that should be excluded from the check. The 'Excluded Services' parameter is shown at the bottom of the Criteria dialog and supports wildcards. This can be used to prevent a generic service monitor from creating an alert for services that auto start but then stop immediately.

> **NOTE:** Code in the Services Monitor checks the version of Windows that is running. For Windows 8 and Server 2012, service status is shown as 'Running'. For all other Windows versions, the service status is shown as 'Started'.

Example uses of the Service Monitor

- Check if (Windows) services are running
- Check startup type
- Check logon account details

Creating File & Folder Monitor Rules

The File and Folder Monitor rules allow you to browse both local and remote devices for a specific folder and check for any changes.

File & Folder Monitor specific criteria fields

When adding criteria the following pages and fields are specific are specific to the File & Folder Monitor.

Criteria page

Location section

The fields in this section are used to define the location of the File/Folder in the network.

Search Path

Enter the full **Search Path** for the File/Folder location. Click [...] to open the **Browse For Folder** dialog. This allows you to select any folder from the devices listed in the Device Manager and drill down to select subsequent folders as you would in the usual Windows operating environment.

TIP: The **Browse for Folder** option also allows you to specify a 'symbolic link' folder such as OneDrive.

Use Results From Previous Criteria

This option can be used to perform actions on the results generated by the previous criteria in this monitor. When this option is enabled, the **Search Path** field changes to **Variable**. Enter the variable '**&EN**' to represent the **Matched Name** of the previous criteria.

This option is useful for scenarios such as ensuring that a series of files have been received by FTP correctly. On receipt of the final file, an action can be taken to copy all files to another folder.

Search Parameters section

Alert If

Specifies the option used to determine the method by which the alert is first triggered.

- **File/Folder Exists**: Alert is raised if the specified file or folder exists.
- **File/Folder Does Not Exist**: Alert is raised if the specified or folder does not exist.
- **File Count**: Alert is raised if the file count matches the comparator and value in the subsequent parameters that become enabled as a result of selecting this option.

Trigger On

Trigger actions are used to determine at which point the alert is raised. This option is unavailable if File Count is specified in the 'Alert If' parameter.

- **First Matching**: The alert is triggered on the first matching instance found.
- **Each Matching**: Separate alerts are triggered for each matching instance found.
- **All**: A single alert is triggered with the information of up to 50 matching instances found.

Scan Filters section

The fields in this section are used to filter file and/or folders from the results.

Scan Filter parameters

Scan filters can be set to Ignore files/folders of specific types, and/or Include or Exclude specific rule criteria on which to search. Filters can be applied to files/folders that fall into one or more of the following categories:

- **Read Only**
- **System**
- **Temporary**
- **Hidden**
- **Archive**
- **Compressed**

Alert Page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Thresholds

When adding rule criteria for the File and Folder Monitor, size and time-stamp threshold information can be applied to further refine the criteria requirements.

Size Threshold section

These fields are used to define the size threshold of any file and/or folders.

Size

Click **Size** to enable the Size threshold fields.

Comparator

Select the type of comparator to be used in the calculation of the size threshold. Select from:

- **Equal to**
- **Greater than**
- **Greater than or equal to**
- **Less than**
- **Less than or equal to**
- **Not equal to**

Value

Either enter the value directly into this field or use the up/down arrows to adjust the current value,

Measure

Select the unit of measure by which the size threshold is set.

- **Bytes**
- **Kilobytes**
- **Megabytes**
- **Gigabytes**
- **Terabytes**

- **Petabytes**
- **Exabytes**

Timestamp Thresholds section

This section contains three variations of timestamp thresholds that can be used to filter file and folder criteria. These three options use the same selection criteria to determine the result.

Created

Click **Created** to be able to specify either a general time period or a specific date and time at which the file/folder was created.

Modified

Click **Modified** to be able to specify either a general time period or a specific date and time at which the file/folder was modified.

Accessed

Click **Accessed** to be able to specify either a general time period or a specific date and time at which the file/folder was accessed.

Test

Once the required criteria have been entered, use the **Test** button to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'. See Local v Remote Testing for more information on conducted this test on local and remote systems.

Creating an example File/Folder Monitor rule

This File/Folder Monitor rule checks that the critical system.ini file has not been deleted.

1. From the **Systems** panel of Central Configuration Manager, select the **system** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **File & Folder Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of '**Check for System.ini file**'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.

5. Enter the **Search Path** of where the system.ini file is resident. (This is usually C:\Windows).
6. Change the **Alert If** parameter to '**File/Folder Does Not Exist**'.
7. In the **Scan Filters** section override the **Include Filter** option of '*.*' with '**system.ini**'.
8. Click **Test** (ensure that this is carried out of the local system) to determine that the file currently exists (the criteria does not trigger). Close the **Test** dialog and click **OK** to add the criteria detail.
9. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
10. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
11. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the File/Folder Monitor.
12. From the Central Configuration Manager menu ribbon, click **Save**. The rule is now active within the monitor.

Creating Log File Monitor Rules

The Log File Monitor checks log files for any character string or text within any standard Windows log or text file, whether stored locally or on a network drive.

Log File Monitors can raise alerts for each new line of text that is added to the file that matches either the include/exclude filter or Regular Expression criteria.

> **NOTE:** The default setting is 'Include "*".' If left as this setting once the rule is created, a new alert is generated for each new line added to the selected log file.

Log File Monitor Rule specific criteria fields

When adding rule criteria the following pages and fields are specific are specific to the Log File Monitor.

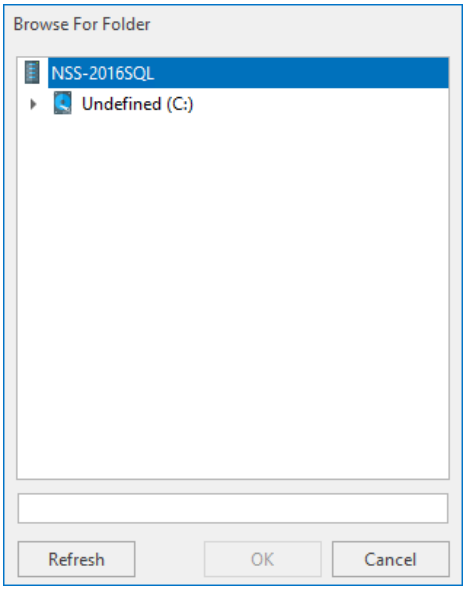
Criteria page

Location section

The field in this section is used to select the Log File to be monitored for the rule.

Log File

Either type the directory path and log file name (wildcards '*****' and '**?**' are accepted) directly into the **Log File** field, or click ... to open the **Browse for Folder** dialog.



Navigate to the required directory path. Once the folder containing the log files to be monitored has been located, click **OK**. The path is entered in the **Log File** field.

> **NOTE:** When entering or selecting a path, any file extensions that have been entered in the Excluded file extensions parameter within the Advanced Tab are omitted from the search.

Log File Filters section

The fields in the section allow the inclusion or exclusion of particular files. Use **Browse** for a fast way to populate these fields. Alternatively, simply type the required text/character string into the relevant filter setting. Wildcards '*' and '?' can be used to construct the required string.

Press Enter to add multiple lines of text to the rule. When entering multiple lines of text, be aware that an alert is raised if **any** of the text is found/not found in the selected log files.

Include Filter

Specifies the text or character sting to include. By default, the wildcard '*' is used to indicate that all text in the log file is included. Position the cursor in this field and use the **Browse** > **Select** function to include a specific line of text. See Browse for more information.

Exclude Filter

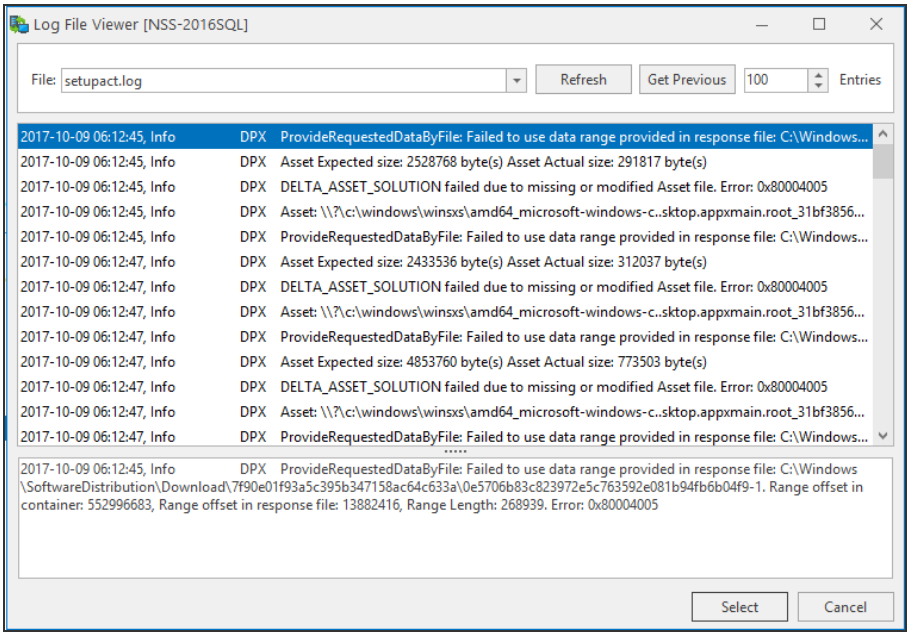
Specifies the text or character sting to exclude. By default, this field is blank to indicate that nothing in the log file is excluded. Position the cursor in this field and use the **Browse** > **Select** function to exclude a specific line of text. See Browse for more information.

Regular Expressions

A regular expression (regex or regexp for short) is a special text string for describing a search pattern that can be used to pinpoint a specific item of information within a log file. The search can be as generic or specific as required. Position the cursor in this field and use the **Browse** > **Select** function to create a regular expression from a specific line of text. See Browse for more information.

Browse

Click **Browse** to view the most recent entries in the selected log file using the Log File Viewer.



File

Displays the name of the selected Log File. If a directory path was specified, use the arrow to open a drop-down menu displaying other log files within the directory that can be selected. If another log file is selected, the contents of the main display change accordingly.

Refresh

Click **Refresh** to update the display with any log file entries created since the log file was opened in the Viewer.

Get Previous

By default, the last 100 entries in the log file are displayed. Use **Get Previous** and set a **Value** to retrieve any entries that were created prior to the last 100 entries.

Select

Click **Select** to select the entry that is currently highlighted in the main display panel as a string to **Include**, **Exclude** or set as a **Regular Expression** dependent in which field the cursor was positioned on the criteria page.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

Advanced Settings section

Advanced settings within the Log File Monitor allow the exclusion of files with specific extensions and specify whether any entries that have been generated since the monitor was last stopped, are ignored or processed.

Excluded file extensions

Use this field to enter the extension of any files that you wish the Log File Monitor to ignore when browsing or searching for files. File extensions that are included by default are:

- .exe
- .dll
- .bin
- .res
- .ico
- .wmv
- .avi
- .xvid
- .identcache

Add

Click **Add** to open the Add Item dialog where additional file extensions can be added to the exclusion list.

Edit

Highlight an existing selection and click **Edit** to change the extension name.

Delete

Highlight an existing selection and click **Delete** and confirm the action to remove the selection from the exclusion list.

Require A Terminating Line Feed Character

This option specifies that log file entries must include a terminating line feed character in order to be recognized. This is on by default. If this setting is not active, a text string may exist at the end of an entry even though a terminating line feed character has not be used in the log file.

Startup section

The fields in this section determine whether the monitor processes or ignores all entries generated since the monitor was last stopped.

Ignore Log Entries Since Monitor Was Last Stopped

Select this option to specify that any log entries in the selected file which have been created since the Log File Monitor was last stopped are ignored.

Process Log Entries Since Monitor Was Last Stopped

Select this option to specify that any log entries in the selected file which have been created since the Log File Monitor was last stopped are processed.

Error if Folder Path Not found

An alert can be raised if the entered search path is not found when the rule is run. Select this option so that if the Search Path does not exist an alert is sent to the Enterprise Console. If this option is not checked, any search path errors are ignored.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating an example Log File Monitor Rule

The following rule checks the Enterprise Console Log named Console.hlf and sends a text alert if text is found in the log file that indicates that no response has been received from the server for 1 minute.

1. From the **Systems** panel of the Central Configuration Manager, select the **system** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **Log File Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of '**Check Enterprise Console Log For Error**'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**. The **Log File Criteria** dialog is displayed.
5. Click ... next to the **Log File** field. From the **Browse for Folder** dialog, navigate to the following path:
   C:\Program Data\Halcyon\Enterprise Console\Logs\Console.hlf

   (this assumes that you followed a typical installation ofNetwork Server Suite). Click **OK**.
6. Returning to the **Log File Criteria dialog**, ensure that the cursor is positioned in the **Include Filter** field and remove the existing entry of '*'.
7. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
8. Select the **Send Instant Alert Message** action. Click **OK** to open the **Message Action** dialog.

9. Ensure that the intended recipient is listed in the **Recipients** field and that **SMS** is selected as the Message Type (assumes Recipients exist in Instant Alert Address Book and that they have a mobile number configured). Click **OK** to confirm the action.
10. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the Log File Monitor.
11. From the Central Configuration Manager menu ribbon, click **Save**. The rule is now active within the monitor.

Creating Service Monitor Rules

The Service Monitor ensures that critical services, such as Anti-Virus software, are running on the selected device.

A useful feature of this is that it automatically allows control of the service dependent on the result of the alert. For example, if the monitor detects that the Anti-Virus software has stopped running, the monitor can automatically restart the service without the need for any interaction.

Service Monitor also allows Services that should be excluded from the check criteria to be specified. The 'Excluded Services' parameter is shown at the bottom of the Criteria dialog and supports wildcards. Any services entered into this parameter are omitted from the rule criteria. This can be used to prevent a generic service monitor from creating an alert for services that auto start but then stop immediately.

When setting the Control Service action for a service monitor, it is possible to use the service from the criteria (i.e. if a service has stopped, this is the service required to start) or use another of the listed services to perform the required action.

> **NOTE:** Code in the Services Monitor checks the version of Windows that is running. For Windows 8 and Server 2012 upwards, service status is shown as 'Running'. For all other Windows versions, the service status is shown as 'Started'.

Service Monitor Rule specific criteria fields

When adding rule criteria the following pages and fields are specific are specific to the Service Monitor.

Criteria page

Service Selection section

The fields in this section are used to specify the service to be controlled by this rule.

Display Name

Use the drop down menu to select the service to be controlled by this rule. Any generic service can be started (or stopped) by over-typing the service from within the **Display Name** field and using '*' as a wildcard. For example, typing 'HAL*' would perform the specified action on any service beginning with the characters HAL.

Service Parameters section

The fields in this section determine the control parameters of the service.

Status

Use the comparator of equal (or not equal) with the required status type which can be selected from the drop-down menu to determine the service to be selected (or omitted). The possible options are:

- Any Status
- Stopped
- Start Pending
- Stop Pending
- Renaming
- Continue Pending
- Pause Pending
- Paused

Startup

Use the comparator of equal (or not equal) with the required startup option which can be selected from the drop-down menu to determine the service to be selected (or omitted). The possible options are:

- Any Startup Type
- Automatic
- Automatic (Delayed Start)
- Boot
- Manual
- System
- Disabled

Logon Account

Use the comparator of equal (or not equal) with the required Logon Account which can be selected from the drop-down menu to determine the service to be selected (or omitted). The possible options are:

- Any Logon Account
- Local System
- Local Service
- Network Service

Excluded Services

Use this field to determine any services to be excluded from this rule.

Add

Click **Add** to open the Add Item dialog where services can be added to the exclusion list.

Edit

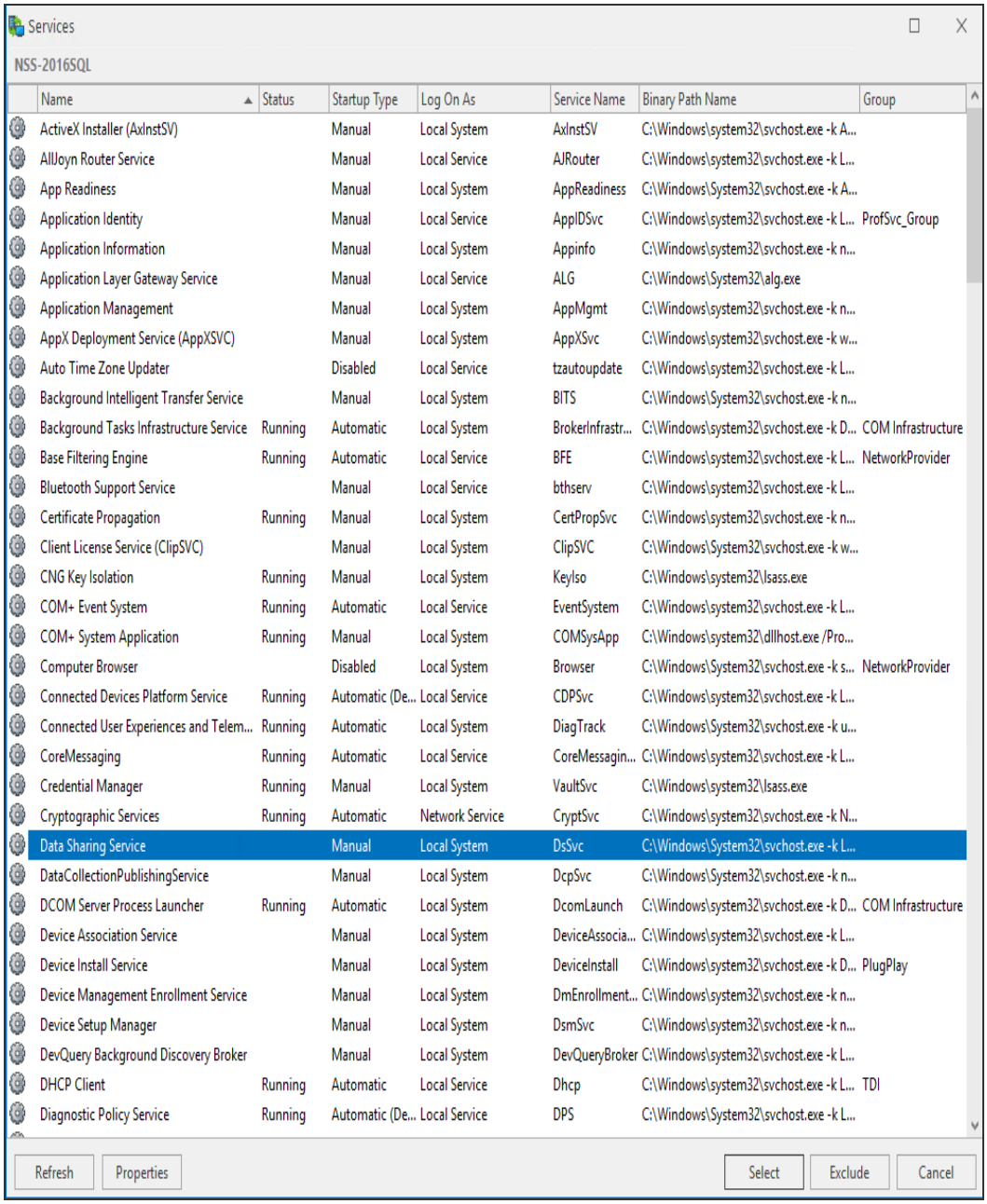
Highlight an existing selection and click **Edit** to change the service name.

Delete

Highlight an existing selection and click **Delete** and confirm the action to remove the service from the exclusion list.

Using the Service Browse Utility

When adding criteria for Service monitor rules, click **Browse** to view a list of services that are currently running on the device being monitored.



Refresh

Click **Refresh** to update this display with any services that may been started or stopped since the **Browse** option was taken.

Properties

Select a service from the display and click **Properties** to open the **Service Properties** dialog which displays all of the characteristics of the service.

Select

Select a service from the display and click **Select** to automatically populates the corresponding criteria detail fields on the criteria page.

Exclude

Select a service from this display and click **Exclude** to automatically exclude this service from this rule.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating an example Service Monitor Rule

This Service Monitor rule checks anti-virus software and restarts it if it has stopped.

1. From the **Systems** panel of the Central Configuration Manager, select the **System** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **Service Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of '**Check and Restart Anti-Virus**'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.
5. Either select the anti-virus service from the **Display Name** choice menu or click **Browse**, highlight the anti-virus service from those services listed and click **Select**. The **Service Name**, **Status** and **Startup Type** fields on the **Criteria** dialog are automatically populated.
6. In the **Service Thresholds** section of the **Criteria** dialog, set the **Status** operator to '**=**' and the value as '**Stopped**'.
7. In the left navigation pane of the **Criteria** page, click **Alert**.
8. Enable the **Override Rule Default** option and change the **Alert Text** to 'Anti-Virus software service had stopped. Automatically restarted by Halcyon NSS'. Click **OK**.
9. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
10. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
11. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the Service monitor.
12. From the Central Configuration Manager menu ribbon, click **Save**. The rule is now active within the monitor.

Windows TCP Monitors

These monitors allow the monitoring of typical network services to port level, internally and externally.

TCP Monitors allow the grouping of rules under the title of a master rule. For example, if a series of rules check a router and subsequent connections, the master rule would first check that the router can be contacted. If not, a single alert is raised for the master rule and subsequent rules in the group are ignored. If the router can be contacted, the other rules are then run in sequence. This prevents multiple alerts being generated in circumstances where a single point of failure is the cause.

> **NOTE:** Only one master rule is allowed per Rule Group.

> **WARNING:** If a specific Group is not defined then a '(default)' Group is created and used.

TCP Rule Grouping and setting a Master Rule

Groups are added at TCP Monitor level.

To specify a new group for a TCP Monitor:

1. Click the **Add Group** button at the bottom of the display.
2. Enter a unique **Name** and **Description** for the new TCP Rule Group. If there are rules highlighted in the main display when this Group is created, the option is given to move the selected rules to the new group.

Setting a Master Rule

Once the rules in the TCP Group have been defined, right-click on the rule to be defined as the master rule for this Group. From the pop-up menu, select **Set As Master Rule**. An asterisk '*' symbol is placed next to the rule in the main display to identify it as the master rule.

This rule is the one that is initially checked for this Group. If this fails, an alert is raised and remaining rules are ignored.

To remove the master rule setting, select the rule with the '*' icon beside it and right-click. From the pop-up menu select **Clear Master Rule**.

> **NOTE:** Master rules have less settings: It is not possible to specify when the rule is active, and the 'Advanced' settings cannot be used to, for example, suspend the rule.

The following TCP Monitors are available in Network Server Suite:

TCP FTP Monitor

Checks the operation of FTP servers by connecting to them and issuing a command. An alert is raised if the connection fails or invalid response is received to the command.

TCP HTTP Monitor

Checks the operation of HTTP servers by connecting to them and requesting a URL. Alert raised if connection fails or invalid page data returned. Pages can also be checked for contents. Pages requiring authentication and proxy servers are supported as are secure addresses (i.e those beginning with HTTPS). In order for the connection to an HTTPS address to be successful, the required domain must prefix the user name, for example; halcyon\jsmith, in the Authentication Settings tab.

> **NOTE:** If multiple criteria are specified when entering Page Must Include/Page Must Not Include data, use **Enter** to separate criteria.

> **NOTE:** URL Authentication only works with a browser based pop-up request for user name and password. HTTP and HTTPS pages that embed this information are not supported.

The TCP HTTP Monitor also supports a file path as well as a URL. Use the 'Load Page From' drop-down selection, available on the criteria tab to specify whether the path is a URL or a file path.

> **NOTE:** If a wildcard file path is specified, only the most recent file is processed.

TCP HTTP Monitor Status Code Checking

An additional feature within the TCP HTTP Monitor allows you to check the HTTP status code returned.

Enable this feature to be able to compare the returned HTTP Status Code against a pre-defined value, range of values or series of values.

Use the first set of selection parameters to be able to enter a range of values between (or outside of) which the returned status code must be returned in order to raise an alert or pass the check (dependent on other criteria settings).

Use the second set of selection parameters to enter a single value or comma separated values against a comparator to specify the status code check to be made.

TCP HTTP Monitor Authentication

The TCP HTTP Monitor supports TLS authentication.

TCP NNTP Monitor

Checks the operation of NNTP (news) servers by connecting to them and issuing a command. Alert raised if connection fails or invalid response received to command.

TCP Ping Monitor

Checks the status of remote devices by sending ICMP ping. The number of ping attempts per device and success percentage can be specified. Alert raised if success percentage falls below threshold.

TCP POP3 Monitor

Checks the operation of POP3 servers by connecting to them and issuing a command. Alert raised if connection fails or invalid response received to command.

TCP SMTP Monitor

Checks the operation of SMTP (mail) servers by connecting to them and issuing a command. Alert raised if connection fails or invalid response received to command.

TCP Telnet Monitor

Checks the operation of TCP and User Datagram Protocol Servers (UDP) by connecting to them and optionally issuing a command. Alert raised if connection fails or invalid response received to command.

TCP/UDP Generic Monitor

Checks the operation of TCP and User Datagram Protocol Servers (UDP) by connecting to them and optionally issuing a command. Alert raised if connection fails or invalid response received to command.

All TCP Monitors check a specific IP address or host name with optional port, username and password.

All TCP Monitors have a default interval setting of 5 minutes between connections.

TCP Monitor Testing

All TCP Monitors have test facilities that can check the current settings prior to creating the rule. In most instances, a command and trigger value can be applied so that the criteria can be fine-tuned.

Local v Remote Testing

Test options allow you to run the tests from either the local or remote device. If the test is run locally, testing is performed on the machine on which the rule is being created, typically the machine on which Central Configuration Manager is installed.

If the test is run remotely, it is run from server agent on the device for which the rule is intended.

> EXAMPLE:
> By creating a TCP HTTP rule on a remote system to find an instance of 'monitoring' on www.fortra.com, you would expect both the local and remote tests to return the same result.
>
> However, the remote system may be behind a firewall, or connect via a proxy server, in which case the local test would still pass but the remote test would fail, and you would have to reconfigure the rule criteria (for that remote device only) to provide authentication /proxy server details in order for the criteria to return the desired result.
>
> It is therefore good practice to test both locally and remotely on all rule where the option is available to ensure that the results are as expected.

Detailed Logging

Detailed logging displays a comprehensive report of the test results rather than a summary view.

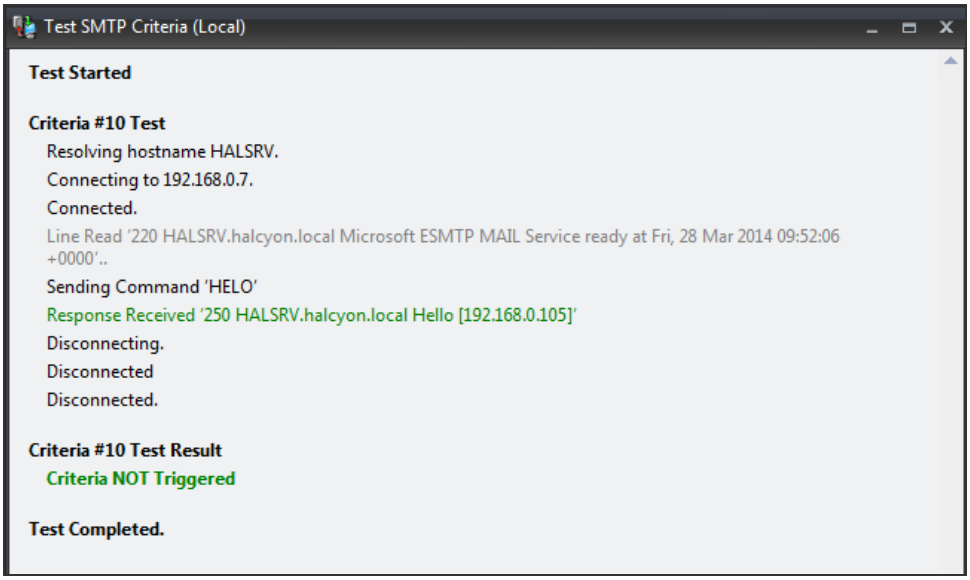
Test Results

When using the Command and Trigger Value Options it is recommended that the test facility is used to ensure that you have applied the correct trigger value to the command in order to generate the expected result. The following two examples demonstrate the different results obtained when using two different settings:

Example One:

In the following example, the test on the TCP SMTP Monitor is to ensure that the Response code 250 is not received from the HELO Command.

When **Test** is used the following result is obtained:

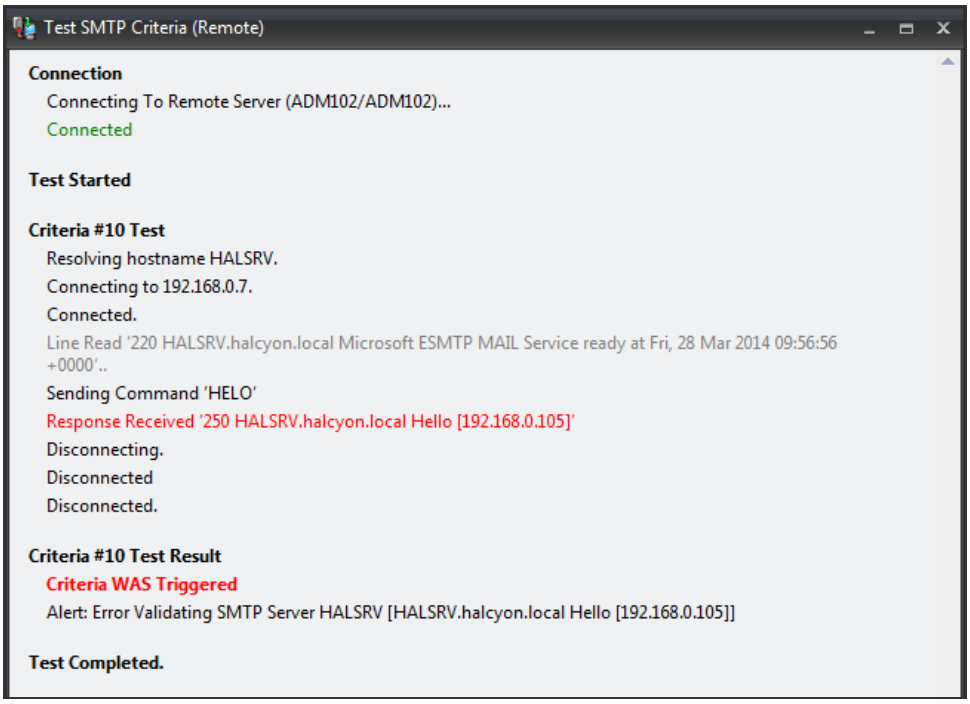


In the above example, an alert **IS NOT** raised as the response was 250 and the trigger value was set at <> (not equal to). Any other result, other than 250 would have resulted in an alert being raised.

Example Two:

In the following example, the test on the TCP SMTP Monitor is to ensure that the Response code 250 is received from the HELO Command.

When Test is used, the following result is obtained:



An alert **IS** raised as the response was again 250 but the trigger value in this instance was set at = (equals). Therefore the correct response of 250 triggered the criteria and raised an alert. Any response other than 250 would have passed this test.

TCP Monitor Options

Please refer to the following table for the options available for each TCP Monitor:

TCP Monitor	Test Facility?	Command?	Trigger Values?	Comparators
FTP	✓	✓	✓	=, >, >=, <, <=, <>
HTTP	✓	✘	✘	
NNTP	✓	✓	✓	=, >, >=, <, <=, <>
PING	✓	✘	✘	
POP3	✓	✓	✓	=, <>
SMTP	✓	✓	✓	=, >, >=, <, <=, <>
Telnet	✓	✓	✓	=, >, >=, <, <=, <>
UDP/Generic	✓	✓	✓	=, <>

Creating TCP FTP Monitor Rules

The following section provides instructions on how to create a typical TCP FTP Rule.

TCP FTP Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP FTP Monitor.

Criteria page

FTP Server Parameters section

The fields in this section define the FTP Server configuration parameters.

Host /Address

Enter the Host name or IP Address of the FTP Server to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Port Number

Select the Port Number on which the FTP connection is made. The default setting is 21.

Timeout

Specify the timeout, in milliseconds, after which an FTP connection to the specified server is deemed unsuccessful. The default setting is 5000 milliseconds.

User Name

If the FTP server requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

FTP Command section

The fields in this section specify the FTP command to use and the expected response.

Command

Enter the Command to be sent to the FTP server. The default setting is NOOP. The NOOP command is simply used as a "ping" instruction for the server. This command is mainly used to keep the control channel alive during idle periods.

Response

Enter the expected response from the server using a comparator (equals, greater then, and so on) and a value. If the response is matched when the rule is running, an alert is generated. The default setting for this parameter is 'Not Equal' to '200'. Therefore, any response other than 200 from the FTP server generates an alert.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Proxy section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the FTP server.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to the FTP server.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 21.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating TCP HTTP Monitor Rules

The following section provides instructions on how to create a typical TCP HTTP Rule.

TCP HTTP Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP HTTP Monitor.

Criteria page

HTTP Parameters section

The fields in this section define the HTTP configuration parameters.

Load Page From

Defines whether the page to be monitored is loaded from a URL or a File. Use the drop-down menu to select the required option.

For a **URL** entry, enter the full path of the required Hostname/IP Address page to be checked.

If **File** is selected, ... **Browse** is enabled allowing navigation to the required directory and file path.

Use Results From Previous Criteria

This option can be used to perform actions on the results generated by the previous criteria in this monitor. When this option is enabled, the **Search Path** field changes to **Variable**. Enter the variable '**&EN**' to represent the **Matched Name** of the previous criteria.

This option is useful for scenarios such as ensuring that a series of files have been received by FTP correctly. On receipt of the final file, an action can be taken to copy all files to another folder.

Retry

Specify the number of retries allowed before the connection to the URL or File is deemed unsuccessful.

Timeout

Specify the amount of time, in milliseconds, before a connection is deemed to have failed and a retry (if specified) is attempted.

Scan Options section

The fields in this section define whether a page must or must not include a specific Character string.

Page Must Include

Enter the required characters, numeric or textual string that must be found on the page or in the file in order to trigger the criteria.

Use the drop-down menu and select ALL if multiple entries are used in this field and all are required to be found.

Page Must Not Include

Enter the required characters, numeric or textual string that must not be found on the page or in the file in order to trigger the criteria.

Use the drop-down menu and select ALL if multiple entries are used in this field and all are required to be missing.

Status Code Checking section

The fields in this section allow the checking of the returned HTTP Status Code.

Enable this feature to be able to compare the returned HTTP Status Code against a pre-defined value, range of values or series of values.

Use the first set of selection parameters to be able to enter a range of values between (or outside of) which the returned status code must be returned in order to raise an alert or pass the check (dependent on other criteria settings).

Use the second set of selection parameters to enter a single value or comma separated values against a comparator to specify the status code check to be made.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Authentication page

URL Authentication Settings section

The fields in this section define the type of authentication used (if needed) and the user name and password required to access the HTTP server.

Authentication Scheme

Defines the type of authentication used, if any, required to access the HTTP server.

- **Basic**: Basic authentication is the simplest technique for enforcing access controls to web resources because it doesn't require cookies, session identifiers, or login pages
- **Digest**: This can be used to confirm the identity of a user before sending sensitive information, such as online banking transaction history. It applies a hash function to the username and password before sending them over the network.
- **None**: No authentication is required for the HTTP Server.
- **NTLM**: NT LAN Manager (NTLM) is a challenge-response authentication protocol which uses three messages to authenticate a client in a connection oriented environment, and a fourth additional message if integrity is desired.
- **Negotiate**: Negotiate authentication automatically selects between the Kerberos protocol and NTLM authentication, depending on availability.

User Name

If required, enter the user name needed for the selected authentication scheme.

Password

Enter the password associated with the entered user name.

Proxy Server Settings section

The settings in this section specify the settings required if a proxy server is in use.

Use Proxy Server

Click to specify that a proxy server is used to connect to the URL.

Host/Address

Enter the Host name or IP Address of the proxy server used to connect to the HTTP server.

Port Number

Enter the port number on which the connection is made. The default setting is 8080.

Authentication Scheme

If required, select the method of authentication used to access the proxy server.

- **Basic**: Basic authentication is the simplest technique for enforcing access controls to web resources because it doesn't require cookies, session identifiers, or login pages
- **Digest**: This can be used to confirm the identity of a user before sending sensitive information, such as online banking transaction history. It applies a hash function to the username and password before sending them over the network.
- **None**: No authentication is required for the HTTP Server.
- **NTLM**: NT LAN Manager (NTLM) is a challenge-response authentication protocol which uses three messages to authenticate a client in a connection oriented environment, and a fourth additional message if integrity is desired.
- **Negotiate**: Negotiate authentication automatically selects between the Kerberos protocol and NTLM authentication, depending on availability.

User Name

If required, enter the user name needed for the selected authentication scheme.

Password

Enter the password associated with the entered user name.

Enabled Protocols section

This section specifies the protocols that are enabled for this HTTP server. Multiple protocol selection is allowed.

The following protocols can be selected:

- **SSL2**: The Secure Socket Layer SSL2 protocol is a version of SSL that has been deprecated since 2011 and is considered insecure. This is disabled by default.
- **SSL3**: The SSL3 protocol is a newer version of SSL but has also been depreciated and is also considered insecure following a vulnerability known as a POODLE attack. This is disabled by default.

- **TLS1**: TLS1 is the first version of Transport Layer Security that supersedes the SSL protocols. This and the following TLS protocaols are enabled by default.
- **TLS1.1**: TLS1.1 is an updated version, released in 2006
- **TLS1.2**: TLS1.2 is the lastest version, released in 2008.

Firewall page

Firewall Proxy section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the HTTP server.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to the HTTP server.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 443.

Firewall Proxy Type

From the drop-down menu, select the type of firewall proxy used. Select from:

- **None**: No firewall proxy is used.
- **Tunneling**: In this mechanism, the client asks an HTTP proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client.
- **SOCKS4**: SOCKS uses a handshake protocol to inform the proxy software about the connection that the client is trying to make, and then acts as transparently as possible.
- **SOCKS5**: An extension of the SOCKS4 protocol offering more choices for authentication and adding support for IPv6 and UDP, the latter of which can be used for DNS lookups.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

User Agent section

This section is used to define any User Agent string.

User Agent String

In HTTP, the User-Agent string is often used for content negotiation, where the origin server selects suitable content or operating parameters for the response. The User-Agent string is one of the criteria by which Web crawlers may be excluded from accessing certain parts of a website. The information in the User-Agent string contributes to the information that the client sends to the server.

If required, enter the User Agent string to be used in this rule.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating an example TCP HTTP Monitor Rule

The following instructions create a simple TCP HTTP Monitor rule.

1. From the **Systems** panel of the Central Configuration Manager, select the **system** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **TCP HTTP Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of 'HTTP Web Page Check'. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.
5. Enter the actual URL of the web page that you wish to monitor or the IP Address of the web server on which the page is hosted.

> **NOTE:** Using generic pages such as www.google.com can lead to a denial of service as the host machine may believe that it is the subject of a malicious attack.

6. If required, enter text that either **must** or **must not** be included in the returned page text. Click **Test** to experiment with these settings. Close the **Test** dialog and make any changes to the settings and text (if entered). Re-test if required. When finished, click **OK**.
7. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
8. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
9. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the TCP HTTP Monitor.
10. From the Central Configuration Manager menu ribbon, click **Save**. The rule is now active within the monitor.

Creating TCP IMAP Monitor Rules

The following section provides instructions on how to create a typical TCP IMAP Rule.

TCP IMAP Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP IMAP Monitor.

Criteria page

IMAP Server Parameters section

The fields in this section define the IMAP Server configuration parameters.

Host /Address

Enter the Host name or IP Address of the IMAP Server to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Port Number

Select the Port Number on which the IMAP connection is made. The default setting is 143.

Timeout

Specify the timeout, in milliseconds, after which an IMAP connection to the specified server is deemed unsuccessful. The default setting is 5000 milliseconds.

User Name

If the IMAP server requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

IMAP Command section

The fields in this section specify the IMAP command to use and the expected response.

Command

Enter the Command to be sent to the IMAP server. The default setting is NOOP. The NOOP command is simply used as a "ping" instruction for the server. This command is mainly used to keep the control channel alive during idle periods.

Response

Enter the expected response from the server using a comparator (equals, greater then, and so on) and a value. If the response is matched when the rule is running, an alert is generated. The default setting for this parameter is 'Not Equal' to 'OK'. Therefore, any response other than OK from the IMAP server generates an alert.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Proxy section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the IMAP server.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to the IMAP server.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 993.

Firewall Proxy Type

From the drop-down menu, select the type of firewall proxy used. Select from:

- **None**: No firewall proxy is used.
- **Tunneling**: In this mechanism, the client asks a proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client.
- **SOCKS4**: SOCKS uses a handshake protocol to inform the proxy software about the connection that the client is trying to make, and then acts as transparently as possible.
- **SOCKS5**: An extension of the SOCKS4 protocol offering more choices for authentication and adding support for IPv6 and UDP, the latter of which can be used for DNS lookups.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating TCP Ping Monitor Rules

The following section provides instructions on how to create a typical TCP Ping Rule.

TCP Ping Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP Ping Monitor.

Criteria page

Ping Destination section

The fields in this section define the Ping destination configuration parameters.

Host /Address

Enter the Host name or IP Address of the Ping destination to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Timeout

Specify the timeout, in milliseconds, after which a ping command to the specified server is deemed unsuccessful. The default setting is 2000 milliseconds.

Ping Parameters section

The fields in this section specify the configuration of the ping command. These settings work together to define whether an alert is generated.

Ping Attempts

Defines how many attempts are made before an alert is generated. The default setting is 4.

Success Percentage

This setting gives the required percentage of ping success rate before an alert is generated. The default setting is 50%

Time-to-Live

This setting defines for how long the ping is active. The default setting is 128 milliseconds.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click ? to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Proxy section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy to reach the ping destination.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating an example TCP Ping Monitor Rule

The following instructions create a simple TCP Ping Monitor rule.

1. From the **Systems** panel of the Central Configuration Manager, select the **system** to which the monitor rule is applied and expand the view so that the monitors are displayed.
2. Select the **TCP Ping Monitor** and click **Add Rule** to display the **Add Rule Detail** dialog.
3. Enter a **Description** of **Ping Connection**. Leave other fields on this page as the default settings.
4. Select the **Criteria tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Criteria**.
5. Enter the **IP Address** of the device to which the ping connection is sent.
6. Keep the system defaults and click **Test** to experiment with these settings. Close the **Test** dialog and make any changes to the default settings that are more suited to your own operational environment. Re-test if required. When finished, click **OK**.
7. Select the **Actions tab** in the left navigation pane of the **Add Rule Detail** dialog and click **Add Action**.
8. Select the **Send Enterprise Console Alert** action. Click **OK** to open the **Console Action** dialog. Leave the fields as their default settings and click **OK**.
9. On the **Add Rule Detail** dialog, click **OK** to create the rule, which is then displayed in the **System Rule** panel for the TCP Ping Monitor.
10. From the Central Configuration Manager menu ribbon, click **Save**. The rule is now active within the monitor.

Creating TCP POP3 Monitor Rules

The following section provides instructions on how to create a typical TCP POP3 Rule.

TCP POP3 Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP POP3 Monitor.

Criteria page

POP3 Server Parameters section

The fields in this section define the POP3 Server configuration parameters.

Host /Address

Enter the Host name or IP Address of the POP3 Server to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Port Number

Select the Port Number on which the POP3 connection is made. The default setting is 1110.

Timeout

Specify the timeout, in milliseconds, after which an POP3 connection to the specified server is deemed unsuccessful. The default setting is 5000 milliseconds.

User Name

If the POP3 server requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

POP3 Command section

The fields in this section specify the POP3 command to use and the expected response.

Command

Enter the Command to be sent to the POP3 server. The default setting is STAT. The STAT command is simply used as a "ping" instruction for the server. This command is mainly used to keep the control channel alive during idle periods.

Response

Enter the expected response from the server using a comparator (equals, greater then, and so on) and a value. If the response is matched when the rule is running, an alert is generated. The default setting for this parameter is 'Not Equal' to '+OK'. This can be changed to 'Equal' to '=OK' or 'Not Equal' or 'Equal' to '-ERR'. Therefore, any response other than the selected response combination generates an alert.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Proxy section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the POP3 server.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to the POP3 server.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 995.

Firewall Proxy Type

From the drop-down menu, select the type of firewall proxy used. Select from:

- **None**: No firewall proxy is used.
- **Tunneling**: In this mechanism, the client asks a proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client.
- **SOCKS4**: SOCKS uses a handshake protocol to inform the proxy software about the connection that the client is trying to make, and then acts as transparently as possible.
- **SOCKS5**: An extension of the SOCKS4 protocol offering more choices for authentication and adding support for IPv6 and UDP, the latter of which can be used for DNS lookups.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating TCP SMTP Monitor Rules

The following section provides instructions on how to create a typical TCP SMTP Rule.

TCP SMTP Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP SMTP Monitor.

Criteria page

SMTP Server Parameters section

The fields in this section define the SMTP Server configuration parameters.

Host /Address

Enter the Host name or IP Address of the SMTP Server to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Port Number

Select the Port Number on which the SMTP connection is made. The default setting is 25.

Timeout

Specify the timeout, in milliseconds, after which an SMTP connection to the specified server is deemed unsuccessful. The default setting is 5000 milliseconds.

SMTP Command section

The fields in this section specify the SMTP command to use and the expected response.

Command

Enter the Command to be sent to the SMTP server. The default setting is HELO. The HELO command is simply used to identify yourself to the SMTP server.

Response

Enter the expected response from the server using a comparator (equals, greater then, and so on) and a value. If the response is matched when the rule is running, an alert is generated. The default setting for this parameter is 'Not Equal' to '250'. Therefore, any response other than 250 from the SMTP server generates an alert. Other comparators and response values can be used if required.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Settings section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the SMTP server.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to the SMTP server.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 25.

Firewall Proxy Type

From the drop-down menu, select the type of firewall proxy used. Select from:

- **None**: No firewall proxy is used.
- **Tunneling**: In this mechanism, the client asks a proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client.
- **SOCKS4**: SOCKS uses a handshake protocol to inform the proxy software about the connection that the client is trying to make, and then acts as transparently as possible.
- **SOCKS5**: An extension of the SOCKS4 protocol offering more choices for authentication and adding support for IPv6 and UDP, the latter of which can be used for DNS lookups.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> **NOTE:** SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating TCP Telnet Monitor Rules

The following section provides instructions on how to create a typical TCP Telnet Rule.

TCP Telnet Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP Telnet Monitor.

Criteria page

TCP Telnet Server Parameters section

The fields in this section define the TCP Telnet server configuration parameters.

Host /Address

Enter the Host name or IP Address of the Telnet server to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Port Number

Select the Port Number on which the connection to the Telnet server is made. The default setting is 23.

Timeout

Specify the timeout, in milliseconds, after which a connection to the specified Telnet server is deemed unsuccessful. The default setting is 5000 milliseconds.

Telnet Command section

The fields in this section specify the Telnet command to use and the expected response.

Command

Enter the Command to be sent to the Telnet server. The default setting is HELP.

Response

Enter the expected response from the server using a comparator (equals, greater then, and so on) and a value. If the response is matched when the rule is running, an alert is generated. The default setting for this parameter is 'Not Equal' to '250'. Therefore, any response other than 250 from the Telnet server generates an alert. Other comparators and response values can be used if required.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Settings section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the Telnet server.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to the Telnet server.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 23.

Firewall Proxy Type

From the drop-down menu, select the type of firewall proxy used. Select from:

- **None**: No firewall proxy is used.
- **Tunneling**: In this mechanism, the client asks a proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client.
- **SOCKS4**: SOCKS uses a handshake protocol to inform the proxy software about the connection that the client is trying to make, and then acts as transparently as possible.

- **SOCKS5**: An extension of the SOCKS4 protocol offering more choices for authentication and adding support for IPv6 and UDP, the latter of which can be used for DNS lookups.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

Creating TCP/UDP Generic Monitor Rules

The following section provides instructions on how to create a typical TCP/UDP Generic Monitor Rule.

TCP/UDP Generic Monitor specific criteria fields

When adding criteria the following pages and fields are specific to the TCP/UDP Generic Monitor.

Criteria page

Generic Server Parameters section

The fields in this section define the connection configuration parameters of the TCP or UDP server.

Host /Address

Enter the Host name or IP Address of the TCP or UDP server to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Port Number

Select the Port Number on which the connection to the TCP or UDP server is made. The default setting is 0.

Timeout

Specify the timeout, in milliseconds, after which a connection to the TCP or UDP server is deemed unsuccessful. The default setting is 5000 milliseconds.

Protocol

Select the type of protocol to use for this rule.

- **TCP**: Select the TCP protocol and optionally select to read a specified number of lines on connection.
- **UDP**: Select the UDP protocol and optionally select that no response indicates an error.

TCP Command section

The fields in this section specify the command to use and the expected response.

Command

Enter the Command to be sent to the TCP or UDP server. This field is blank by default.

If Response

Enter the expected response from the server using a comparator (equals, greater then, and so on) and a value. If the response is matched when the rule is running, an alert is generated. The expected response can use wildcard characters '*' and '?' in order to obtain a result.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Firewall page

Firewall Settings section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy with the TCP or UDP server.

Enable Firewall Proxy

Click to enable the use of a firewall proxy when connecting to the TCP or UDP server.

Host /Address

Enter the Host name or IP Address of the firewall proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the firewall proxy is made. The default setting is 1.

Firewall Proxy Type

From the drop-down menu, select the type of firewall proxy used. Select from:

- **None**: No firewall proxy is used.
- **Tunneling**: In this mechanism, the client asks a proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client.
- **SOCKS4**: SOCKS uses a handshake protocol to inform the proxy software about the connection that the client is trying to make, and then acts as transparently as possible.
- **SOCKS5**: An extension of the SOCKS4 protocol offering more choices for authentication and adding support for IPv6 and UDP, the latter of which can be used for DNS lookups.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Source Device section

These fields in this section allow to you override the source device. This means that for any alerts raised by this rule criteria, the Device for the alert is shown as the selected 'Override Source Device' rather than the Device that actually performed the check.

Override Source Device

Click to enable the override source device functionality.

Source Device

From the drop-down list, select the device to be used as the source device for any alerts raised by this rule criteria. The device must already exist in Device Manager

Wildcard Characters section

Fields in this section determine alternative characters that can be used for multiple or single character substitution.

Use * As A Substitute For Zero Or More Characters

Specify a character, other than '*' that will be used as a wildcard substitution for none or multiple characters in this rule.

Use ? As A Substitute For A Single Character

Specify a character, other than '?', that will be used as a wildcard substitution of a single character in this rule.

Auto-Close Options section

These fields determine if the auto-closing of Enterprise Console Alerts is required and if so, the delay invoked before the auto-close becomes effective.

Auto-Close Enterprise Console Alerts

Click this option to automatically close any alerts sent to the Enterprise Console by this rule. 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 either immediately or after the specified **Delay By** 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.

Delay By

If the **Auto-Close Enterprise Console Alerts** option is enabled, specify the delay time period after which the alert is automatically closed providing the criteria has not triggered again in the next check interval. The time period can be specified in Minutes, Hours or Days.

AIX Monitors

The AIX Server Manager monitors check specific elements of any licensed AIX system located on the network and loaded into Network Server Suite via the Device Manager. The AIX Monitors work in the same way as the Windows monitors, in that rules are created, criteria specified and actions set.

Each rule has default alert text assigned, which can be overridden at criteria level so that the actual alert text is specific to the criteria from which it was raised.

The following monitors are available for the specific monitoring of AIX servers.

AIX Error Report Monitor

The AIX Error Report Monitor checks the output from the AIX command `ERRPT` and looks for the occurrence of specific errors. An alert is raised if the error is found.

Subsystem Monitor

The AIX Subsystem Monitor checks the status of AIX subsystems for one of four conditions, raising an alert if the condition is proven.

Logical Volume Monitor

The AIX Logical Volume Monitor checks the status of Logical Groups, Logical Volumes and Physical Volumes of the AIX system. Alerts are raised if the criteria exists, does not exist or triggers a pre-defined value. The current status of the Logical Groups, Logical Volumes and Physical Volumes can be displayed when setting the rule criteria.

A test facility is also available that allows the pre-test of the rule with the current criteria settings and amending as required based on the received results.

Script Monitor

The AIX Script Monitor runs custom AIX scripts and commands and checks the output against Regular Expressions.

File & Folder Monitor

The AIX File & Folder Monitor checks AIX files and folders for existence, non-existence or for any physical changes. Alerts are raised if any of the selected conditions are proven or for any

changes in selected folders and/or files. For example, when a new file is created in a folder or when the size of a file changes. This is useful for ensuring that critical files are not deleted.

Log File Monitor

The AIX Log File Monitor checks the standard AIX event logs. New events in the log can be filtered and alerts raised accordingly. Rule Criteria use Regular Expressions to filter information. Regular expressions allow the selection of specific strings from a set of character strings.

CPU, Filesystem & Memory Monitor

The AIX CPU, FileSystem and Memory Monitor gives administrators the ability to monitor the CPU, Filesystem and Memory statistical data of any AIX system loaded into the Central Configuration Manager.

System Monitor

Th AIX System Monitor checks system load average over a pre-defined time period. Alert raised if load exceeds, equals or falls short of user-defined criteria. The System Monitor can also monitor system up-time of AIX device.

Process Monitor

The AIX Process Monitor checks AIX system processes by a series of processor measurements, such as CPU Usage %, Cumulative CPU Time and so on. Alerts are raised when a process triggers a pre-defined value.

Ping Monitor

The AIX Ping Monitor checks the status of remote devices by sending an ICMP ping. The number of ping attempts per device and success percentage can be specified. An alert is raised if success percentage falls below threshold.

AIX Actions

Only three actions are available when creating AIX Monitor rules:

- Execute Command action
- Send Enterprise Console Alert action
- Send Instant Alert Message action

See Adding Rule Actions for more information on these three action types.

AIX Error Report Monitor

The AIX Error Report Monitor checks the output from the **ERRPT** command and looks for specific errors occurring within the report.

To run the **ERRPT** command type:

ERRPT -A

at a valid input point. Output is produced which is similar in appearance to that shown below:

```
---------------------------------------------------------
LABEL:          REBOOT_ID
Date/Time:       Tue 14 Apr 12:30:40 2009
Type:            TEMP
Resource Name:   SYSPROC
Description
SYSTEM SHUTDOWN BY USER
Detail Data
USER ID
          0
0=SOFT IPL 1=HALT 2=TIME REBOOT
          0
TIME TO REBOOT (FOR TIMED REBOOT ONLY)
          0
---------------------------------------------------------
LABEL:          ERRLOG_ON
Date/Time:       Tue 14 Apr 12:32:00 2009
Type:            TEMP
Resource Name:   errdemon
Description
ERROR LOGGING TURNED ON
---------------------------------------------------------
LABEL:          ERRLOG_OFF
Date/Time:       Tue 14 Apr 12:26:58 2009
Type:            TEMP
Resource Name:   errdemon
Description
ERROR LOGGING TURNED OFF
---------------------------------------------------------
```

> **NOTE:** In order to set meaningful rule criteria, familiarity with the contents of the ERRPT output is required.

Adding AIX Error Report rule criteria

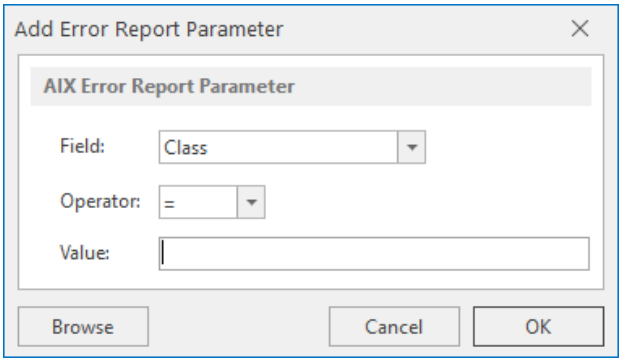
AIX Error Report criteria allow the application of a trigger value from a pre-defined list of common variables, the setting of a comparator and entering a suitable description for the trigger value.

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Error Report Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **AIX Error Report Criteria** dialog.

There are two pages to complete when adding AIX Error Report Monitor criteria.

Criteria Page

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Error Report Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **AIX Error Report Criteria** dialog.
3. Click **Add Parameter** to open the **Add Error Report Parameter** dialog.



4. Select the **Field** from the drop-down menu, select the **Operator** and enter a **Value** on which this rule criteria is based and click **OK** or alternatively, click **Browse** to open the **Error Reports** dialog that shows the current error report contents.
5. Click on an item from within this report and the full details are shown in the **Details** pane of this dialog. Click **Select** to select this error as the parameter criteria for the rule.
6. Click **OK** to add the parameter to the criteria for this rule.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

AIX Subsystem Monitor

The AIX Subsystem Monitor is a simple monitor that checks the AIX subsystems of group of subsystems for one of five conditions:

- Subsystem Exists
- Subsystem Does Not Exist
- Subsystem Is Operative
- Subsystem Is Inoperative
- Subsystem Is Stopping

Subsystems can be specified by Name or by Group. An alert is raised when the chosen condition is met for the specified Subsystem Name or Group.

When the instance of the Subsystem to which this rule criteria applies is specified, a full path to the required instance can be entered or Wildcards '*' and '?' used to create a generic entry. Regular expressions can also be entered by changing the entry in the first drop down choice

menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Wildcards and regular expressions can be used to create generic rules that can then be included in a template in order to monitor multiple systems.

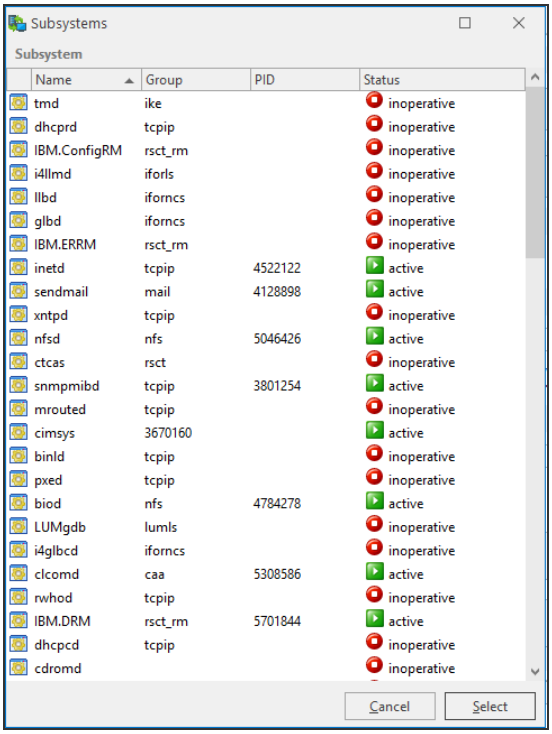
> **NOTE:** In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to the Enterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Adding AIX Subsystem rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Subsystem Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Subsystem Criteria** dialog.

Rapid Method

1. From the **Subsystem Criteria** dialog click **Browse** to open the **Subsystems** dialog, listing all the subsystems and status information.



2. Click on a subsystem to highlight and then click **Select**.

The Subsystem Parameters for this criteria are automatically populated with the data from the selected subsystem.

In-depth Method

There are three pages to complete when adding AIX Subsystem rule criteria.

Criteria page

Category section

This section defines how the subsystem is selected.

Monitor Type

Use the drop-down menu to define the type of subsystem monitor for the rule:

- **Subsystem by Name**: Just the named subsystem is monitored
- **Subsystem by Group**: The group which contains the subsystem is monitored.

> NOTE: Subsequent fields and values change dependent on the selection made in this field.

Instance section

This section defines how subsystem name or group is defined.

Subsystem Name (Group)

Use the drop down menu to select whether the subsystem name or group is defined by the use of wildcards '*' and '?' or by Regular Expression (Regex).

Trigger section

This section defines the unit of measure and how actions are performed.

Measure

Use the drop-down menu to determine how the criteria is measured for this rule.

For Subsystem Names the following options are available. In each case the criteria is triggered if:

- **Subsystem Exists**: The named subsystem is found
- **Subsystem Does Not Exist**: The named subsystem is not found
- **Subsystem Is Active**: The named subsystem is active
- **Subsystem Is Inoperative**: The named subsystem is inoperative
- **Subsystem Is Stopping**: The named subsystem is stopping

For Subsystem Groups, the following options are available. In each case the criteria is triggered if:

- **Group Has Subsystems**: The group contains subsystems
- **Group Has No Subsystems**: The group does not contain subsystems
- **Group Has Active Subsystems**: The group contains active subsystems
- **Group Has Inactive Subsystems**: The group contains inactive subsystems
- **Group Has Stopping Subsystems**: The group contains subsystems that are stopping

Perform Actions For:

If the criteria is set to **perform actions for the first triggered instance**, any resulting alert contains a summary of the instances that breached the criteria threshold. If it is set to **perform actions for all triggered instances,** then an alert is raised for each instance containing only details of that particular instance.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> **NOTE:** SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Testing

Once the Subsystem parameters have been defined for the criteria, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to define and confirm the subsystem parameters as criteria for this rule.

AIX Logical Volume Monitor

AIX uses a Logical Volume Manager (LVM) to manage, at a logical level, all of the file systems and directories created within an AIX system. The LVM maps data between logical and physical storage, allowing data to be non-contiguous, span multiple disks, flexible and dynamically expanded.

The AIX Logical Volume Monitor checks the Volume Group, Physical Volumes and Logical Volumes of the AIX system as defined in the LVM.

- **Volume Groups**: The containers for both the Physical and Logical Volumes
- **Physical Volumes**: The Physical Volumes are segmented into physical partitions
- **Logical Volumes**: The Logical Volumes are logical partitions logged to the physical partitions

Rule criteria change depending on the type of logical volume being monitored. However for each Monitor Type it is possible to specify if a logical volume exists, does not exist or if a performance type triggers user-defined criteria.

Specifying the instance of the Logical Volume to which this rule criteria applies allows the entry of a full path to the required instance or the use of Wildcards '*' and '?' to create a generic entry. Regular expressions can also be entered by changing the entry in the first drop down choice menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Wildcards and regular expressions can be used to create generic rules that can then be included in a template in order to monitor multiple systems.

> NOTE: In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to theEnterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Practical Examples

- A stale physical partition is a physical partition which contains data that you cannot use. Monitoring for Stale Physical Partitions alerts you when this happens so that you can take correcting action to update the stale partitions so that they contain the same information as valid physical partitions.
- Monitoring for Free Physical Partitions can alert you to when a low level of space remains on your AIX system.

Adding AIX Logical Volume rule criteria

> TIP: When setting criteria, click **Display Status** to open the **Logical Volume Status** dialog which displays the individual properties of each of the three Logical Volume monitor types and allows for more precise rule entry.

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Logical Volume Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Logical Volume Criteria** dialog.

There are three pages to complete when adding AIX Logical Volume rule criteria.

Criteria page

Category section

This section is used to define the type of volume to monitor and the trigger criteria.

Monitor Type

Use the drop-down menu to select the type of Logical Volume to be monitored:

- Volume Group
- Physical Volume
- Logical Volume

Alert If

Select from the drop-down menu when an alert is generated.

- **Exists**: An alert is generated if the named instance exists
- **Does Not Exist**: An alert is generated if the named instance does not exist
- **Criteria Triggers**: An alert is generated if the remaining criteria are met

Instance section

This section is used to identify the actual instance of the selected Monitor Type for this rule.

Logical Volume/Physical Volume/Volume Group

Use the first drop down menu to select whether the Logical Volume, Physical Volume or Volume Group is defined by the use of wildcards @*' and '?' or by Regular Expression (Regex). Use the second drop-down menu to select the required instance or enter the full path to an entry of your choice.

Trigger section

This section is used to define the Performance Type and Trigger Value for the rule criteria.

Performance Type

From the drop-down menu, select the performance type by which the Logical Volume, Physical Volume or Volume Group is measured. The selections available in the drop-down menu are dependent on the Monitor Type for which the criteria is being set.

Trigger Value

Specify the comparator (equals, greater than, less than, etc.) and enter the value threshold which if met or breached, depending on the comparator used, triggers an alert.

> **NOTE:** For Physical and Logical Volume Monitor Types, a Regex can also be used as a comparator.

Perform Actions For

If the criteria is set to **perform actions for the first triggered instance**, any resulting alert contains a summary of the instances that breached the criteria threshold. If it is set to **perform actions for all triggered instances,** then an alert is raised for each instance containing only details of that particular instance.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> **TIP:** When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Testing

Once the criteria has been set, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to define the entered parameters as criteria for this rule.

AIX Script Monitor

The AIX Script Monitor is a high-level monitor that runs a user-defined script or command against a Regular Expression.

The entered script must exist and must use the absolute path, not a relative path.

Alerts are raised if the selected Regular Expression is matched.

Adding AIX Script rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Script Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Script Criteria** dialog.

There are three pages to complete when adding AIX Script rule criteria.

Criteria Page

Script Parameters section

This section defines how the command or script to be run and Regular Expression used.

Command/Script

Type the command or script to be run.

Regular Expression

Enter the details of the Regular Expression against which the command or script is run. The default entry is '.+'.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

Advanced Settings section

Omit Lines Containing Script Process Id From Results

Select this option to remove any lines that contains the ID of the script process that was used to generate the result. This prevents any false results being generated by the process that is performing the actual monitoring.

Testing

Once the Subsystem parameters have been defined for the criteria, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to define and confirm the subsystem parameters as criteria for this rule.

AIX File & Folder Monitor

The AIX File and Folder monitor allows the browsing of both local and remote AIX devices for a specific folder and check for any changes.

Adding AIX File & Folder rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX File & Folder Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **File & Folder Criteria** dialog.

There are four pages to complete when adding AIX File & Folder rule criteria.

Criteria page

Location section

The field in this section is used to determine the path to the required File or Folder.

Search Path

Either type the path to the required folder or file directly into this field or click ... to open the **Select Folder** dialog. This allows the selection of any folder from the AIX device and the subsequent drill-down into subsequent folders.

Search Parameters section

The fields in this section specify the alert criteria and trigger actions.

Alert If

Select whether an alert should be generated if the File/Folder does or does not exist. Check the **Include Sub-Folders** option to ensure that the AIX sub-folders are included in any search.

Trigger On

Trigger actions are used to determine at which point the alert is raised and can be set against events happening against individual files, folders or file or folder.

- **First Matching**: The alert is triggered on the first matching instance of the File, Folder or File or Folder found.
- **Each Matching**: Separate alerts are triggered for each matching instance found for each File, Folder or File or Folder found.

Scan Filters section

Scan filters allow you to include or exclude specific criteria on which to search.

Include/Exclude Filters

Include and Exclude Filters allow you to enter a list of files or folders to include or exclude from the scan. Wildcards (*) can be used as a full or part replacement for file/folder name characters. When inserting file/folder names, use carriage return to generate a new line on which the next file/folder name can be entered.

Permission Filters section

Permission Filters allow you to specify the access rights to the files/folders for which you are scanning. The permission filters are split into three types:

- **User**: The owner of the file or folder
- **Group**: The group to which the owner belongs
- **Other**: Everyone else

Permission levels allow to you define, within each type, whether the file can be read, written or executed, by specifying:

- **Granted**: Permission allowed
- **Not Granted**: Permission denied
- **Both**: Permission is not checked

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Thresholds page

File Size Threshold section

The File Size Threshold is used to specify criteria that trigger an alert if the file size equals, exceeds, falls below or does not equal the entered value.

Size

Click to enable the setting of a file size threshold. Then select the comparator, enter a value and select the unit of measurement. The file size can be specified in:

- Bytes
- Kilobytes
- Megabytes
- Gigabytes
- Terabytes

Timestamp Thresholds section

This section contains fields to specify a time period or a specific time and date at which the file was modified.

Modified

Click to enable the setting of a time period or specific date and time at which the file was modified.

To specify a time period, click the top radio button and select a comparator, value and time period. The time period can be specified in:

- Seconds
- Minutes
- Hours
- Days

To specify an actual date and time, click the bottom radio button and select a time preposition, date and time at which the file was modified. The time preposition can be specified as:

- At
- After
- On Or After
- Before
- On or Before
- Not At

User Filters section

This section is used to filter the results by user or group.

User Name

Enter a user name by which the threshold results are filtered.

Group Name

Enter a Group Name by which the threshold results are filtered.

> NOTE: When entering User Filters of **User Name** and **Group Name**, you must enter the actual names and not their numerical representations.

Advanced page

Firewall Settings section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to a remote device.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 8080.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Testing

When you have entered the criteria that you require, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule ‘Live’.

Click **OK** to define the entered parameters as criteria for this rule.

AIX Log File Monitor

The AIX Log File Monitor discovers and monitors log files. When criteria are added, the monitor searches the Unix Syslog configuration file (/etc/syslog.conf) and examines the /var/log/directory and its subdirectories for plain files. A typical discovery routine may include the following log files:

- /var/log/daemon
- /var/log/kern
- /var/log/mail
- /var/log/messages
- /var/log/secure
- /var/log/sudo
- /var/log/syslog
- /var/log/user

although many more log file examples are supplied as default.

Log File Monitors can raise alerts for each new line of text that is added to the file that matches both the comparison and Regular Expression criteria.

Adding AIX Log File rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Log File Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Log File Criteria** dialog.

There are two pages to complete when adding AIX Log File rule criteria.

Criteria page

Log File Parameters section

This section is used to specify the Log File to be monitored and the Regular Expression criteria.

Log File

This field is used to define the Log File for the rule. Either type the directory path into the field or use the drop-down menu to select a log file from those already discovered

on the AIX system. Click ... to open the **Select File** dialog which allows navigation to a directory path and log file.

Expression

Enter the expression against which this log file is checked. The default entry is '.+'.

Browse

Click **Browse** to view the most recent entries in each log file. Selecting an entry from within this dialog, automatically enters it as the Expression criteria for the current rule.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Click **OK** to define the entered parameters as criteria for this rule.

AIX CPU, Filesystem and Memory Monitor

The AIX CPU, Filesystem and Memory Monitor operates in the same way as the Windows CPU, Disk & Memory Monitor and is used to check common attributes of system performance.

CPU Monitor

The CPU monitor is used to monitor either the load or the spare capacity of the machine's CPU. Use the Performance Data feature to obtain a current 'snapshot' of the system on which threshold decisions can be made.

An alert is triggered when the entered percentage is reached or equaled.

> NOTE: A CPU Load greater than 100% is allowed when totaling up across devices. For example, if a single device has multiple processors.

Filesystem Monitor

The Filesystem monitor is used to monitor both Drive Space and I-Node usage. An I-Node is a data structure on a file system on Linux and other Unix-like operating systems that stores all the information about a file except its name and its actual data.

A data structure is a way of storing data so that it can be used efficiently. Different types of data structures are suited to different types of applications, and some are highly specialized for specific types of tasks.

Drives and I-Nodes can be monitored by physical or percentage space available or by space used.

An alert is triggered when the selected criteria value for the required drive and Performance Type is reached. Alternatively, alerts can be raised if the drive exists or does not exist.

When the instance of the Filesystem volume to which this rule criteria applies is specified, a full path to the required instance can be entered or Wildcards '*' and '?' used to create a generic entry. Regular expressions can also be entered by changing the entry in the first drop down choice menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Using wildcards and regular expressions allow the creation of generic rules that can then be included in a template in order to monitor multiple systems.

> NOTE: In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to the Enterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Memory Monitor

The AIX Memory monitor is used to monitor different aspects of the memory usage of the AIX device. Physical memory, virtual memory, page file, memory load and buffers used can all be monitored and alerts raised when specific trigger value targets are reached.

Adding AIX CPU Filesystem & Memory rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX CPU Filesystem & Memory Monitor** and click **Add Rule**.

2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Performance Criteria** dialog.

There are three pages to complete when adding AIX CPU Filesystem & Memory rule criteria.

Criteria page

Category section

The fields in this section determine the type and trigger value of the selected area of system performance.

Performance Group

From the drop-down menu select the area of performance for which the rule is created. Select from:

- CPU
- Filesystem
- Memory

> **NOTE:** Further fields on this page are dependent on the selection made in this field.

Alert If

If Filesystem is selected as the Performance Group this field determines if an alert is raised based on whether the Filesystem does or does not exist or if the remaining criteria trigger.

Instance section

The fields in this section determine the instance on which the rule checks. This section is not required for Memory Performance checks.

CPU (For CPU Performance Group)

Select the CPU instance on which this rule measures performance. Select **Partition** to measure performance across the partition.

Instance (For Filesystem Performance Groups)

Select the Volume on which this rule measures performance. Select an instance from the drop-down menu, or specify an instance using either Wildcard or Regex to define the entry.

Trigger section

Fields in this section determine the trigger values on which an alert is generated.

Performance Type

From the drop-down menu select the performance type to which the rule applies.

For CPU Performance, the following choices are available:

- CPU Idle
- CPU Load

For Filesystem Performance, the following choices are available:

- Filesystem Space Available
- Filesystem Space Available %
- Filesystem Space Used
- Filesystem Space Used %
- Filesystem Space Total
- Inodes Available
- Inodes Available %
- Inodes Used
- Inodes Used %
- Inodes Total

For Memory Performance, the following choices are available:

- Buffers Used
- Memory Load
- Page File Available
- Page File Available %
- Page File Used
- Page File Used %
- Page File Total

- Physical Memory Available
- Physical Memory Available %
- Physical Memory Used
- Physical Memory Used %
- Physical Memory Total
- Virtual Memory Available
- Virtual Memory Used
- Virtual Memory Total

Trigger Value

The trigger value is used to specify a percentage value threshold at which the Performance criteria is set. The following comparators can be used:

- **=** The trigger value is exactly equal to the percentage value entered.
- **>** The trigger value is greater than the percentage value entered.
- **>=** The trigger value is greater than or equal to the percentage value entered.
- **<** The trigger value is less then the percentage value entered.
- **<=** The trigger value is less than or equal to the percentage value entered.
- **<>** The trigger value is anything other than the percentage value entered.

Trigger On

Trigger actions are used to determine at which point the alert is raised. This option is only available if Filesystem is selected in the Performance Group.

- **First Triggered Instance**: The alert is triggered on the first matching instance found.
- **All Triggered Instances**: A single alert is triggered with the information of up to 50 matching instances found.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> **NOTE:** SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

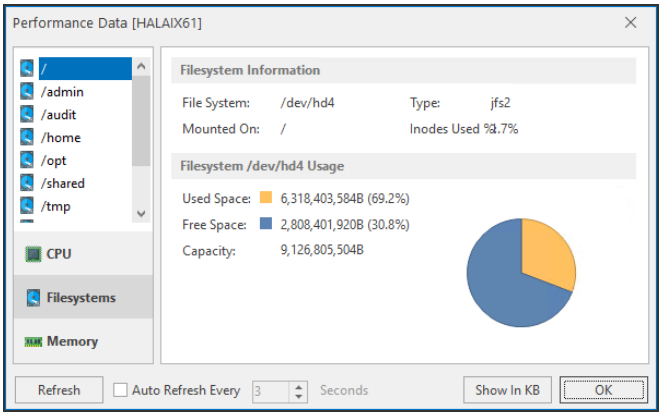
Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Using the Performance Data utility

Prior to setting any criteria for this monitor, it is advisable to use the **Performance Data** button, on the **Performance Criteria** dialog to display the current Performance Data for the chosen system.



Use the tabs in the left-hand navigation panel of this display to view the relevant performance data of each attribute of the selected system.

Refresh

Use **Refresh** to periodically update the display or set the **Auto Refresh** setting to automatically update the display every specified number of seconds.

Show in MB/KB

Data can be displayed in KB or MB. Click **Show in MB/KB** to toggle the display between size metrics.

When you have the required information, click **OK** to close the **Performance Data** dialog.

Testing

When the required criteria has been entered, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define the entered parameters as criteria for this rule.

AIX System Monitor

Load averages are a simple measure of the number of processes that are ready to run but required to wait for access to the CPU. A load average of more than two on a system with a single CPU, for example, would indicate that the system is unable to keep up with the processes that are being submitted.

Load average represents the load averages over 1, 5, and 15-minute intervals prior to a server's transmission. The load averages are multiplied by 10 to represent the value in decimal format.

An alert is sent when the trigger value for the condition is breached.

Adding AIX System rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX System Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **System Criteria** dialog.

There are three pages to complete when adding AIX System rule criteria.

Criteria page

Category section

The fields in this section are used to determine the unit of measure.

Measure

Select the unit of measure against which to test the load average.

- **Load Average Over Past 1 Minute**
- **Load Average Over Past 5 Minutes**
- **Load Average Over Past 15 Minutes**
- **System Up Time**: The Load Average is taken against the time that the system has been running.

Trigger section

Sets the trigger value for this criteria.

Trigger Value

From the drop-down list select the comparator and enter the trigger value against which the criteria is set.

For System Up Time rules, specify a trigger value for Seconds, Minutes or Hours.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Testing

When the required criteria has been entered, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define and confirm the entered parameters as criteria for this rule.

AIX Process Monitor

The AIX Process Monitor is used to monitor all processes running on the AIX system. Processes can be monitored by Process Name, Process Owner or Process Identification Number (PID). You can select to generate alerts based on whether the process does or does not exist or if it is triggered by the rule criteria.

When you specify the instance of the Process to which this rule criteria applies, you can enter a full path to the required instance or use Wildcards '*' and '?' to create a generic entry. Regular expressions can also be entered by changing the entry in the first drop down choice menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Using wildcards and regular expressions allow you to create generic rules that can then be included in a template in order to monitor multiple systems.

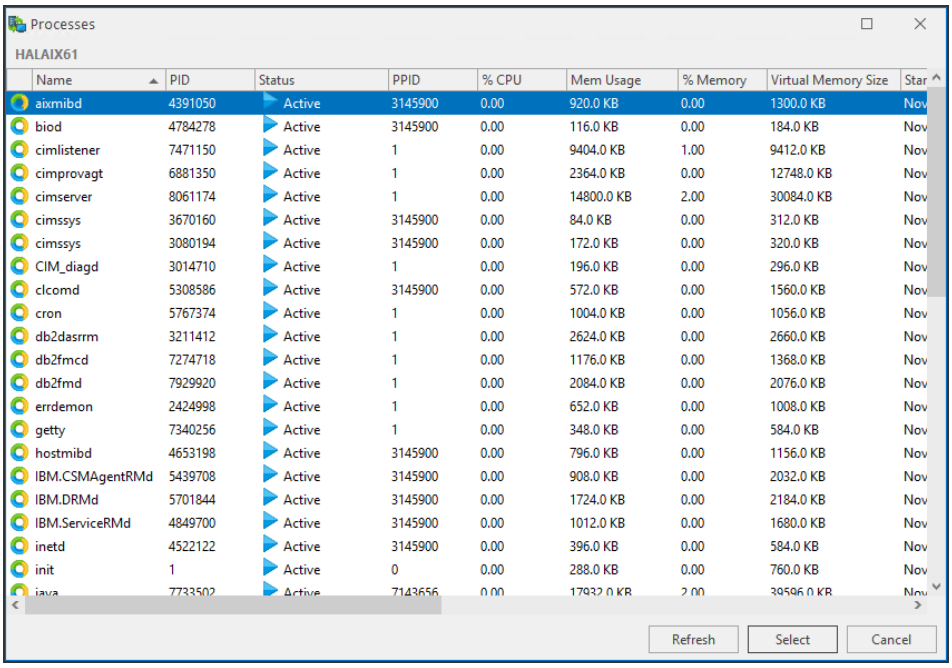
> NOTE: In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to the Enterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Adding AIX Process rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Process Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Process Criteria** dialog.

Rapid Method

1. From the **Process Criteria** dialog click **Browse** to open the **Processes** dialog, listing all the subsystems and status information.



2. Click on a process to highlight and then click **Select**.

   The Process Parameters for this criteria are automatically populated with the data from the selected process.

In-depth Method

There are three pages to complete when adding AIX Process rule criteria.

Criteria page

Category section

This section defines how the process is selected.

Monitor Type

Use the drop-down menu to define the type of process to be monitored for the rule:

- **Process by PID**: The named Process Identifier (PID) is monitored.
- **Process by Name**: The process is monitored by name.
- **Process by Owner**: The process is monitor by owner.

> NOTE: Subsequent fields and values change dependent on the selection made in this field.

Alert If

From the drop-down menu select the method by which an alert is triggered for this rule.

- **Process Exists**: An alert is triggered if the process exists.
- **Process Does Not Exist**: An alert is triggered if the process does not exist.
- **If Criteria Triggers**: An alert is raised if other criteria for this rule are triggered.

Instance section

This section defines how process name or owner is defined. If the **Monitor Type** is **Process by PID**, enter the PID into the Instance field

Process Name (Owner)

Use the drop down menu to select whether the process name or owner is defined by the use of wildcards '*' and '?' or by Regular Expression (Regex).

Trigger section

This section defines the unit of measure and how actions are performed.

> NOTE: This only applies if the **Alert If** parameter is set to **If Criteria Triggers**.

Measure

Use the drop-down menu to determine how the criteria is measured for this process rule.

- **CPU Usage %**: The selected process is measured against Used CPU %.
- **Cumulative CPU Time**: The selected process is measured against Cumulative CPU Time used (in seconds).
- **Number of Processes**: The selected process is measured against the number of this process running,
- **Process Physical Memory Used %**: The selected process is measured against the amount of physical memory used expressed as a percentage.
- **Process Physical Memory Used**: The selected process is measured against the actual amount of process physical memory used
- **Elapsed Time**: The selected process is measured against an elapsed time period which can be defined as seconds, minutes or hours
- **Virtual Memory Size**: The selected process is measured against the Virtual Memory Size, which can be defined in Bytes, Kilobytes, Megabytes or Gigabytes.

Trigger Value

Specify a comparator, value and if available for the selected measure the unit value fro the threshold.

Perform Actions For:

If the criteria is set to **perform actions for the first triggered instance**, any resulting alert contains a summary of the instances that breached the criteria threshold. If it is set to **perform actions for all triggered instances,** then an alert is raised for each instance containing only details of that particular instance.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Testing

Once the Subsystem parameters have been defined for the criteria, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to confirm the entered parameters as criteria for this rule.

AIX Ping Monitor

The AIX Ping Monitor checks the status of remote devices by sending an Internet Control Message Protocol (ICMP) ping. The number of ping attempts per device and success percentage can be specified. An alert is raised if success percentage falls below threshold.

Adding AIX Ping Monitor rule criteria

1. From the AIX system in the Systems panel of Central Configuration Manager, select **AIX Ping Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Ping Criteria** dialog.

There are three pages to complete when adding AIX Ping rule criteria.

Criteria page

Ping Destination section

The fields in this section define the Ping destination configuration parameters.

Host /Address

Enter the Host name or IP Address of the Ping destination to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Timeout

Specify the timeout, in milliseconds, after which a ping command to the specified server is deemed unsuccessful. The default setting is 2000 milliseconds.

Ping Parameters section

The fields in this section specify the configuration of the ping command. These settings work together to define whether an alert is generated.

Ping Attempts

Defines how many attempts are made before an alert is generated. The default setting is 4.

Success Percentage

This setting gives the required percentage of ping success rate before an alert is generated. The default setting is 50%

Time-to-Live

This setting defines for how long the ping is active. The default setting is 128 milliseconds.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click  to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Testing

When you have entered the criteria that you require, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define the entered parameters as criteria for this rule.

Linux Monitors

The Linux Server Manager monitors check specific elements of any licensed Linux system and loaded into Network Server Suite via the Device Manager. The Linux Monitors work in the same way as the Windows Monitors, in that rules are created, criteria specified and actions set.

The following monitors are available for the specific monitoring of Linux Servers.

Linux Logical Volume Monitor

The Linux Logical Volume Monitor checks the status of Logical Groups, Logical Volumes and Physical Volumes of the Linux system. Alerts are raised if the criteria exists, does not exist or triggers a pre-defined value. The current status of the Logical Groups, Logical Volumes and Physical Volumes can be displayed when setting the rule criteria. A test facility is also available that allows the pre-testing of the rule with the current criteria settings and make amendments as required based on the received results.

Script Monitor

The Linux Script Monitor runs custom Linux scripts and commands and checks the output against Regular Expressions.

File & Folder Monitor

The Linux File & Folder Monitor checks Linux files and folders for existence, non-existence or for any physical changes. Alerts are raised if any of the selected conditions are proven or for any changes in selected folders and/or files.

For example, when a new file is created in a folder or when the size of a file changes. This is useful for ensuring that critical files are not deleted.

Log File Monitor

The Linux Log File Monitor checks the standard Linux Event Logs. New events in the log can be filtered and alerts raised accordingly. Rule criteria use Regular Expressions to filter information. Regular expressions allow you to select specific strings from a set of character strings.

CPU, Filesystem & Memory Monitor

The Linux CPU, Filesystem & Memory Monitor gives administrators the ability to monitor the CPU, Filesystem and Memory statistical data of any Linux system loaded into the Central Configuration Manager.

System Monitor

The Linux System Monitor checks system load average over a pre-defined time period. Alert raised if load exceeds, equals or falls short of user-defined criteria.

The System Monitor can also monitor the system up-time of Linux device.

Process Monitor

The Linux Process Monitor checks Linux system processes by a series of processor measurements, such as CPU Usage %, Cumulative CPU Time and so on. Alerts are raised when a process triggers a pre-defined value.

Ping Monitor

The Linux Ping Monitor checks the status of remote devices by sending an ICMP ping. The number of ping attempts per device and success percentage can be specified. An alert is raised if success percentage falls below threshold.

Linux Actions

Only three actions are available when creating Linux Monitor rules:

- Execute Command action
- Send Enterprise Console Alert action
- Send Instant Alert Message action

See Adding Rule Actions for more information on these three action types.

Linux Logical Volume Monitor

Linux uses a Logical Volume Manager (LVM) to manage, at a logical level, all of the file systems and directories created within an Linux system. The LVM maps data between logical and physical storage, allowing data to be non-contiguous, span multiple disks, flexible and dynamically expanded.

The Linux Logical Volume Monitor checks the Volume Group, Physical Volumes and Logical Volumes of the Linux system as defined in the LVM.

- **Volume Groups**: The containers for both the Physical and Logical Volumes
- **Physical Volumes**: The Physical Volumes are segmented into physical partitions
- **Logical Volumes**: The Logical Volumes are logical partitions logged to the physical partitions

Rule criteria change depending on the type of logical volume being monitored. However for each Monitor Type it is possible to specify if a logical volume exists, does not exist or if a performance type triggers user-defined criteria.

Specifying the instance of the Logical Volume to which this rule criteria applies allows the entry of a full path to the required instance or the use of Wildcards '*' and '?' to create a generic entry. Regular expressions can also be entered by changing the entry in the first drop down choice menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Wildcards and regular expressions can be used to create generic rules that can then be included in a template in order to monitor multiple systems.

> NOTE: In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to theEnterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Practical Examples

- A stale physical partition is a physical partition which contains data that you cannot use. Monitoring for Stale Physical Partitions alerts you when this happens so that you can take correcting action to update the stale partitions so that they contain the same information as valid physical partitions.
- Monitoring for Free Physical Partitions can alert you to when a low level of space remains on your Linux system.

Adding Linux Logical Volume rule criteria

> TIP: When setting criteria, click **Display Status** to open the **Logical Volume Status** dialog which displays the individual properties of each of the three Logical Volume monitor types and allows for more precise rule entry.

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux Logical Volume Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Logical Volume Criteria** dialog.

There are three pages to complete when adding Linux Logical Volume rule criteria.

Criteria page

Category section

This section is used to define the type of volume to monitor and the trigger criteria.

Monitor Type

Use the drop-down menu to select the type of Logical Volume to be monitored:

- Volume Group
- Physical Volume
- Logical Volume

Alert If

Select from the drop-down menu when an alert is generated.

- **Exists**: An alert is generated if the named instance exists
- **Does Not Exist**: An alert is generated if the named instance does not exist
- **Criteria Triggers**: An alert is generated if the remaining criteria are met

Instance section

This section is used to identify the actual instance of the selected Monitor Type for this rule.

Logical Volume/Physical Volume/Volume Group

Use the first drop down menu to select whether the Logical Volume, Physical Volume or Volume Group is defined by the use of wildcards @*' and '?' or by Regular Expression (Regex). Use the second drop-down menu to select the required instance or enter the full path to an entry of your choice.

Trigger section

This section is used to define the Performance Type and Trigger Value for the rule criteria.

Performance Type

From the drop-down menu, select the performance type by which the Logical Volume, Physical Volume or Volume Group is measured. The selections available in the drop-down menu are dependent on the Monitor Type for which the criteria is being set.

Trigger Value

Specify the comparator (equals, greater than, less than, etc.) and enter the value threshold which if met or breached, depending on the comparator used, triggers an alert.

> **NOTE:** For Physical and Logical Volume Monitor Types, a Regex can also be used as a comparator.

Perform Actions For

If the criteria is set to **perform actions for the first triggered instance**, any resulting alert contains a summary of the instances that breached the criteria threshold. If it is set to **perform actions for all triggered instances,** then an alert is raised for each instance containing only details of that particular instance.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> **TIP:** When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Testing

Once the criteria has been set, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to define the entered parameters as criteria for this rule.

Linux Script Monitor

The Linux Script Monitor is a high-level monitor that runs a user-defined script or command against a Regular Expression.

The entered script must exist and must use the absolute path, not a relative path.

Alerts are raised if the selected Regular Expression is matched.

Adding Linux Script rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux Script Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Script Criteria** dialog.

There are three pages to complete when adding Linux Script rule criteria.

Criteria Page

Script Parameters section

This section defines how the command or script to be run and Regular Expression used.

Command/Script

Type the command or script to be run.

Regular Expression

Enter the details of the Regular Expression against which the command or script is run. The default entry is '.+'.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

Advanced Settings section

Omit Lines Containing Script Process Id From Results

Select this option to remove any lines that contains the ID of the script process that was used to generate the result. This prevents any false results being generated by the process that is performing the actual monitoring.

Testing

Once the Subsystem parameters have been defined for the criteria, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to define and confirm the subsystem parameters as criteria for this rule.

Linux File & Folder Monitor

The Linux File and Folder monitor allows the browsing of both local and remote Linux devices for a specific folder and check for any changes.

Adding Linux File & Folder rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux File & Folder Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **File & Folder Criteria** dialog.

There are four pages to complete when adding Linux File & Folder rule criteria.

Criteria page

Location section

The field in this section is used to determine the path to the required File or Folder.

Search Path

Either type the path to the required folder or file directly into this field or click ... **Browse** to open the **Select Folder** dialog. This allows the selection of any folder from the Linux device and the subsequent drill-down into subsequent folders.

Search Parameters section

The fields in this section specify the alert criteria and trigger actions.

Alert If

Select whether an alert should be generated if the File/Folder does or does not exist. Check the **Include Sub-Folders** option to ensure that the Linux sub-folders are included in any search.

Trigger On

Trigger actions are used to determine at which point the alert is raised and can be set against events happening against individual files, folders or file or folder.

- **First Matching**: The alert is triggered on the first matching instance of the File, Folder or File or Folder found.
- **Each Matching**: Separate alerts are triggered for each matching instance found for each File, Folder or File or Folder found.

Scan Filters section

Scan filters allow you to include or exclude specific criteria on which to search.

Include/Exclude Filters

Include and Exclude Filters allow you to enter a list of files or folders to include or exclude from the scan. Wildcards (*) can be used as a full or part replacement for file/folder name characters. When inserting file/folder names, use carriage return to generate a new line on which the next file/folder name can be entered.

Permission Filters section

Permission Filters allow you to specify the access rights to the files/folders for which you are scanning. The permission filters are split into three types:

- **User**: The owner of the file or folder
- **Group**: The group to which the owner belongs
- **Other**: Everyone else

Permission levels allow to you define, within each type, whether the file can be read, written or executed, by specifying:

- **Granted**: Permission allowed
- **Not Granted**: Permission denied
- **Both**: Permission is not checked

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Thresholds page

File Size Threshold section

The File Size Threshold is used to specify criteria that trigger an alert if the file size equals, exceeds, falls below or does not equal the entered value.

Size

Click to enable the setting of a file size threshold. Then select the comparator, enter a value and select the unit of measurement. The file size can be specified in:

- Bytes
- Kilobytes
- Megabytes
- Gigabytes
- Terabytes

Timestamp Thresholds section

This section contains fields to specify a time period or a specific time and date at which the file was modified.

Modified

Click to enable the setting of a time period or specific date and time at which the file was modified.

To specify a time period, click the top radio button and select a comparator, value and time period. The time period can be specified in:

- Seconds
- Minutes

- Hours
- Days

To specify an actual date and time, click the bottom radio button and select a time preposition, date and time at which the file was modified. The time preposition can be specified as:

- At
- After
- On Or After
- Before
- On or Before
- Not At

User Filters section

This section is used to filter the results by user or group.

User Name

Enter a user name by which the threshold results are filtered.

Group Name

Enter a Group Name by which the threshold results are filtered.

> NOTE: When entering User Filters of **User Name** and **Group Name**, you must enter the actual names and not their numerical representations.

Advanced page

Firewall Settings section

This section contains fields that enable and then specify the parameters required for the use of a firewall proxy.

Enable Firewall Proxy

Click to enable the use of a Firewall Proxy when connecting to a remote device.

Host /Address

Enter the Host name or IP Address of the Firewall Proxy to be used in this rule.

Port Number

Select the Port Number on which the connection to the Firewall Proxy is made. The default setting is 8080.

User Name

If the firewall proxy requires authentication, enter a valid user name.

Password

If a user name has been entered, enter the associated password in this field.

Testing

When you have entered the criteria that you require, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define the entered parameters as criteria for this rule.

Linux Log File Monitor

The Linux Log File Monitor discovers and monitors log files. When criteria are added, the monitor searches the Unix Syslog configuration file (/etc/syslog.conf) and examines the /var/log/directory and its subdirectories for plain files.

Log File Monitors can raise alerts for each new line of text that is added to the file that matches both the comparison and Regular Expression criteria.

Adding Linux Log File rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux Log File Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Log File Criteria** dialog.

There are two pages to complete when adding Linux Log File rule criteria.

Criteria page

Log File Parameters section

This section is used to specify the Log File to be monitored and the Regular Expression criteria.

Log File

This field is used to define the Log File for the rule. Either type the directory path into the field or use the drop-down menu to select a log file from those already discovered on the Linux system. Click ... **Browse** to open the **Select File** dialog which allows navigation to a directory path and log file.

Expression

Enter the expression against which this log file is checked. The default entry is '.+'.

Browse

Click **Browse** to view the most recent entries in each log file. Selecting an entry from within this dialog, automatically enters it as the Expression criteria for the current rule.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click ? to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Click **OK** to define the entered parameters as criteria for this rule.

Linux CPU, Filesystem & Memory Monitor

The Linux CPU, Filesystem and Memory Monitor operates in the same way as the Windows CPU, Disk & Memory Monitor and is used to check common attributes of system performance.

CPU Monitor

The CPU monitor is used to monitor either the load or the spare capacity of the machine's CPU. Use the Performance Data feature to obtain a current 'snapshot' of the system on which threshold decisions can be made.

An alert is triggered when the entered percentage is reached or equaled.

> **NOTE:** A CPU Load greater than 100% is allowed when totaling up across devices. For example, if a single device has multiple processors.

Filesystem Monitor

The Filesystem monitor is used to monitor both Drive Space and I-Node usage. An I-Node is a data structure on a file system on Linux and other Unix-like operating systems that stores all the information about a file except its name and its actual data.

A data structure is a way of storing data so that it can be used efficiently. Different types of data structures are suited to different types of applications, and some are highly specialized for specific types of tasks.

Drives and I-Nodes can be monitored by physical or percentage space available or by space used.

An alert is triggered when the selected criteria value for the required drive and Performance Type is reached. Alternatively, alerts can be raised if the drive exists or does not exist.

When the instance of the Filesystem volume to which this rule criteria applies is specified, a full path to the required instance can be entered or Wildcards '*' and '?' used to create a generic entry.

Regular expressions can also be entered by changing the entry in the first drop down choice menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Using wildcards and regular expressions allow the creation of generic rules that can then be included in a template in order to monitor multiple systems.

> **NOTE:** In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to the Enterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Memory Monitor

The Linux Memory monitor is used to monitor different aspects of the memory usage of the Linux device. Physical memory, virtual memory, page file, memory load and buffers used can all be monitored and alerts raised when specific trigger value targets are reached.

Adding Linux CPU Filesystem & Memory rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux CPU Filesystem & Memory Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Performance Criteria** dialog.

There are three pages to complete when adding Linux CPU Filesystem & Memory rule criteria.

Criteria page

Category section

The fields in this section determine the type and trigger value of the selected area of system performance.

Performance Group

From the drop-down menu select the area of performance for which the rule is created. Select from:

- CPU
- Filesystem
- Memory

> NOTE: Further fields on this page are dependent on the selection made in this field.

Alert If

If Filesystem is selected as the Performance Group this field determines if an alert is raised based on whether the Filesystem does or does not exist or if the remaining criteria trigger.

Instance section

The fields in this section determine the instance on which the rule checks. This section is not required for Memory Performance checks.

CPU (For CPU Performance Group)

Select the CPU instance on which this rule measures performance. Select **Partition** to measure performance across the partition.

Instance (For Filesystem Performance Groups)

Select the Volume on which this rule measures performance. Select an instance from the drop-down menu, or specify an instance using either Wildcard or Regex to define the entry.

Trigger section

Fields in this section determine the trigger values on which an alert is generated.

Performance Type

From the drop-down menu select the performance type to which the rule applies.

For CPU Performance, the following choices are available:

- CPU Idle
- CPU Load

For Filesystem Performance, the following choices are available:

- Filesystem Space Available
- Filesystem Space Available %
- Filesystem Space Used
- Filesystem Space Used %
- Filesystem Space Total
- Inodes Available
- Inodes Available %
- Inodes Used
- Inodes Used %
- Inodes Total

For Memory Performance, the following choices are available:

- Buffers Used
- Memory Load
- Page File Available
- Page File Available %
- Page File Used
- Page File Used %
- Page File Total
- Physical Memory Available
- Physical Memory Available %
- Physical Memory Used

- Physical Memory Used %
- Physical Memory Total
- Virtual Memory Available
- Virtual Memory Used
- Virtual Memory Total

Trigger Value

The trigger value is used to specify a percentage value threshold at which the Performance criteria is set. The following comparators can be used:

- **=** The trigger value is exactly equal to the percentage value entered.
- **>** The trigger value is greater than the percentage value entered.
- **>=** The trigger value is greater than or equal to the percentage value entered.
- **<** The trigger value is less then the percentage value entered.
- **<=** The trigger value is less than or equal to the percentage value entered.
- **<>** The trigger value is anything other than the percentage value entered.

Trigger On

Trigger actions are used to determine at which point the alert is raised. This option is only available if Filesystem is selected in the Performance Group.

- **First Triggered Instance**: The alert is triggered on the first matching instance found.
- **All Triggered Instances**: A single alert is triggered with the information of up to 50 matching instances found.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

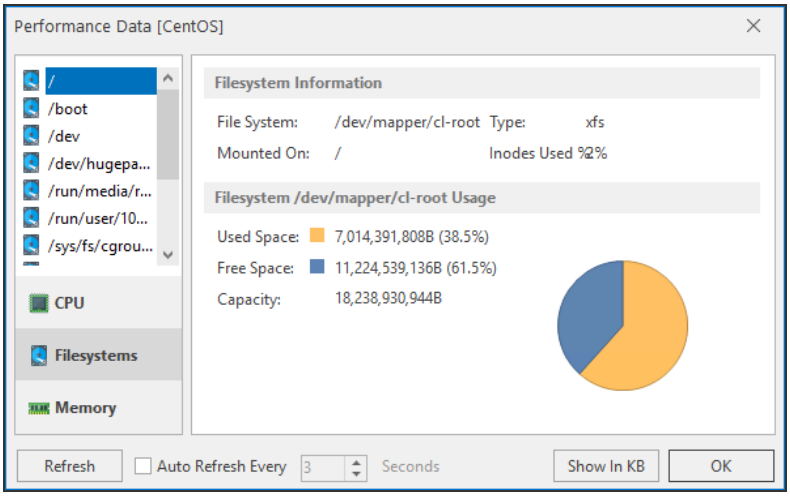
Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Using the Performance Data utility

Prior to setting any criteria for this monitor, it is advisable to use the **Performance Data** button, on the **Performance Criteria** dialog to display the current Performance Data for the chosen system.



Use the tabs in the left-hand navigation panel of this display to view the relevant performance data of each attribute of the selected system.

Refresh

Use **Refresh** to periodically update the display or set the **Auto Refresh** setting to automatically update the display every specified number of seconds.

Show in MB/KB

Data can be displayed in KB or MB. Click **Show in MB/KB** to toggle the display between size metrics.

When you have the required information, click **OK** to close the **Performance Data** dialog.

Testing

When the required criteria has been entered, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define the entered parameters as criteria for this rule.

Linux System Monitor

Load averages are a simple measure of the number of processes that are ready to run but required to wait for access to the CPU. A load average of more than two on a system with a single CPU, for example, would indicate that the system is unable to keep up with the processes that are being submitted.

Load average represents the load averages over 1, 5, and 15-minute intervals prior to a server's transmission. The load averages are multiplied by 10 to represent the value in decimal format.

An alert is sent when the trigger value for the condition is breached.

Adding Linux System rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux System Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **System Criteria** dialog.

There are three pages to complete when adding Linux System rule criteria.

Criteria page

Category section

The fields in this section are used to determine the unit of measure.

Measure

Select the unit of measure against which to test the load average.

- **Load Average Over Past 1 Minute**
- **Load Average Over Past 5 Minutes**
- **Load Average Over Past 15 Minutes**
- **System Up Time**: The Load Average is taken against the time that the system has been running.

Trigger section

Sets the trigger value for this criteria.

Trigger Value

From the drop-down list select the comparator and enter the trigger value against which the criteria is set.

For System Up Time rules, specify a trigger value for Seconds, Minutes or Hours.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Testing

When the required criteria has been entered, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define and confirm the entered parameters as criteria for this rule.

Linux Process Monitor

The Linux Process Monitor is used to monitor all processes running on the Linux system. Processes can be monitored by Process Name, Process Owner or Process Identification Number (PID). You can select to generate alerts based on whether the process does or does not exist or if it is triggered by the rule criteria.

When you specify the instance of the Process to which this rule criteria applies, you can enter a full path to the required instance or use Wildcards '*' and '?' to create a generic entry. Regular expressions can also be entered by changing the entry in the first drop down choice

menu from Wildcard to Regex and entering a valid Regular Expression in the second drop-down choice menu.

Using wildcards and regular expressions allow you to create generic rules that can then be included in a template in order to monitor multiple systems.

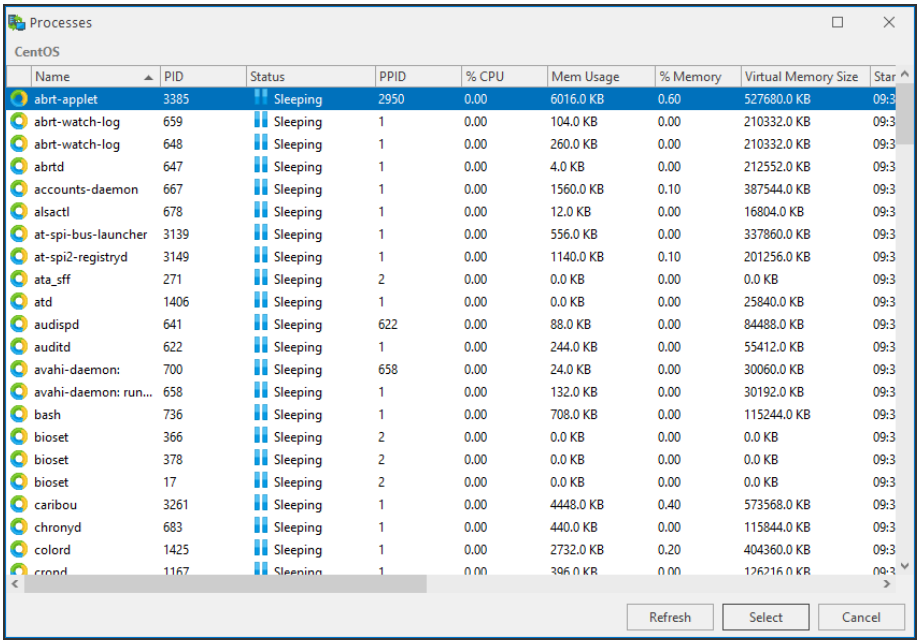
> **NOTE:** In previous versions of Network Server Suite, defining an instance that was not subsequently found by the rule criteria resulted in an error being sent to the Enterprise Console. Due to the methodology used in processing Wildcard and Regular Expression entries, this no longer happens. It is recommended that you define specific 'Does Not Exist' rules to raise an alert in these circumstances.

Adding Linux Process rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux Process Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Process Criteria** dialog.

Rapid Method

1. From the **Process Criteria** dialog click **Browse** to open the **Processes** dialog, listing all the subsystems and status information.



2. Click on a process to highlight and then click **Select**.

   The Process Parameters for this criteria are automatically populated with the data from the selected process.

In-depth Method

There are three pages to complete when adding Linux Process rule criteria.

Criteria page

Category section

This section defines how the process is selected.

Monitor Type

Use the drop-down menu to define the type of process to be monitored for the rule:

- **Process by PID**: The named Process Identifier (PID) is monitored.
- **Process by Name**: The process is monitored by name.
- **Process by Owner**: The process is monitor by owner.

> NOTE: Subsequent fields and values change dependent on the selection made in this field.

Alert If

From the drop-down menu select the method by which an alert is triggered for this rule.

- **Process Exists**: An alert is triggered if the process exists.
- **Process Does Not Exist**: An alert is triggered if the process does not exist.
- **If Criteria Triggers**: An alert is raised if other criteria for this rule are triggered.

Instance section

This section defines how process name or owner is defined. If the **Monitor Type** is **Process by PID**, enter the PID into the Instance field

Process Name (Owner)

Use the drop down menu to select whether the process name or owner is defined by the use of wildcards '*' and '?' or by Regular Expression (Regex).

Trigger section

This section defines the unit of measure and how actions are performed.

> NOTE: This only applies if the **Alert If** parameter is set to **If Criteria Triggers**.

Measure

Use the drop-down menu to determine how the criteria is measured for this process rule.

- **CPU Usage %**: The selected process is measured against Used CPU %.
- **Cumulative CPU Time**: The selected process is measured against Cumulative CPU Time used (in seconds).
- **Number of Processes**: The selected process is measured against the number of this process running,
- **Process Physical Memory Used %**: The selected process is measured against the amount of physical memory used expressed as a percentage.
- **Process Physical Memory Used**: The selected process is measured against the actual amount of process physical memory used
- **Elapsed Time**: The selected process is measured against an elapsed time period which can be defined as seconds, minutes or hours
- **Virtual Memory Size**: The selected process is measured against the Virtual Memory Size, which can be defined in Bytes, Kilobytes, Megabytes or Gigabytes.

Trigger Value

Specify a comparator, value and if available for the selected measure the unit value fro the threshold.

Perform Actions For:

If the criteria is set to **perform actions for the first triggered instance**, any resulting alert contains a summary of the instances that breached the criteria threshold. If it is set to **perform actions for all triggered instances,** then an alert is raised for each instance containing only details of that particular instance.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

NOTE: SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Ignore Instances section

This field is used to define any instances that can be ignored by the rule.

Click **Add** to open the **Add Instance** dialog. Type the name of the instance to be ignored and click **OK**. Wildcards '*' and '?' can be used to create the entry. Multiple ignored instances can be added to a single rule.

Testing

Once the Subsystem parameters have been defined for the criteria, click **Test** to ensure that the returned results are the same as would be expected if the rule was live.

Click **OK** to confirm the entered parameters as criteria for this rule.

Linux Ping Monitor

The Linux Ping Monitor checks the status of remote devices by sending an Internet Control Message Protocol (ICMP) ping. The number of ping attempts per device and success percentage can be specified. An alert is raised if success percentage falls below threshold.

Adding Linux Ping Monitor rule criteria

1. From the Linux system in the Systems panel of Central Configuration Manager, select **Linux Ping Monitor** and click **Add Rule**.
2. From the **Add Rule Detail** dialog, click **Criteria**. Click **Add Criteria** to open the **Ping Criteria** dialog.

There are three pages to complete when adding Linux Ping rule criteria.

Criteria page

Ping Destination section

The fields in this section define the Ping destination configuration parameters.

Host /Address

Enter the Host name or IP Address of the Ping destination to be used in this rule. This is set to the localhost 127.0.0.1 by default.

Timeout

Specify the timeout, in milliseconds, after which a ping command to the specified server is deemed unsuccessful. The default setting is 2000 milliseconds.

Ping Parameters section

The fields in this section specify the configuration of the ping command. These settings work together to define whether an alert is generated.

Ping Attempts

Defines how many attempts are made before an alert is generated. The default setting is 4.

Success Percentage

This setting gives the required percentage of ping success rate before an alert is generated. The default setting is 50%

Time-to-Live

This setting defines for how long the ping is active. The default setting is 128 milliseconds.

Alert page

Criteria Alert Details section

Fields in this section define alert settings that override the settings made on the Alert page at Rule level. This provides a more criteria specific alert message to be generated.

Override Rule Default

Click **Override Rule Default** to specify that the entries on this page override the default Alert page settings at Rule level. From the drop-down menu, select the alert warning level.

Alert Text

Enter the actual text of the alert or use the available Substitution Variables to construct the message text of the alert.

> TIP: When Substitution Variables are used, click to display a list of textual and numeric parameters that can be used to amend the actual Substitution Variable value.

Alert Example

Displays an example of how the Alert Text will read using the selected Substitution Variables and user-entered text.

Advanced page

SLA Statistic section

Fields in this section are used to indicate that the criteria for this rule are used to determine performance against Service Level Agreements (SLA).

SLA Statistic

Click the SLA Statistic field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> TIP: If multiple SLA flags are being set for different criteria and/or monitors, we recommend that a Send Enterprise Console alert action is created to determine which of the SLA criteria has failed.

> **NOTE:** SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).
>
> We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.
>
> System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Testing

When you have entered the criteria that you require, click **Test** to assess the validity of the data, and if necessary make any changes prior to putting the rule 'Live'.

Click **OK** to define the entered parameters as criteria for this rule.

Business Software Monitors

These monitors are not included in the standard release of Network Server Suite but are fully compatible with the software. These monitors can be purchased for an additional license fee.

Please contact: halcyon.sales.admin@fortra.com for more information.

> **NOTE:** If you have not purchased an additional license, the Business Software Monitors are not displayed in the Systems view of Central Configuration Manager.

Web Application Monitor

The Web Application Monitor is used to check the status of web page data and data within programs that use websites to display information, for example IBM Blade Center information or Infor M3 (Movex) applications.

> **NOTE:** A separate user manual is available for the Web Application Monitor.

SNMP Monitoring

Simple Network Management Protocol (SNMP) is an 'Internet-standard' protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers and so on.

Each SNMP device is capable of sending 'traps', pockets of information that provide details of current operating status. For example, a network router may send a message that an invalid logon has been attempted or a printer may send a message that it is out of paper or that a ink cartridge needs replacing.

Network Server Suite is capable of monitoring these messages and sending an alert whenever an issue arises. SNMP versions 1, 2c and 3 are supported.

System Requirements:

- A license to use SNMP Traps must be included within the license code applied to the system on which SNMP Traps are being monitored.
- Devices to be monitored must exist within Device Manager.

Setting up the SNMP Device in Device Manager

1. Open the Device Manager component of Network Server Suite and add the device details. See Adding a Device for more information on how to do this.
2. Once the basic system details have been entered, select **SNMP** from side-navigation panel on the **Add Device** dialog.
3. Click **Device Is A Trap Target** to register this device as being able to send and receive SNMP Trap information.
4. Leave the **Trap Port** set to 162. Only change this value if required by your operating environment.
5. Click **OK** to add the SNMP Device.

Making a Device a SNMP Trap Target

In order that SNMP traps may be received correctly, a device must be identified as being able to handle the incoming information and process it into meaningful data. For this purpose, the Enterprise Server running on the local device must be defined as a Trap Target.

Defining the local Enterprise Server as a SNMP Trap Target

1. From within Device Manager, double-click on the local device hosting the Enterprise Server. This is normally the machine on which all of the Network Server Suite components are installed. The Edit Device dialog is displayed.
2. Select the **SNMP** tab. In the options page, if not already enabled for this device, click SNMP Capable. The **Traps** page is now available
3. Click **Device Is A Trap Target** so that it is enabled.
4. Unless required by your operating environment, leave the remaining fields on this page set to their default settings.
5. Click **OK** to set this device as a SNMP Trap Target.
6. Close **Device Manager**.

This accepts the changes made in Device Manager so that they are recognized within Enterprise Console.

Defining SNMP Settings on the SNMP Device

Nearly all SNMP devices, and it varies by device, have a SNMP Settings menu option within their web-interface configuration options. From within these SNMP Settings, the IP Address of the Enterprise Server, previously set-up in Device Manager, can be identified as the Trap Target Device.

> **NOTE:** Please refer to your individual device user reference guides and help to assist you with entering these settings.

Configuring Trap Receiver Send Intervals

By default, the Trap Receiver sends information every 60 seconds or when the batch size reaches 50 traps, whichever occurs first.

These settings can be manually reconfigured to suit specific operating requirements.

To reconfigure Trap Receiver Send Intervals (32-bit Default Install Path):

1. Open **Windows Explorer** or use Windows **Start** | **Computer**.
2. Navigate to:

```
C:\Program Files\Halcyon\Trap Receiver\TrapReceiver.exe.config
```

3. Double-click on this file to open it ready for editing (normally opens in Notepad but may open in Microsoft Visual Studio Tools for Applications if these are installed).

To reconfigure Trap Receiver Send Intervals (64bit Default Install Path):

1. Open **Windows Explorer** or use Windows **Start** | **Computer**.
2. Navigate to:

```
C:\Program Files(x86)\Halcyon\Trap Receiver\TrapReceiver.exe.config
```

3. Double-click on this file to open it ready for editing (normally opens in Notepad but may open in Microsoft Visual Studio Tools for Applications if these are installed).
4. Use **Edit** | **Find** to locate '**halcyon batchInterval="60"**'. The following should now be displayed:

5. Edit the '**halcyon batchInterval**' and '**batchSize**' fields to the new required settings.
6. Select **File** | **Save** to save the file with the new configuration settings.

Adding MIB information

Network Server Suite comes pre-supplied with MIB files; files that contain a set of definitions for each managed object. They define the data type of the object, as well as the current validity of the object.

In Network Server Suite, MIB files are used to provide detailed information regarding the SNMP Trap from which they were sent. This information is available in the details panel of any SNMP Trap alert received at the Enterprise Console for which MIB details exist.

Additional MIB files can be added to the existing database so that they build into a comprehensive knowledge base.

To add a MIB file to the existing database:

1. Select Windows **Start** | **Control Panel** | **Administrative Tools** | **Services**
2. Stop the **Halcyon Trap Receiver** service.
3. Open Windows Explorer or use Windows **Start** | **Computer**.
4. Navigate to:
   C:\Program Files(x86)\Halcyon\Trap Receiver\Mibs
5. Add any additional MIB files to this directory from the location on the network where they are currently stored.
6. Restart the **Halcyon Trap Receiver** service.

NOTE: The information contained within a MIB file may or may not be available from within Network Server Suite dependent on the construction method used to create the MIB file.

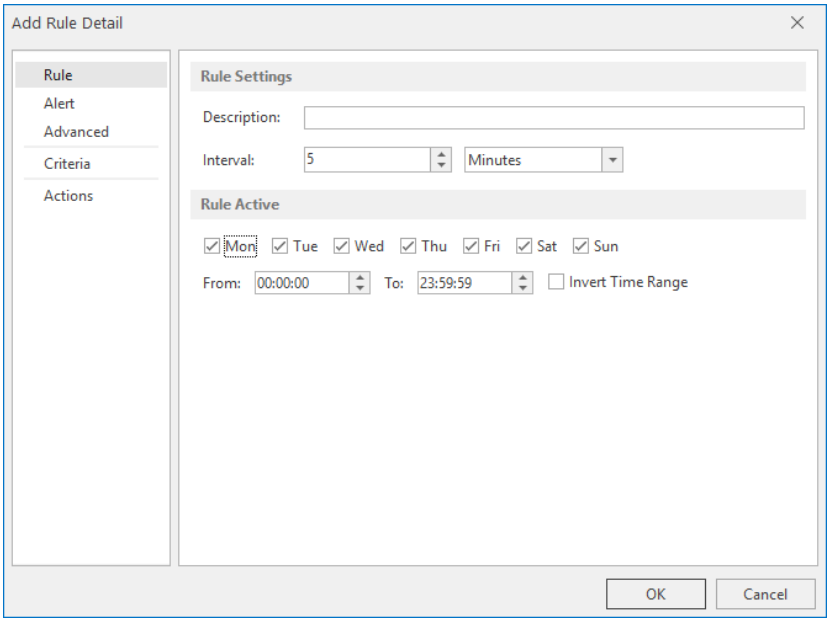
Adding Monitor Rules

Once it has been decided on the information to be monitored, or in some cases (more importantly), information that you want to ignore, the following needs to be entered:

- What needs to be monitored (full monitor descriptions can be found in the section Network Server Suite Monitors).
- The frequency with which the checks are made.

To add a monitor rule:

1. From the **Systems** panel in the left navigation pane of Central Configuration Manager, select the monitor to which the rule will be added.
2. From the **Monitor Summary** panel, click **Add Rule**, to start the process of adding rules to a selected monitor. The **Add Rule Detail** dialog is displayed.



The **Add Rule Detail** dialog contains five tabs that allow you to specify the following:

- **Rule Tab**: The Rule tab is used to specify general rule settings
- **Alert tab**: The Alert tab is used to specify the default alert detail settings
- **Advanced tab**: The Advanced tab is used to specify rule suspension settings
- **Criteria Tab**: The Criteria tab is used to specify the criteria that trigger an alert if met
- **Actions Tab**: The Action tab is used to specify the actions that occur when an alert is triggered

Rule Sequence Numbers

Each rule is given its own unique sequence number within the Monitor in which it is created.

> **NOTE:** During rule configuration you can be as simple or as complex as you wish. Rules are run in the numerical order in which they are listed under each monitor.

Adding Rules - Rule tab

The rule page is used to determine description and activity settings.

Rule Settings section

Description

Enter a description to accurately describe the purpose of this rule. The rule description is displayed in the summary page at Monitor level.

Interval

For rules where the check interval is not undertaken at Monitor level, these settings specify how frequently this individual rule runs, unless the rule is held. The time period can be defined in seconds, minutes, hours or days.

Rule Active section

Days Active

Select the days on which the rule is active. The default setting is to run on all days.

Times Active

Select the times of day between which the rule is active. The default setting is 24 hours from 00:00:00 to 23:59:59.

Invert Time Range

If a specific time range has been entered in the **Times Active** parameters, check this box to indicate the rule is active **outside** the time range indicated in the '**From**' and '**To**' parameters.

Using Inverse Time Ranges

Using Inverse Time Ranges allows the setting of different actions for the same alert or specify different criteria that cause the alert to be generated. By copying a rule it is possible to quickly create a duplicate of an existing rule and then set the inverse time range option on the copied rule.

With the Inverse Time Range set, it is possible to specify a different action when the rule criteria is activated. A possible use for this would be to send an alert to the Enterprise Console during working hours and then send an email/SMS message to an on-call support group if the rule criteria was met during the Inverse Time Range period.

Alternatively, the rule criteria can be edited, such as extending the number of times a threshold has to be broken in order for the alert to be generated. This may be required if the importance of being notified about a threshold being breached or a device being unavailable, such as a printer being offline, diminishes after the official working day has ended.

Adding Rules - Alert tab

The Alert page of the **Add Rule Detail** dialog determines the default alert settings for any alert generated by this rule.

Each rule has default alert text assigned, which can be overridden at criteria level so that the actual alert text is specific to the criteria from which it was raised.

Default Alert Details section

Alert Type

The alert type that is displayed in the event of any alert being raised by the rule. This sets the level of severity for any alerts raised by this rule. Use the drop-down choice menu to select a different alert type for this rule.

> **NOTE:** The Alert Type is automatically set to the 'Error' default for Event Log Monitors, although this can be overridden if required.

Alert Text

Substitution Variables can be used with free text to compile the alert text.

> **NOTE:** An example of what the alert text will look like if generated, is displayed as substitution variables and free text are added in the Alert Text field.

Reset

Click **Reset** to return the current **Alert Type** and **Alert Text** entries to the default settings if errors have been made when setting replacement text.

Adding Rules - Criteria tab

You now need to define the monitor specific criteria necessary to generate the alert should the terms of the criteria be met. The Criteria Summary page, displayed when you select the Criteria tab when adding a rule shows the current criteria setup for this rule.

Criteria Summary page

From this page, you can Add, Edit and Delete Rule criteria.

Each separate rule criteria is automatically assigned a unique sequence number when created. Criteria are actioned in the order sequence that they appear.

Changing the sequence of criteria

To change the criteria sequence order on this page, use the up / down arrows on the right-hand side of this display.

Criteria Description and Parameters are also shown as part of this display.

Perform Actions For Each Criteria That Triggers

When setting rule criteria it is possible to state that actions for the first, last or each criteria that triggers are performed.

- **First**: If set to **First**, the first criteria in the list that triggers (not necessarily the first criteria in the sequenced list) and the associated actions are performed. Subsequent criteria are ignored.
- **Last:** If set to **Last**, **ALL** the criteria in the list must be triggered before the associated actions are performed.
- **Each**: If set to **Each**, **ANY** of the criteria that are triggered in the rule sequence perform the associated actions. This means that the set of actions are performed each time a criteria is triggered. This can result in the actions being performed one, two, three (or however many triggered criteria there are in the rule) or not at all if none of the criteria is triggered.

> **NOTE:** This option only works for all criteria within a single rule. If there is only one criterion set per rule, then this option has no affect. Likewise, the option is not cross rule. Therefore, setting the perform actions for all matching criteria on one rule does not perform actions set on a separate rule.

Adding Rule Criteria

On the **Rule Criteria** summary page, click **Add Criteria** to open the associated **Monitor Rule Criteria** dialog.

> NOTE: The available pages and field settings are monitor specific and are covered in detail under each monitor.

Adding Rules - Advanced tab

The **Advanced** page provides options to automatically suspend the rule and reset alert counters on Startup.

Advanced Settings section

Automatically Suspend Rule

Suspending a rule means that any further alerts can be prevented from being generated by this rule while you investigate the cause. This can also prevent an unnecessary number of alerts being generated for the same reason.

When enabled, this option automatically suspends the rule once triggered either:

Until the trigger criteria has been activated a specified number of times within a determined time frame.

For an amount of time once the rule has been triggered a specified number of times. This can be set as Minutes, Hours or Days so that repetitive alerts are not generated.

The default setting suspends the rule for 30 minutes when triggered once.

Reset Counters on Startup

Enable this option to reset the alert counters when the rule restarts. This ensures any historical alerts still in the system are ignored by the monitor. A restart can be either a full system restart or when the rule is edited and then saved.

Adding Rules - Actions tab

The final step in creating a rule is to define the actions performed when the rule criteria is triggered.

TIP: A rule can have a single or multiple actions applied but at least one action must be defined per rule. For rules with multiple actions defined see Setting the order of Rule Actions.

The Actions Summary page, displayed when the Actions tab is selected during the process of adding a rule, shows the current actions setup for this rule.

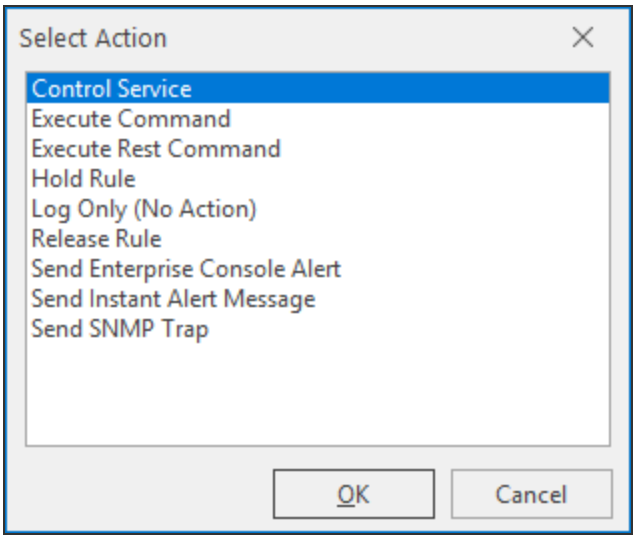
Actions Summary page

From this page, you can Add, Edit and Delete rule actions.

Each separate action is automatically assigned a unique sequence number when created. Action Description and Parameters are also shown as part of this display.

Adding Rule Actions

1. From the **Add Rule Detail - Actions** tab, click **Add Action**, to start the process of adding rules to a selected monitor. The Select Action dialog is displayed.



2. Select the action to take when the criteria is met on this rule.

   Control Service: Allows Network Server Suite to Start/Stop/Pause/Resume the selected Windows service. This option also caters for dependency and stops or restarted associated services if required.

   Execute Command: Runs a command, for example, an OS specific command or bespoke script.

   Execute REST Command: Allows a Representational State Transfer (REST) command to be run.

   Log Only (No Action): Stores the alert in the Server.hlf log file but takes no other action.

Send Enterprise Console Alert: Sends the alert to any defined instance of Enterprise Console.

Send Instant Alert Message: Sends an email (or SMS if a GSM Data Terminal is installed) to a specified recipient, call schedule or broadcast group.

Send SNMP Trap: Sends an SNMP Trap to a specified device.

Control Service Action

The Control Service action starts, stops, pauses or resumes the selected Windows service. This option also caters for service dependency and stops or restarts associated services if required.

Multiple Control Service actions can be added to a single rule to stop and restart or pause and resume a service.

Service Parameters section

Service

The Service parameter allows selection of the service to be controlled by this action.

- **Use Criteria Service**: Selects the service specified in the rule criteria as the service on which the action is performed.
- **Use This Service**: From the drop-down choice menu, select a different service, from those currently available on this device.

Action

Select the action to perform on the service. Select from **Start**, **Stop**, **Pause** or **Resume**.

Timeout

For all control actions other than **Start Service**, select the period of time, in seconds, for the selected action to be successful, after which the attempt fails. The default time period is 30 seconds.

Stop Dependent Services

If the **Stop Service** action has been selected in the **Action** parameter, check this option to also stop any other services that are dependent on the selected service running.

Click **OK** to confirm the action.

Execute Command Action

The Execute Command action invokes a command, such as running an OS Command or a bespoke script.

Command

Type the command that you wish to run once this action is invoked. Both Substitution and Environment Variables, displayed within this dialog can be used to complete the command.

Example

Displays an example of the command as it will appear.

Click **OK** to confirm the action.

Execute REST Command Action

Representational State Transfer (REST) is a software architecture style consisting of guidelines and best practices for creating scalable web services. The Execute REST Command action performs actions on these web services.

> **NOTE:** It is recommended that the web service to be monitored is running or available for view so that the parameter details can be copied accurately into the parameters of the REST Command action.

> **NOTE:** If a table value has previously been saved as a variable within the separate Web Application Monitor, this can be called as one of the parameters for a REST Command Action.

Address

Enter the address of the web server on which the service is running.

> **EXAMPLE:** https://devcms:444/

Command

Enter the command to be performed on the web service.

> **EXAMPLE:** killthread

Parameters

Use the **Add** button to enter the parameter key and value settings for each part of the command, building up the full address of the web service.

EXAMPLE:

Key	Value
addr	DEVCMS
&port	4269
&p1	13362

Request Method

Select the request method that defines what to do with the data identified by the Address, Command and Parameter fields.

- **GET**: GET is the simplest type of HTTP request method. It instructs the server to transmit the data identified by the URL to the client
- **POST**: POST is used when the processing on the server needs to be repeated if the POST request is repeated. Additionally, POST requests should cause processing of the request body as a subordinate of the URL to which the post is being made
- **PUT**: A PUT request is used to create or update the resource identified by the URL
- **DELETE**: DELETE performs the opposite of PUT and should be used to delete the resource identified by the URL of the request

Authentication

Specify whether the web server requires authentication in order for the command to be run. If authentication is required, select the **Basic Authentication** option and enter a **User Name** and valid **Password** for this server.

Rest Command Example

As details are entered into the fields in this dialog, an example of how the final command will look is displayed in this field.

Substitution Variables

Use the available substitution variables to build further identifiers and commands into the REST Command action.

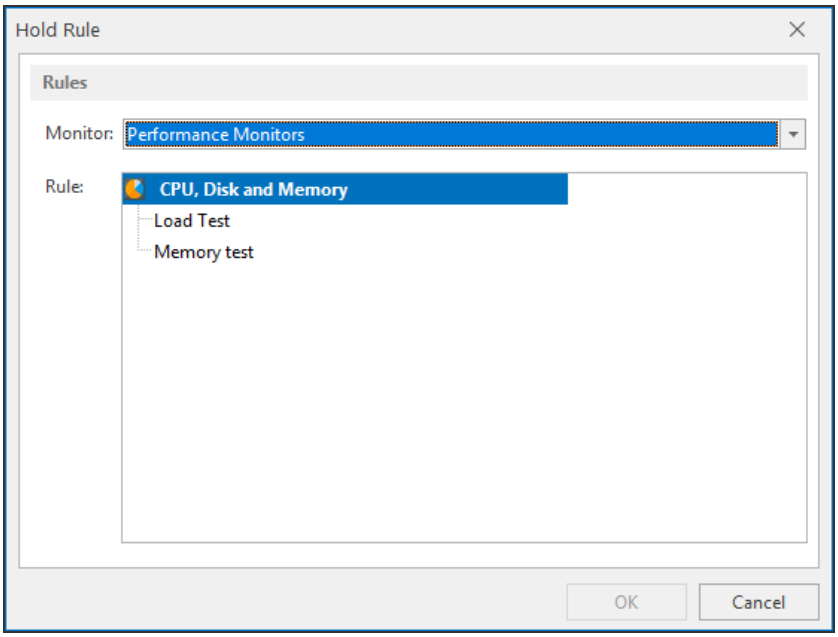
Once completed click **OK** to add the REST Command action to the rule.

Hold Rule Action

The Hold Rule action can be used to hold any other rule that has been defined.

> **NOTE:** This action cannot be used to hold the rule for which this action is being defined.

Select the **Hold Rule** action to display the **Hold Rule** dialog.



Rules Section

The options in the Rules section define the rule to be held as a result of this action being invoked.

Monitor

From the drop-down menu, select the Monitor under which the rule to be held was created.

Rule

Under the chosen Monitor is a list of all the defined rules. Select the rule to be held and click **OK**.

Whenever this rule triggers this action the selected rule will be held until a subsequent release action is triggered.

> **NOTE:** It is not possible to manually release the rule once the Hold Rule action has been applied. It must be released using a Release Rule action.

Log Only Action

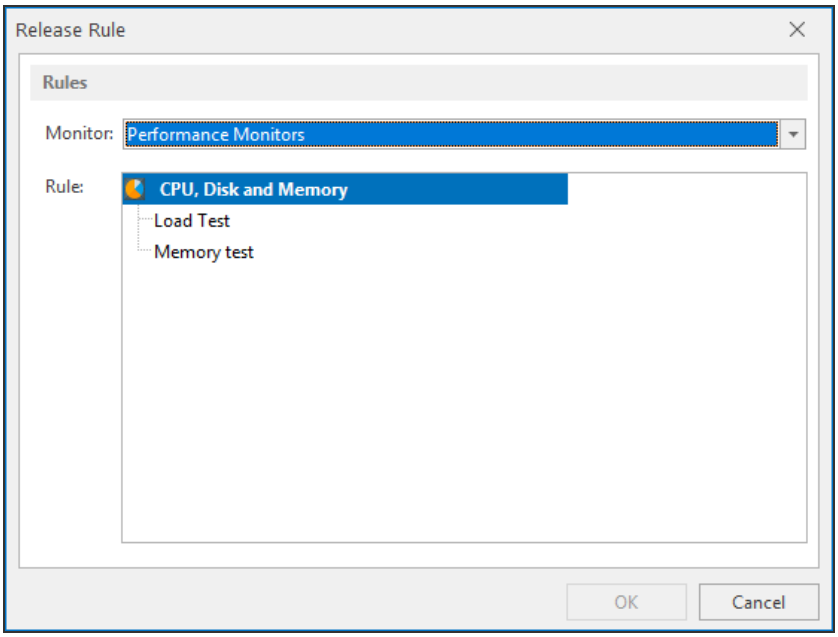
Selecting the Log Only (No Action) option, simply results in the alert being logged.

No further action is taken and subsequently there are no additional parameters to fulfill in order for the logging action to complete.

Release Rule Action

The Release Rule action can be used to release any rule that is currently held by use of the Hold Rule action.

Select the **Release Rule** action to display the **Release Rule** dialog.



Rules Section

The options in the Rules section define the rule to be released as a result of this action being invoked.

Monitor

From the drop-down menu, select the **Monitor** under which the rule to be released was created.

Rule

Under the chosen **Monitor** is a list of all the defined rules. Select the rule to be released and click **OK**.

Whenever this rule triggers this action the selected rule will be released.

> **NOTE:** If the action is applied against a rule that was not held using the Hold Rule action then it is ignored.

Send Enterprise Console Alert Action

Select the Send Enterprise Console Alert action to send the alert to any defined Enterprise Console in your network.

Alert Settings section

Include Result Information

Check this option to include in the alert details, any test information, where available, that was returned as part of the rule criteria.

Include Status Information

Check this option to include in the alert details, any status information, where available, that was returned as part of the rule criteria.

Include Rule Information

Check this option to include in the alert details, the details of the rule that caused the alert to be raised.

Enterprise Server section

In all instances where the Send Enterprise Console Alert is selected as the action, the alert is sent to the default device selected at the time when the system was added to Central Configuration Manager.

This device can be overridden for specific alerts if required, or for example, if the initial alert has not been resolved on the default device.

Override Default Device

Check to be able to select a different device, other than the default, to which to send the alert.

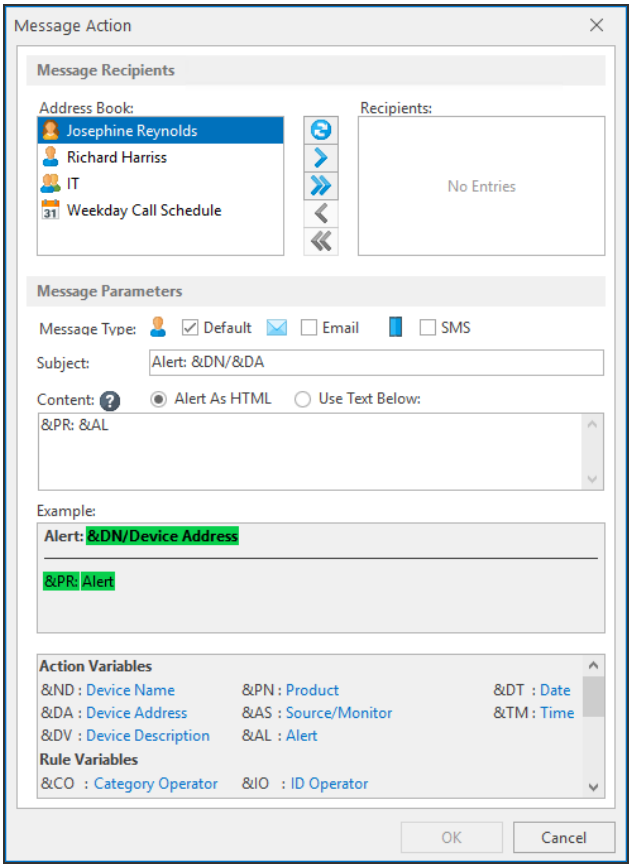
Select Server

Click to display details of other devices, which must already exist in Device Manager, to which to send this alert.

Click **OK** to confirm the action.

Send Instant Alert Message Action

This action sends a message by email, SMS or both mediums to any individual, call schedule and/or broadcast group that has been defined in the Instant Alert Address Book.



Message Recipients section

1. From the **Address Book** panel, click on the intended recipients for the message.
2. Click [›] to move the selected members to the **Recipients** panel or click [»] to move all members to the **Recipient** panel without having to select them first.

3. The < and << arrows perform the reverse action when moving members from the **Recipients** panel to the **Address Book** panel.
4. Click to refresh the contents of the **Address Book** panel, if new members have been added while the Central Configuration Manager has been active.

Message Parameters section

Message Type

Select the method to be used for the transmission of this message. Multiple selections are possible.

- **Default**: Uses the default method defined against each recipient in the Instant Alert Address Book.
- **Email**: Sends the message as an email.
- **SMS**: Sends the message as an SMS.

Subject

Specifies the subject text of the message. Substitution variables may be used in this field.

Content

Specifies the body text of the message. Substitution variables may be used in this field.

- **Alert as HTML**: Select this options to send the alert in HTML format
- **Use Text Below**: Select this option to send the alert using user-defined text entered in the Content panel. Substitution variables can be included

Example

An example view of how the message will read when sent is displayed in the **Example** panel.

Substitution Variables

Displays a list of substitution variables that can be included in the Message Text. Use the vertical scroll bar to view additional variables not visible from the initial view.

Click **OK** to confirm the action.

Send SNMP Trap Action

Select this action to send an SNMP Trap to a specified device identified as being able to accept SNMP Traps.

In all instances where Send SNMP Trap is selected as the action, the alert is sent to the default device selected at the time when the system was added to Central Configuration Manager. This device can be overridden for specific alerts if required, or for example, if the initial alert has not been resolved on the default device.

SNMP Trap Options section

SNMP Trap Target section

Select Target

Click to display details of other devices, which must already exist in Device Manager and be defined as a Trap Target device, to which to send this alert.

Click **OK** to confirm the action.

Setting the order of Rule Actions

Once the rule actions have been determined it is possible to re-sequence the order in which they are processed.

In the **Actions For Rule** panel, click to highlight the required action then click either the up or down arrow to move one place in the chosen direction. If either the first or last action in the list is selected, only the arrow in which the action may be moved is available.

When the all the required actions have been added, click **OK** to complete the creation of the rule and return to the main Central Configuration Manager display.

> WARNING: Remember to save the settings using the **Save** icon prior to exiting Central Configuration Manager.

Templates

Templates are designed to provide the same level of monitoring across a number of similar devices by applying a set of user-defined rules with a single-click. This greatly reduces set-up time and ensures all systems are covered by at least a basic level of monitoring. Should it be necessary to make a system-wide change at a later date, a single update covers all systems using the template.

Network Server Suite comes supplied with default monitoring templates for all three operating systems that cover the majority of everyday scenarios that your organization is likely to encounter. A reporting template is also included.

Windows Templates

The following Windows templates are shipped with Network Server Suite by default:

- Active Directory
- Advanced Reporting (Data Warehouse)
- Exchange Server (Performance)
- Exchange Server (Services)
- HP Data Protector
- IIS (Data Warehouse)
- Infor M3 Grid Monitoring
- JAMS
- Lawson Movex ServerView Monitoring
- Oracle JDE EnterpriseOne
- Server Performance (Advanced)
- Server Performance (Standard)
- SQL Server
- Symantec Backup Exec
- Symantec NetBackup
- Terminal Services
- Windows Update

AIX Templates

The following AIX templates are shipped with Network Server Suite by default:

- Advanced Reporting (Data Warehouse)
- Oracle JDE EnterpriseOne
- System Monitoring (Advanced)
- System Monitoring (Standard)
- Temenos T24
- VIOS

Linux Templates

The following Linux templates are shipped with Network Server Suite by default:

- Advanced Reporting (Data Warehouse)
- Oracle JDE EnterpriseOne
- Oracle Linux System Monitoring (Advanced)
- Oracle Linux System Monitoring (Standard)
- Red Hat System Monitoring (Advanced)
- Red Hat System Monitoring (Standard)
- SUSE System Monitoring (Advanced)
- SUSE System Monitoring (Standard)

Templates are created using the Central Configuration Manager and can then be quickly applied to all systems. More than one template can be applied to a system at any one time and it is also possible to have individual rules running alongside the templates on any system.

Basic templates which monitor devices for routine issues and concerns such as low disk space, memory and so on can be deployed enterprise-wide. Business critical machines may require the application of an ‘advanced’ template additionally covering, for example, application event log and service monitoring.

Additionally, templates can be created and applied to cover the generic performance reporting of systems in your enterprise. See Reporting Templates for more information on creating and applying reporting templates.

Templates are designed to provide the same level of monitoring across a number of similar devices by applying a set of user-defined rules with a single-click. This greatly reduces set-up time and ensures all defined systems are covered by at least a basic level of monitoring. Should a system-wide change be needed at a later date, a single update covers all systems using the template.

Select the **Templates** tab in the left-hand navigation panel of the Central Configuration Manager to display the currently defined templates that are available.

It is possible to open a template from either the left-hand or right-hand pane of this screen.

See Applying Templates for further information on how to use these templates across your network.

Applying Templates

Once a template has been created it can then be applied to other systems via the Templates tab of the Central Configuration Manager.

Templates can be applied directly to each system shown in the Template Systems panel.

To apply a template:

1. From the left-hand navigation panel of Central Configuration Manager, select the **Templates** tab.
2. Expand the view of the operating system to which the template will be applied.
3. From the list of templates, select the template to be applied. Upon clicking the template, all systems that have been defined for the chosen operating system are displayed in the **Template Systems** panel.
4. Click the check box next to each system to which the template is to be applied.
5. Click  **Save** to confirm and save the template settings to the selected systems.

Once saved, the System to which the template has been applied is shown in bold type to Server Manager Level only. Individual monitors and rules remain in light face.

Copy and paste

This short-cut is used primarily to copy an individual system rule into an existing template. It is only possible to do this between same type monitors (with the exception of Event Log Monitors). For example, a Summary Performance Monitor rule can only be copied to a Summary Performance Template.

Modifying Individual Systems

Once a template rule has been applied it is important to ensure that the rule details are applicable to the new system in terms of level of criteria and actions undertaken. It is good housekeeping to keep the template rules as generic as possible and fine-tune them individually at system level.

For example, a rule applied across twenty systems with an action of sending a SMS message, initiates twenty identical messages to the same resource should an alert be raised.

Exporting and Importing Templates

Templates can be exported to and imported from other instances of Network Server Suite. Template files are saved with an extension of .csf.

Exporting and Importing Template options are accessed from the Central Configuration Manager quick access bar. Use **Export Templates** or **Import Templates** .

> **NOTE:** Imported Templates do not override any existing templates on the system to which they are imported but add additional templates that did not previously exist.

Deleting Templates

Click **Delete Template** from the **Home** | **Systems** panel of the Central Configuration Manager, Once a template is deleted it is removed from all systems to which it has been applied.

Windows Active Directory template

Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables inter-operation with other directories. Active Directory is designed especially for distributed networking environments.

Performance Monitors - WMI Monitor

The Windows Active Directory template contains the following generic WMI performance rules:

- **Counter(DRA Inbound Bytes Total/sec) Trigger(>=1)**
- **Counter(DRA Inbound Object Updates Remaining in Packet) Trigger(>=5)**
- **Counter(DRA Outbound Bytes Total/sec) Trigger(>=10240)**
- **Counter(DRA Pending Replication Synchronizations) Trigger(>=50)**
- **Counter(DS Name Cache hit rate) Trigger(<=99)**
- **Counter(LDAP Client Sessions) Trigger(>=250)**
- **Counter(NTLM Authentications) Trigger(>=100)**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Exchange Server (Performance) template

This template covers the performance of the Exchange Server, including mail server, email client and groupware applications (such as shared calendars).

Performance Monitors - WMI Monitor

The Exchange Server (Performance) template contains the following generic WMI performance rules:

- **Counter(Active User Count) Trigger(>=200)**
- **Counter(Messages/Sec) Trigger(>=10)**
- **Counter(Work Queue Length) Trigger(>=10)**
- **Instance(_Total) Counter(Average Delivery Time) Trigger(=10,000,000)**
- **Instance(_Total) Counter(Send Queue Size) Trigger(>=20)**
- **Instance(_Total) Counter(Send Queue Size) Trigger(>=10)**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Exchange Server (Services) template

This template covers services used by Exchange Server.

System Monitors - Service Monitor

The Exchange Server (Services) template contains seven system service rules:

- **Service(Microsoft® Exchange IMAP4) Status(<> 'Started') Startup(= Automatic) Logon A/C(='Local System')**
- **Service(Microsoft® Exchange Information Store) Status(<>'Started') Startup('Automatic') Logon A/C('Local System')**
- **Service(Microsoft® Exchange Management) Status(<>'Started') Startup (= 'Automatic') Logon A/C('Local System')**
- **Service(Microsoft® MTA Stacks) Status(<>'Started') Startup(= 'Automatic') Logon A/C('Local System')**
- **Service(Microsoft® Exchange POP3) Status(<>'Started') Startup ('Automatic') Logon A/C('Local System')**
- **Service(Microsoft® Exchange Routing Engine) Status(<>'Started') Startup (= 'Automatic') Logon A/C('Local System')**
- **Service(Microsoft® System Attendant) Status(<>'Started') Startup (= 'Automatic' Logon A/C('Local System')**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows HP Data Protector template

HP Data Protector software is automated backup and recovery software for single-server to enterprise environments, supporting disk storage or tape storage targets. It provides cross-platform, online backup of data for Microsoft Windows, Unix, and Linux operating systems.

The HP Data Protector template contains the following components:

Event Log Monitors (Standard) - Application Event Log

Contains the following rules:

- **15 Minute Backup Check - Source('Data Protector') Category('None') ID('1') User('N/A) Message('*SQL 15 Minute A*Backup Statistics***

- Backup Not Completed - Example - Source(='Data Protector') Category (='None') ID('1') User('N/A') Message('*MailServer Daily*Backup Statistics*
- Backup Not Started - Example - Source('Data Protector') Category ('None') ID('1') User('N/A/) Message('*MailServer Daily*Backup session * started.*
- Backup Started - Source('Data Protector') Category('None') ID('1') User('N/A') Message('*Backup session * started.*')
- Critical BSM Errors - Source('Data Protector') Category('None') ID('1') User('N/A') Message('[Critical] From: BSM*')
- Finished Backups - Source('Data Protector') Category('None') ID('1') User('N/A') Message('*Backup Statistics*Failed Disk Agents 0*Failed Media Agents 0*')
- Preview Started - Source('Data Protector') Category('None') ID('1') User('N/A') Message('*Preview of the media in device repository*')

Performance Monitors - CPU, Disk and Memory

Contains the following rule:

- Drive C - Low Disk Space - Group(Disk) Instance(C:)Type(Drive Space Available %) Trigger(<10%)

System Monitors - File & Folder Monitor

Contains the following rule:

- DCBF Directory Size - Patch(C:\Program Files\OmniBack\db40\) TriggerOn(First Matching Matching Folder) SubFolders(True) Thresholds (Size)

System Monitors - Service Monitor

Contains the following rules:

- HP Data Protector CRS - Service(Data Protector CRS) Status(<>'Started') Startup('Automatic')
- HP Data Protector Inet - Service(Data Protector Inet) Status(<>'Started') Startup('Automatic')
- HP Data Proctector RDS - Service(Data Protector RDS) Status (<>'Started') Startup('Automatic')
- HP Data Protector UIProxy - Service(Data Protector UIProxy) Status(<> 'Started') Startup('Automatic')

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Infor M3 Grid Monitoring template

Infor Grid is a distributed application server that provides a distributed run-time environment to other applications. The distributed nature of a grid means that an instance of the Infor Grid may span multiple server machines.

The M3 Grid Monitoring template includes the following rules:

Business Software Monitors - Web Application Monitor*

Contains the following rules:

- **M3_PRD (M3BE) CPU - URL(http://localhost:36666/applications/M3BE_14.1.2-PRD/status,html) Timeout(5 Secs) TriggerType(Each Matching) TriggerObject(Row)**
- **M3_PRD (M3BE) Heap Usage - URL (http://localhost:36666/application/M3BE_14.1.2-PRD/status.html) Timeout(5 Secs) TriggerType(Each Matching) TriggerObject(Row)**
- **M3_PRD(Nodes) CPU - URL(http://localhost:36666/grid/nodes.html) Timeout(5 Secs) TriggerType(Each Matching) TriggerObject(Row)**
- **M3_PRD(Nodes0 Heap Usage - URL (http://localhost:36666/grid/nodes.html) Timeout(5 Secs) TriggerType (Each Matching) TriggerObject(Row)**
- **M3_PRD (Status) 'Errors' - (Multiple Criteria Defined)**
- **M3_PRD (Status) 'Not ok' - URL(http://localhost:36666/grid/status.html) Timeout(5 Secs) TriggerType(Each Matching) TriggerObject(Row)**
- **M3_PRD (Status) 'Not running' - URL (http://localhost:36666/grid/status.html) Timeout(5 Secs) TriggerType (Each Matching) TriggerObject(Row)**
- **M3_PRD (Status) 'Warnings' - (Multiple Criteria Defined)**

(*Only available if a Web Application Monitor license has been purchased separately).

System Monitors - Service Monitor

Contains the following rules:

- Backup Exec Services Started - Service(Backup Exec Remote Agent for Windows Systems) Status(<>'Running')
- MecService - M3 Enterprise Collaborator - Service(MECServer) Status (<>'Running')
- MapGenServer Service Started - Service(MapGenServer) Status (<>'Running')
- OpenText StreamServe Repository Server Service Started - Service (StreamServe Repository Server) Status(<>'Running')
- OpenText StreamServe Service Started - Production Environment - Service(StreamServe Prod) Status(<>'Running')
- OpenText StreamServe Service Started - Standard Environment - Service (StreamServe zSTD) Status(<>'Running')
- OpenText StreamServe Service Started - Test Envrionment - Service (StreamServe Test) Status(<>'Running')
- Print Spooler Service Started - Service(Print Spooler) Status(<>'Running')

TCP Monitors - HTTP Monitor

Contains the following rules:

- Grid: Check JVM locked - URL (http://localhost:36666/monitor.xml?category=Jvms) Timeout(5 Secs) NotInclude('status='"locked")
- Grid: Checking for looping M3 Auto Job - URL (http://127.0.0.1:6666/monitor?category=news) Timeout(5 Secs) NotInclude('Job may be looping')
- Grid: High Severity for News page - URL (http://127.0.0.1:6666/monitor?category=news) Timeout(5 Secs)
- Grid: M3 Excessive Interactive Job CPU - URL (http://127.0.0.1:6666/monitor?category=interactivejobs) Timeout(5 Secs)
- Grid: M3 Excessive Subsystem CPU - URL (http://127.0.0.1:6666/monitor?category=counters) Timeout(5 Secs)
- Grid: Supervisor Status = Critical - URL (http://127.0.0.1:6666/monitor?category=status) Timeout(5 Secs) NotInclude('supervisorStatus='"critical"')
- Grid: Transaction Server Check - URL (http://127.0.0.1:6666/monitor?category=services) Timeout(5 Secs)
- Grid: XML Autojobs count - URL (http://127.0.0.1:6666/monitor?category=autojobs) Timeout(5 Secs) Include ('"Autojobs jobs currently running in the system" count="52"')

- **Grid: XML Autojobs List - URL (http://127.0.0.1:6666/monitor?category=autojobs) Timeout(5 Secs)**
- **Grid: XML Job Queue Length > 25 - URL (http://127.0.0.1:6666/monitor?category=status) Timeout(5 Secs) Include (OneOf 'jobQueueLength=1 to 25)**

> NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows JAMS Template

JAMS centralizes batch processes and workloads that are critical to the modern enterprise. Our streamlined solutions consolidate job scheduling into a single command center – one with a wealth of automation features to execute jobs reliably and securely. The cross-platform capabilities of JAMS enable organizations to extract maximum value from IT investments in platforms and applications, both on premise and in the cloud.

Performance Monitors - WMI Monitor

The JAMS template contains the following WMI performance rules:

- **JAMS Requests MSMQ Queue Length - Instance(ij-jams02\private$\jamsrequests) Counter(Messages in Queue) Trigger(> 1000)**
- **JAMS Scheduler Time to Process Completion - Counter (Avg. time to process completion) Trigger(> 1.0)**
- **JAMS Scheduler Time to Start Entry - Counter (Avg. time to start an entry) Trigger(> 1.0)**

System Monitors - File and Folder Monitor

The JAMS template contains the following File and Folder rules:

- **JAMS Dead Man Switch - Path(C:\Program Files\MVPSI\JAMS\Scheduler\) TriggerOn(First Matching Matching File) SubFolders(True) Thresholds(Modified)**
- **JAMS Job Log Count - Path(C:\ProgramData\JAMS\Logs\) File Count (Greater Than 100000)**
- **JAMS Web Client - Path(C:\Program Files\MVPSI\JAMS\WebClient\) TriggerOn(First Matching Matching File or Folder) SubFolders(True) Thresholds(Created,Modified)**

System Monitors - Log File Monitor

The JAMS template contains the following Log File rules:

- **JAMSAgent - Log File - Log File(C:\Program Files\MVPSI\JAMS\Agent\JAMSAgent.log) Include(error) Exclude()**
- **JAMSExecutor Log - Log File(C:\Program Files\MVPSI\JAMS\Scheduler\JAMSExecutor.log) Include (error;failed) Exclude()**
- **JAMSScheduler Log - Log File(C:\Program Files\MVPSI\JAMS\Scheduler\JAMSScheduler.log) Include(error;failed) Exclude()**
- **JAMSServer Log - Log File(C:\Program Files\MVPSI\JAMS\Scheduler\JAMSServer.log) Include(error;failed) Exclude()**

System Monitors - Service Monitor

The JAMS template contains the following Service rules.

- **JAMS Executor Service - Service(JAMS Executor) Status(<>'Running') Startup(='Automatic') Logon A/C(='Local System')**
- **JAMS Scheduler Service - Service(JAMS Scheduler) Status(<>'Running') Startup(='Automatic') Logon A/C(='Local System')**
- **JAMS Server Service - Service(JAMS Server) Status(<>'Running') Startup (='Automatic') Logon A/C(='Local System')**

Windows Lawson ServerView Monitoring template

The Windows Infor ServerView Monitoring template includes monitors for Infor ServerView solutions and uses Web Application, File and Folder, Service and TCP HTTP monitoring components.

> **NOTE:** If you have not purchased the Web Application Monitor, this template only includes the File and Folder, Service and TCP HTTP elements.

The Windows Infor ServerView Monitoring template contains the following components:

Business Application Monitors - Web Application Monitor*

Contains the following rules:

- **Checking for looping M3 auto job - URL (http://127.0.0.1:6788/showlog?addr=127.0.0.1&port6101) Timeout(5 Secs) TriggerType(first Matching) TriggerObject(Table) TriggerObject (Table)**

- Excessive CPU - URL(http://127.0.0.1:6666/) Timeout(15 Secs) TriggerType(Each Matching) TriggerObject(Row)
- High severity for NEWS page - URL(http://127.0.0.1:6666/news) Timeout (5 Secs) TriggerType(Each Matching) TriggerObject(Row)
- Instances of an interactive job for a specified user - URL (http://127.0.0.1:6666/) Timeout(15 Secs) TriggerType(Each Matching) TriggerObject(Row)
- Interaction auto job validation - URL(http://127.0.0.1:6666/) Timeout(15 Secs) TriggerType(First Matching) TriggerObject(Row)
- Interactive job CPU% Check - URL(http://127.0.0.1:6666/) Timeout(15 Secs) TriggerType(Each Matching) TriggerObject(Row)
- ServerView Counters Check - URL(http://127.0.0.1:6666/) Timeout(15 Secs) TriggerType(First Matching) TriggerObject(Row)
- ServerView Dumplogs in NEWS page - URL(http://127.0.0.1:6666/news) Timeout(5 Secs) TriggerType(Each Matching) TriggerObject(Row)
- ServerView Status Check - URL(http://127.0.0.1:6666/) Timeout(15 Secs) TriggerType(Each Matching) TriggerObject(Row)
- Supervisor Check - URL(http://127.0.0.1:6666/) Timeout(25 Secs) TriggerType(First Matching) TriggerObject(Table)
- Transaction Server Check - URL(http://127.0.0.1:6666/) Timeout(25 Secs) TriggerType(First Matching) TriggerObject(Table)

(*Only available if a Web Application Monitor license has been purchased separately).

System Monitors - File and Folder Monitor

Contains the following rule:

- Alert if SalesCube is not updated overnight - Path(D:\) TriggerOn(First Matching Matching File Or Folder) SubFolders (True) Thresholds (Modified)

System Monitors - Service Monitor

Contains the following rules:

- Backup Exec Services Started - Service(Backup Exec Remote Agent for Windows Systems) Status(<>'Running')
- M3 Enterprise Collaborator (MEC) Service Started - Service(MECServer) Status(<>'Running')

- **MapGenServer Service Stared - Service(MapGenServer) Status (<>'Running')**
- **OpenText® StreamServe Repository Server Service Started - Service (StreamServe Repository Server) Status(<>'Running')**
- **OpenText® StreamServe Service Started - Production Environment - Service(StreamServe Prod) Status(<>'Running')**
- **OpenText® StreamServe Service Started - Standard Environment - Service(StreamServe zSTD) Status(<>'Running')**
- **OpenText® StreamServe Service Started - Test Environment - Service (StreamServe Test) Status(<>'Running')**
- **Print Spooler Service Started - Service(Print Spooler) Status(<>'Running')**

TCP Monitors - HTTP Monitor

Contains the following rule:

- **Check CONNECT Site - URL(http://127.0.0.1:8780/) Timeout(5 Secs) Include('News') NotInclude('404')**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Oracle JDE EnterpriseOne template

Oracle's JD Edwards EnterpriseOne is an integrated applications suite of comprehensive enterprise resource planning software.

The Windows Oracle JDE EnterpriseOne template contains the following components:

Performance Monitors - WMI Monitor

Contains the following rules:

- **JDE: Binary Large Object Handler Process Active - Instance(ipcsrv) Trigger(Does Not Exist)**
- **JDE: Execute Submitted Jobs Process Active - Instance(runbatch) Trigger (Does Not Exist)**
- **JDE: Monitor Excessive Jobs on Print Queue - Instance(US Office) Counter(Jobs) Trigger(>10)**
- **JDE: Network Listener Process Active - Instance(jdesnet_n) Trigger (Count < 3)**
- **JDE: Network Listener Process Count - Instance(jdesnet_n) Trigger (Count < 3)**
- **JDE: Primary Process Active - Instance(jdesnet) Trigger(Does Not Exist)**
- **JDE: Server Manager Agent Process Active - Instance(steagent) Trigger (Does Not Exist)**
- **JDE: Server Kernel Process Count - Instance(jdesnet_k) Trigger(Count < 4)**

System Monitors - Log File Monitor

Contains the following rules:

- **JDE: Agent Maintenance Log File - Log File(e:\jde_ home\SCHFA\logs\stderr.log) Include(*) Exclude()**
- **JDE: Java Development Environment Logfile Critical Entries - Log File (C:\jde_home\logs\e1agent_0.log) Include(SEVERE;WARNING) Exclude ()**
- **JDE: Java Runtime Environment Critical Entries - Log File(C;\jre_ home\logs\e1agent_0.log) Include(SEVERE;WARNING) Exclude ()**
- **JDE: Management Agent Log File - Log File(e:\jde_ home|SCFHA\logs\e1agent_0.log) Include(*) Exclude()**

- **JDE: Performance Statistics Log File - Log File (e:\JDEdwards\E910\log\jde_xxxx.log) Include(*) Exclude()**
- **JDE: Snapshot Log File - Log File(e:\SnapShot.log) Include(ERR) Exclude ()**

System Monitors - Service Monitor

Contains the following rules:

- **JDE: 910 B9 Network Service - Service(JDE910 B9 Network) Status(<> 'Started')**
- **JDE: 910 B9 Queue Service - Service(JDE910 B9 Queue Service) Status (<> 'Started')**
- **JDE: JD Edwards EnterpriseOne Service - Service(SM Management Agent) Status(<> 'Started')**
- **JDE: Oracle Weblogic Service - Service(Oracle Weblogic wl_server NodeManager) Status(<> 'Started)**

TCP Monitors - TCP/UDP Generic Monitor

Contains the following rules:

- **JDE: Management Agent Port - Host(127.0.0.1) Port(14502) Timeout(5 Secs) Command(&CM) Result(<> '[Empty]')**
- **JDE: Management Console HTTP Port - Host(127.0.0.1) Port(8999) Timeout(5 Secs) Command(&CM) Result(<> '[Empty]')**
- **JDE: Management Server JMX Port - Host(127.0.0.1) Port(14501) Timeout(5 Secs) Command (&CM) Result(<> '[Empty]')**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Server Performance (Standard) template

The Server Performance (Standard) template provides three summary performance rules to cover standard performance indicators of servers and workstation devices.

Performance Monitors - WMI Monitor

Contains the following rules:

- **CPU Utilization - Group(CPU) Instance(_Total) Type(% Processor Time) Trigger(>= 98%)**

- **Disk space C drive - Group(Disk) Instance(C) Type(Drive Space Used %) Trigger(>= 75%)**
- **Physical memory – Group(Memory) Type(Physical Memory Used %) Trigger (>= 90%)**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Server Performance (Advanced) template

The Windows Server Performance (Advanced) template covers the more technical aspects of server performance aside from those covered by the basic CPU, Disk and Memory template.

Performance Monitors - CPU, Disk & Memory Monitor

The Windows Server Performance (Advanced) template contains the following generic performance rules:

- **Memory Available Bytes - Counter(Available Mbytes) Trigger(<=50)**
- **Memory Committed Bytes - Counter(% Committed Bytes In Use) Trigger (>= 90)**
- **Memory Pages per second – Counter(Pages/sec) Trigger(>=20)**
- **Physical Disk - %Disk Time - Instance(_Total) Counter(% Disk Time) Trigger(>= 99)**

- **Processor - % Processor Time - Instance(_Total) Counter(% Processor Time) Trigger(>=90)**
- **System Processor Queue Length - Counter(Processor Queue Length) Trigger(>= 10)**

> NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows SQL Server template

The SQL Server template monitors the integrity and performance of an SQL Server device.

Performance Monitors- WMI Monitor

Contains the following rules:

- **SQL Server Monitoring & Performance - Counter(Buffer cache hit ratio) Trigger(<=99)**
- **SQL Server Monitoring & Performance - Counter(Connection Memory (KB)) Trigger(>=20480)**
- **SQL Server Monitoring & Performance - Counter(Full Scans/sec) Trigger (>=50)**
- **SQL Server Monitoring & Performance - Counter(Optimizer Memory (KB)) Trigger(>=10240)**
- **SQL Server Monitoring & Performance - Counter(Page Splits/sec) Trigger (>=10)**
- **SQL Server Monitoring & Performance - Counter(SQL Compilations/sec) Trigger(>=5)**
- **SQL Server Monitoring & Performance - Counter(Stolen Pages) Trigger (>=10000)**
- **SQL Server Monitoring & Performance - Counter(Table Lock Escalations/sec) Trigger(>=10)**
- **SQL Server Monitoring & Performance - Counter(User connections) Trigger(>=100)**
- **SQL Server Monitoring & Performance - Instance(Database) Counter (Number of Deadlocks/sec) Trigger(>1)**
- **SQL Server Monitoring & Performance - Instance(First Triggered Instance) Counter(Cache Hit Ratio) Trigger (<=75)**

- **SQL Server Monitoring & Performance - Instance(_Total) Counter(Active Transactions) Trigger(>=10)**
- **SQL Server Monitoring & Performance - Instance(_Total) Counter(Cache Hit Ratio) Trigger(<=75)**
- **SQL Server Monitoring & Performance - Instance(_Total) Counter(Percent Log Used) Trigger(>= 75)**
- **SQL Server Monitoring & Performance - Instance =(_Total) Counter (Transactions/sec) Trigger(>= 25)**

> NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Symantec Backup Exec template

Backup Exec is proprietary backup software developed by Symantec. Backup Exec provides market leading Backup and Recovery software for all sizes of organizations that are predominately Microsoft or VMware centric data-protection solution. Backup Exec protects both virtual and physical environments with a single user interface.

The Symantec Backup Exec template contains the following components:

Event Log Monitors (Standard) - Application Event Log Monitor

Contains the following rules:

- **Error Database Maintenance Failure - Source(='Backup Exec') Category (='*') ID(='57348') User(='*') Message(='*')**
- **Error Device Not Ready - Source(='Backup Exec') Category(='*') ID (='33152') User(='*') Message(='*')**
- **Error Job Cancellation - Source(='Backup Exec') Category(='*') ID (='34114') User(='*') Message(='*')**
- **Error Job Failed - Source(='Backup Exec') Category(='*') ID(='34113') User(='*') Message(='*')**
- **Error Media Error - Source(='Backup Exec') Category(='*') ID(='58057') User(='*') Message(='*')**
- **Error SDR Copy Failed - Source(='Backup Exec') Category(='*') ID (='57751') User(='*') Message(='*')**
- **Error Storage Error - Source(='Backup Exec') Category(='*') ID(='58053') USer(='*') Message(='*')**

- Error Tape Alert Error - Source(='Backup Exec') Category(='*') ID (='65314') User(='*') Message(='*')
- Info Job Success - Source(='Backup Exec') Category(='*') ID(='34112') User(='*') Message(='*')
- User Media Insert - Source(='Backup Exec') Category(='*') ID(='58061') User(='*') Message(='*')
- User Media Intervention - Source(='Backup Exec') Category(='*') ID (='58060') User(='*') Message(='*')
- User Media Overwrite - Source(='Backup Exec') Category(='*') ID (='58062') User(='*') Message(='*')
- User Media Remove - Source(='Backup Exec') Category(='*') ID(='58063') User(='*') Message(='*')
- User Storage Intervention - Source(='Backup Exec') Category(='*') ID (='58056') User(='*') Message(='*')
- Warning Job Completed With Exceptions - Source(='Backup Exec') Category(='*') ID(='57755') User(='*') Message(='*')
- Warning Job Warning - Source(='Backup Exec') Category(='*') ID (='33919') User(='*') Message(='*')
- Warning Library Inset - Source(='Backup Exec') Category(='*') ID (='58064') User(='*') Message(='*')
- Warning License and Maintenance Warning - Source(='Backup Exec') Category(='*') ID(='34581') User(='*') Message(='*')
- Warning Media Warning - Source(='Backup Exec') Category(='*') ID (='58058') User(='*') Message(='*')
- Warning Storage Warning - Source(='Backup Exec') Category(='*') ID (='58054') User(='*') Message(='*')
- Warning Tape Alert Warning - Source(='Backup Exec') Category(='*') ID (='65313') User(='*') Message(='*')

System Monitors (Standard) - Service Monitor

Contains the following rules:

- Backup Exec Agent Browser - Service(Backup Exec Agent Browser) Status(<>'Started') Startup(='Automatic')
- Backup Exec Device Media Service - Service(backup Exec Device & Media Service) Status(<>'Started') Startup(='Automatic')
- Backup Exec DLO Administration Service - Service(Backup Exec DLO Administration Service) Status(<>'Started') Startup(='Automatic')

- **Backup Exec DLO Maintenance Service - Service(Backup Exec DLO Maintenance Service) Status(<>'Started') Startup(='Automatic')**
- **Backup Exec Error Recording Service - Service(Backup Exec Error Recording Service) Status(<>'Started') Startup(='Automatic')**
- **Backup Exec Job Engine - Service(Backup Exec Job Engine) Status (<>'Started') Startup(='Automatic')**
- **Backup Exec Management Service - Service(Backup Exec Management Service) Status(<>'Started) Startup(='Automatic')**
- **Backup Exec Remote Agent for Windows - Service(Backup Exec Remote Agent for Windows) Status(<>'Started') Startup(='Automatic')**
- **Backup Exec Server - Service(Backup Exec Server) Status(<>'Started') Startup(='Automatic')**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Symantec NetBackup template

Symantec NetBackup is an enterprise level backup and recovery suite. It provides cross-platform backup functionality to a large variety of Windows, UNIX and Linux operating systems. It is set up with a central master server that manages both media servers (containing the backup media) and clients. Core server platforms are, Solaris, HP-UX, AIX, Tru64, Linux and Windows.

The Symantec NetBackup template contains the following components:

Event Log Monitors (Standard) - Application Event Log Monitor

Contains the following rules:

- **Any NetBackup Error - Type(Exclude) Source(='NetBackup Database Manager') Category('None') ID('0') User('N/A') Message('*exited with status*')**
- **Backup Not Coimpleted - Example - Source('NetBackup Database Manager') Category('None') ID('0') User('N/A') Message('*4 68*MailServer_Daily*EXIT STATUS *)**
- **Backup Not Started - Example - Source('NetBackup Database Manager') Category('None') ID('0') User('N/A') Message('*started backup job for client*MailServer_Daily*')**
- **Backup Started - Source('NetBackup Database Manager') Category ('None') ID('0') User('N/A') Message ('started backup job for client*')**
- **Finished Backups - Source('NetBackup Database Manager') Category ('None') ID('0') User('N/A') Message('4 68*EXIT STATUS 0*')**

Performance Monitors - CPU, Disk & Memory Monitor

Contains the following rule:

- **Drive C - Low Disk Space - Group (Disk) Instance(C:) Type(Drive Space Available%) Trigger(<10%)**

System Monitors - Service Monitor

Contains the following rules:

- **NetBackup Agent Request Server - Service(NetBackup Agent Request Server) Status(<>'Started') Startup('Automatic')**
- **NetBackup Audit Manager - Service(NetBackup Audit Manager) Status (<>'Started') Startup('Automatic')**
- **NetBackup Authentication - Service(NetBackup Authentication) Status (<>'Started') Startup('Automatic')**
- **NetBackup Authorization - Service(NetBackup Authorization) Status (<>'Started') Startup('Automatic')**
- **NetBackup Bare Metal Restore Boot Server - Service(NetBackup Bare Metal Restore Boot Server) Status(<>'Started') Startup('Automatic')**
- **NetBackup Bare Metal Restore Master Server - Service(NetBackup Bare Metal Restore Master Server) Status (<>'Started') Startup('Automatic')**

- NetBackup BMR MTFTP Service - Service(NetBackup BMR MTFTP Service) Status(<>'Started') Startup(='Automatic')
- NetBackup BMR PXE Service - Service(NetBackup BMR PXE Service) Status(<>'Started') Startup(='Automatic')
- NetBackup Client Service - Service(NetBackup Client Service) Status(<> 'Started') Startup(='Automatic')
- NetBackup Compatibility Service - Service(NetBackup Compatibility Service) Status(<>'Started') Startup(='Automatic')
- NetBackup Database Manager - Service(NetBackup Database Manager) Status(<>'Started) Startup(='Automatic')
- NetBackup Device Manager - Service(NetBackup Device Manager) Status (<>'Started') Startup(='Automatic')
- NetBackup Enterprise Media Manager - Service(NetBackup Enterprise Media Manager) Status(<>'Started') Startup(='Automatic')
- NetBackup Event Manager - Service(NetBackup Event Manager) Status (<>'Started') Startup(='Automatic')
- NetBackup Job Manager - Service(NetBackup Job Manager) Status (<>'Started') Startup(='Automatic')
- NetBackup Key Management Service - Service(NetBackup Key Management Service) Status(<>'Started') Startup(='Automatic')
- NetBackup Legacy Client Service - Service(NetBackup Legacy Client Service) Status(<> 'Started') Startup(='Automatic')
- NetBackup Legacy Network Service - Service(NetBackup Legacy Network Service) Status(<>'Started') Startup(='Automatic')
- NetBackup Policy Execution Manager - Service(NetBackup Policy Execution Manager) Status(<>'Started') Startup(='Automatic')
- NetBackup Proxy Service - Service (NetBackup Proxy Service) Status (<>'Started') Startup(='Automatic')
- NetBackup Relational Database Manager - Service(NetBackup Relational Database Manager) Status(<>'Started) Startup(='Automatic')
- NetBackup Remote Manager and Monitor Service - Service(NetBackup Remote Manager and Monitor Service) Status(<>'Started') Startup ('Automatic')
- NetBackup Request Daemon - Service(NetBackup Request Daemon) Status(<>'Started') Startup(='Automatic')
- NetBackup Resource Broker - Service(NetBackup Resource Broker) Status(<>'Started') Startup(='Automatic')

- **NetBackup SAN Client Fibre Transport Service - Service(NetBackup SAN Client Fibre Transport Service) Status(<>'Started') Startup(='Automatic')**
- **NetBackup Service Layer - Service(NetBackup Service Layer) Status (<>'Started') Startup(='Automatic')**
- **NetBackup Service Monitor - Service(NetBackup Service Monitor) Status (<>'Started') Startup(='Automatic')**
- **NetBackup Storage Lifecycle Manager - Service(NetBAckup Storage Lifecycle Manager) Status(<>'Started') Startup(='Automatic')**
- **NetBackup Vault Manager - Service(NetBackup Vault Manager) Status (<>'Started') Startup(='Automatic')**
- **NetBackup Volume Manager - Service(NetBackup Volume Manager) Status(<>'Started') Startup(='Automatic')**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Terminal Services template

The Windows Terminal Services template provides the following generic performance rules:

Performance Monitors - WMI Monitor

Contains the following rules:

- **Terminal Services Performance - Counter(Active Sessions) Trigger(>=2)**
- **Terminal Services Performance - Counter(Inactive Sessions) Trigger(>=2)**
- **Terminal Services Performance - Instance(Console) Counter(% Processor Time) Trigger(>=20)**
- **Terminal Services Performance - Instance(Console) Counter(Total Bytes) Trigger (>=100,000)**
- **Terminal Services Performance - Instance(Console) Counter(Total Timeouts) Trigger(>=100,000)**
- **Terminal Services Performance - Instance(Console) Counter(Total Errors) Trigger(>=5)**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Windows Update template

The Windows Update template provides three Log File rules for the monitoring of Windows updates:

System Monitors - Log File Monitor

Contains the following monitors:

- **Fatal Errors - Log File(c:\windows\windowsupdate.log) Include(FATAL) Exclude()**
- **Pending Updates - Log File(c:\windows\windowsupdate.log) Expression (".+Reporting status event with [1-9][0-9]*installable.+")**
- **Reboot Required - Log File(c:\windows\windowsupdate.log) Include (Install call completed, reboot required = Yes") Exclude()**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

AIX System Monitoring (Standard) template

The AIX System Monitoring (Standard) template contains rules covering all of the AIX Monitors with the exception of the System Monitor.

AIX Error Report Monitor

Contains the following rules:

- **Hardware Errors - Errpt(Class=H)**
- **Software Errors - Errpt(Class=S)**

Subsystem Report Monitor

Contains the following rules:

- **Critical Subsystem (inetd) Does Not Exist - Subsystem Does Not Exist (inetd)**
- **Critical Subsystem (inetd) is Inoperative - Subsystem is Inoperative(inetd)**
- **Critical Subsystem (qdaemon) Does Not Exist - Subsystem Does Not Exist (qdaemon)**
- **Critical Subsystem (qdaemon) is Inoperative - Subsystem is Inoperative (qdaemon)**
- **Critical Subsystem (syslogd) Does Not Exist - Subsystem Does Not Exist (syslogd)**
- **Critical Subsystem (syslogd) is Inoperative - Subsystem is Inoperative (inetd)**

Logical Report Monitor

Contains the following rules:

- **Alert when Quorum is set to On When Disk Mirroring is Active (rootvg) Measure(Quorum) Trigger(=0)**
- **Volume Group (rootvg) Does Not Exist - Volume Group rootvg Does Not Exist**

Script Monitor

Contains the following rules:

- **Check for Failed Logins - Script(/var/lib/halcyon/logfails.sh denied)**
- **Check for Missing or Removed Disks - Script(lspv missing | removed)**
- **Zombie process - Report on all - Script(ps-ec stat,pid | egrep “^Z” | awk ‘{print $2}’ ^[^$])**
- **Zombie process count - Script(ps -eo stat,pid | egrep “^Z” | wc -l ^[^0])**

File & Folder Monitor

Contains the following rules:

- File (/etc/aixmibd.conf) Has Changed - File(/etc/aixmibd.conf) Trigger (Exists)
- File (/etc/inetd.conf) Has Changed - File(/etc/inetd.conf) Trigger(Exists)
- File (/etc/inittab) Has Changed - File(/etc/inittab) Trigger(Exists)
- File (/etc/profile) Has Changed - File(/etc/profile) Trigger(Exists)
- File (/etc/security/login.cfg) Has Changed - File(/etc/security/login.cfg) Trigger(Exists)
- File (/etc/sendmail.cf) Has Changed - File(/etc/sendmail.cf) Trigger (Exists)
- File (/var/spool/cron/crontabs/root) Has Changed - File (/var/spool/cron/crontabs/root) Trigger(Exists)

Log File Monitor

Contains the following rules:

- **Monitor for Failed Logins - LogFile(/var/lib/halcyon/failedlogins.log Expression(.*)**
- **Monitor for New Entries in Cron Log - LogFile(/var/adm/cron/log) Expression(.*)**

CPU, Filesystem and Memory Monitor

Contains the following rules:

- **Filesystem (/) Disk Space Used >=80% - Group(Filesystem) Volume(/) Type(UsedPercent) Trigger(>=80%)**
- **Filesystem (/) Does Not Exist - Group(Filesystem) Volume(/) Trigger(Does Not Exist)**
- **Filesystem (/) Inode Used >=90% - Group(Filesystem) Volume(/) Type (UUsedInodesPercent) Trigger(>=90%)**
- **Filesystem (/home) Disk Space Used >=80% - Group(Filesystem) Volume (/home) Type(UsedPercent) Trigger(>=80%)**
- **Filesystem (/home) Does Not Exist - Group(Filesystem) Volume(/home) Trigger(Does Not Exist)**
- **Filesystem (/home) Inode Used >=90% - Group(Filesystem) Volume (/home) Type(UUsedInodesPercent) Trigger(>=90%)**
- **Filesystem (/tmp) Disk Space Used >=80% - Group(Filesystem) Volume (/tmp) Type(UsedPercent) Trigger(>=80%)**
- **Filesystem (/tmp) Does Not Exist - Group(Filesystem) Volume(/tmp) Trigger(Does Not Exist)**
- **Filesystem (/tmp) Inode Used >=90% - Group(Filesystem) Volume(/tmp) Type(UUsedInodesPercent) Trigger(>=90%)**
- **Filesystem (/usr) Disk Space Used >=80% - Group(Filesystem) Volume (/usr) Type(UsedPercent) Trigger(>=80%)**
- **Filesystem (/usr) Does Not Exist - Group(Filesystem) Volume(/usr) Trigger (Does Not Exist)**
- **Filesystem (/usr) Inode Used >=90% - Group(Filesystem) Volume(/usr) Type(UUsedInodesPercent) Trigger(>=90%)**
- **Filesystem (/var) Disk Space Used >=80% - Group(Filesystem) Volume (/var) Type(UsedPercent) Trigger(>=80%)**

- **Filesystem (/var) Does Not Exist - Group(Filesystem) Volume(/var) Trigger (Does Not Exist)**
- **Filesystem (/var) Inode Used >=90% - Group(Filesystem) Volume(/var) Type(UUsedInodesPercent) Trigger(>=90%)**
- **Sustained CPU >95% - Group(CPU) CPU(0) Type(Load) Trigger(>95%)**

Process Monitor

Contains the following rules:

- **Critical Process (biod) Does Not Exist - Type(Process By Name) Process (biod) Trigger(DoesNotExist)**
- **Critical Process (cron) Does Not Exist - Type(Process By Name) Process (cron) Trigger(DoesNotExist)**
- **Critical Process (errdemon) Does Not Exist - Type(Process By Name) Process(errdemon) Trigger(DoesNotExist)**
- **Critical Process (inetd) Does Not Exist - Type(Process By Name) Process (inetd) Trigger(DoesNotExist)**
- **Critical Process (portmap) Does Not Exist - Type(Process By Name) Process(portmap) Trigger(DoesNotExist)**
- **Critical Process (qdaemon) Does Not Exist - Type(Process By Name) Process(qdaemon) Trigger(DoesNotExist)**
- **Critical Process (syncd) Does Not Exist - Type(Process By Name) Process(syncd) Trigger(DoesNotExist)**
- **Critical Process (writesrv) Does Not Exist - Type(Process By Name) Process(writesrv) Trigger(DoesNotExist)**

Ping Monitor

Contains a single rule:

- **Check Server Can Ping Router - Host(1.2.3.4) Timeout(2000) Attempts(4) Success(50%) TTL(128)**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

AIX System Monitoring (Advanced) Template

The AIX System Monitoring (Advanced) template contains all of the rules available in the Standard template and adds additional rule coverage.

AIX Error Report Monitor

Contains the following rules:

- **Error Logger Errors - Errpt(Class=O)**
- **Undetermined Errors - Errpt(Class=U)**

Subsystem Monitor

Contains the following rules:

- **Critical Subsystem (dhcpcd) Does Not Exist - Subsystem Does Not Exist (dhcpcd)**
- **Critical Subsystem (dhcpcd) is Inoperative - Subsystem is Inoperative (dhcpcd)**
- **Critical Subsystem (lpd) Does Not Exist - Subsystem Does Not Exist(lpd)**
- **Critical Subsystem (lpd) is Inoperative - Subsystem is Inoperative(lpd)**
- **Critical Subsystem (sendmail) Does Not Exist - Subsystem Does Not Exist (sendmail)**
- **Critical Subsystem (sendmail) is Inoperative - Subsystem is Inoperative (sendmail)**

Logical Volume Monitor

Contains the following rules:

- Stale Physical Partitions Exist (/Mounted on rootvg hd4) - Measure(Stale Physical Partitions) Trigger(>0)
- Stale Physical Partitions Exist (/home Mounted on rootvg hd1) - Measure (Stale Physical Partitions) Trigger(>0)
- Stale Physical Partitions Exist (/tmp Mounted on rootvg hd3) - Measure (Stale Physical Partitions) Trigger(>0)
- Stale Physical Partitions Exist (/usr Mounted on rootvg hd2) - Measure (Stale Physical Partitions) Trigger(>0)
- Stale Physical Partitions Exist (/var Mounted on rootvg hd9) - Measure (Stale Physical Partitions) Trigger(>0)
- Stale Physical Partitions on rootvg - Measure(Stale Physical Partitions) Trigger(>0)

Script Monitor

Contains the following rules:

- Console Log - Script(/var/lib/halcyon/conslog.sh.+)
- Disk I/O Busy >75% Possible I/O Bound System - Script(iostat 1 1 | grep hdisk0 | awk '{print$2}' ^[7-9]{1}[0-9]{1}\..$|^100\..$)
- Disk I/O Wait >25% Possible I/O Bound System - Script(iostat 1 1 | awk 'FNR==5{print$6} 2{1}[6-9]{1}\..$|^[3-9]{1}[0-9]{1}\..$|^100\..$)
- Sustained Disk Utilisation >=80% - Script(iostat -d 1 1 | awk 'FNR==5 {print$2}'[8-9][0-9].)
- Verify Operation Status of Path to MPIO Device - Script(lspath | grep -v Enabled.+)

File & Folder Monitor

Contains the following rules:

- File (/etc/environment) Has Changed - File(/etc/environment) Trigger (Exists)
- File (/etc/hostmibd.conf) Has Changed - File(/etc/hostmibd.conf) Trigger (Exists)
- File (/etc/netsvc.conf) Has Changed - File(/etc/netsvc.conf) Trigger (Exists)
- File (/etc/resolv.conf) Has Changed - File(/etc/resolv.conf) Trigger(Exists)

Log File Monitor

Contains the same two rules available in the AIX System Monitoring (Standard) template.

CPU, Filesystem and Memory Monitor

Contains the following rules:

- **PageFile Used <30% (Suggests Too Much Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(<30%)**
- **PageFile Used >70% (Suggests Not Enough Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(>70%)**
- **Paging Space >95% - Group(Memory) Type(UsedPageFilePercent) Trigger(>95%)**

Process Monitor

Contains the following rules:

- **Optional Process (aixmibd) Does Not Exist - Type(Process By Name) Process(aixmibd) Trigger(DoesNotExist)**
- **Optional Process (hostmibd) Does Not Exist - Type(Process By Name) Process(hostmibd) Trigger(DoesNotExist)**
- **Optional Process (rpc.lockd) Does Not Exist - Type(Process By Name) Process(rpc.lockd) Trigger(DoesNotExist)**
- **Optional Process (rpc.statd) Does Not Exist - Type(Process By Name) Process(rpc.statd) Trigger(DoesNotExist)**
- **Optional Process (sendmail) Does Not Exist - Type(Process By Name) Process(sendmail) Trigger(DoesNotExist)**
- **Optional Process (snmpd) Does Not Exist - Type(Process By Name) Process(snmpd) Trigger(DoesNotExist)**
- **Optional Process (snmpmibd) Does Not Exist - Type(Process By Name) Process(snmpmibd) Trigger(DoesNotExist)**
- **Optional Process (sshd) Does Not Exist - Type(Process By Name) Process(sshd) Trigger(DoesNotExist)**

Ping Monitor

This contains the same rules as available in the AIX System Monitoring (Standard) template.

> NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

AIX MQ Monitor Template

IBM MQ is the most popular system for cross- platform messaging, providing assured delivery of messages across 35 plus IBM and non-IBM platforms, including IBM mainframe and midrange, Windows, AIX and Linux.

Central Configuration Manager contains an AIX Template for managing MQ installations running on AIX. This contains the following monitors:

AIX Script Monitor

The script monitor is the engine-room of the MQ monitor. Use the script provided to interrogate an MQ environment.

The script is installed to, and must reside in **/var/lib/halcyon**

Configure the hmq.config file to point to the MQ installation namely:

- The location of the **runmqsc** command.

- The location of the **mqs.ini** file.

Script Monitor

Contains the following rules:

- MQ *SAMPLE* - Channel indicator running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CHINIT .+)
- MQ *SAMPLE* - Channel is RUNNING? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgqr jupiter.queue.manager -monitor CHANNEL -name HALAIX61.HALAIX71 .+)
- MQ *SAMPLE* - Command Server running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CMDSERV .+)
- MQ *SAMPLE* - Connection count - Script(/bin/ksh /var/lib/halcyon/hq.sh -qmgr jupiter.queue.manager -monitor CONNS -ge 20 .+)
- MQ *SAMPLE* - Dead Letter queue CURDEPTH > 0 - Script/bin.ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name DEADLETTER.QUEUE -gt 0 .+)
- MQ *SAMPLE* - Listener status - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor LISTENER -name HALAIX61.LISTENER.TCP .+)
- MQ *SAMPLE* - Message age test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor MSGAGE -name TEST.SEND.QUEUE -ge 120 .+)
- MQ *SAMPLE* - Monitor the number of handles that are currently open for input for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor IPPROCS -name TEST.SEND.QUEUE -ge 25 .+)
- MQ *SAMPLE* - Monitor the number of handles that are currently open for output for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor OPPROCS -name TEST.SEND.QUEUE -ge 25 .+)
- MQ *SAMPLE* - QMGR Performance Events not enabled? - Script (/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor QMGR -name PERFMEV -value ENABLED .+)
- MQ *SAMPLE* - Queue depth percentage test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor QDEPTHCT -name TEST.SEND.QUEUE -ge 75 .+)
- MQ *SAMPLE* - Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name TEST.SEND.QUEUE -ge 3 .+)

- MQ *SAMPLE* - Queue LASTGET test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor LASTGET -name TEST.SEND.QUEUE -ge120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor LASTGET -name TEST.SEND.QUEUE -ge 120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor LASTGET -name TEST.SEND.QUEUE - ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor LASTPUT -name TEST.SEND.QUEUE -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor LASTPUT -name TEST.SEND.QUEUE -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor LASTPUT -name TEST.SEND.QUEUE -ge 120 .+)
- MQ *SAMPLE* - QUEUE uncommitted message count - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor UNCOM -name TEST.SEND.QUEUE -ne 0 .+)
- MQ *SAMPLE* - Queue with wrong name (Shows error message) - Script (/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name HALAIX61.SEND.QPO -gt 10 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CHANNEL.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor CURDEPTH -name SYSTEM.ADMIN.CHANNEL.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.COMMAND.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor CURDEPTH -name SYSTEM.ADMIN.COMMAND.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CONFIG.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor CURDEPTH -name SYSTEM.ADMIN.CONFIG.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.LOGGER.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor CURDEPTH -name SYSTEM.ADMIN.LOGGER.EVENT -ne 0 .+)
- MQ *SAMPLE - SYSTEM.ADMIN.PERFM.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager - monitor CURDEPTH -name SYSTEM.ADMIN.PERFM.EVENT -ne 0 .+)

- MQ *SAMPLE* - SYSTEM.ADMIN.PUBSUB.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name SYSTEM.ADMIN.PUBSUB.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.QMGR.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name SYSTEM.ADMIN.QMGR.EVENT -ne 0 .+)

File & Folder Monitor

Contains the following rules:

- *SAMPLE* MQ - Queue Manager .ini file permissions and ownership check. - File(/var/mqm/qmgrs/jupiter!queue!manager) Include(qm.ini) Trigger(Does Not Exist)
- *SAMPLE* Queue Manager Error log ownership and permissions - File (/var/mqm/qmgrs/jupiter!queue!Manager/errors) Include(AMQERR*.LOG) Trigger(Does Not Exist)
- MQ - /var/mqm directory permissions an ownership check. - Folder(/var) Include(mqm) Trigger(Does Not Exist)
- MQ - /var/mqm/config directory permissions and ownership check. - Folder(/var/mqm) Include(config) Trigger(Does Not Exist)
- MQ - /var/mqm/conv directory permissions and ownership check. - Folder (/var/mqm) Include(conv) Trigger(Does Not Exist)
- MQ - /var/mqm/errors directory permissions and ownership check. - Folder(/var/mqm) Include(errors) Trigger(Does Not Exist)
- MQ - /var/mqm/errors/*.FDC file(s) found - File(/var/mqm/errors) Include (*.FDC) Trigger(Exists)
- MQ - /var/mqm/exits directory permissions and ownership check. - Folder (/var/mqm) Include(exits) Trigger(Does Not Exist)
- MQ - /var/mqm/exits64 directory permissions and ownership check. - Folder(/var/mqm) Include(exits64) Trigger(Does Not Exist)
- MQ - /var/mqm/log directory permissions and ownership check. - Folder (/var/mqm) Include(log) Trigger(Does Not Exist)
- MQ - /var/mqm/mqft directory permissions and ownership check. - Folder (/var/mqm) Include(Mqft) Trigger(Does Not Exist)
- MQ - /var/mqm/mqs.ini file permissions, ownership and changed check. - (Mulitple Criteria Defined)
- MQ - /var/mqm/qmgrs directory permissions and ownership check. - Folder(/var/mqm) Include(qmgrs) Trigger(Does Not Exist)

- MQ - /var/mqm/shared directory permissions and ownership check. - Folder(/var/mqm) Include(shared) Trigger(Does Not Exist)
- MQ - /var/mqm/sockets directory permissions and ownership check. - Folder(/var/mqm) Include(sockets) Trigger(Does Not Exist)
- MQ - /var/mqm/trace directory permissions and ownership check. - Folder (/var/mqm) Include(trace) Trigger(Does Not Exist)

Log File Monitor

Contains the following rules:

- MQ Error monitor - AMQ5027 (The Listener has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5027*)
- MQ Error monitor - AMQ5041 (The queue manager task has ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQER01.LOG) Expression(^AMQ5041*)
- MQ Error monitor - AMQ5976 (WebSphere MQ Distributed Pub/Sub has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5976*)
- MQ Error monitor - AMQ6090 (WebSphere MQ was unable to display an error message) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6090*)
- MQ Error monitor - AMQ6119 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6119*)
- MQ Error monitor - AMQ6125 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6125*)
- MQ Error monitor - AMQ6183 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6183*)
- MQ Error monitor - AMQ6184 (An internal WebSphere MQ error has occurred on queue manager) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6184*)

- MQ Error monitor - AMQ7469 (Transactions rolled back to release log space) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ7469*)
- MQ Error monitor - AMQ8004 (WebSphere MQ queue manager ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8004*)
- MQ Error monitor - AMQ8101 (WebSphere MQ error (XXXXXXX) has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8101*)
- MQ Error monitor - AMQ8420 (Channel status not found) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8420*)
- MQ Error monitor - AMQ9001 (Channel ended normally) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9001*)
- MQ Error monitor - AMQ9202 (Remote host not available, retry) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9202*)
- MQ Error monitor - AMQ9208 (Error on receive from host) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9208*)
- MQ Error monitor - AMQ9209 (Connection to host XXXXXXXX closed) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9209*)
- MQ Error monitor - AMQ9213 (A communications error for XXXXXXXX occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9213*)
- MQ Error monitor - AMQ9218 (The TCP/IP listener program could not bind to port number) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9218*)
- MQ Error monitor - AMQ9228 (The XXXXXXXX responder program could not be started) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9228*)

- MQ Error monitor - AMQ9503 (Channel negotiation failed) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9503*)
- MQ Error monitor - AMQ9513 (Maximum number of channels reached) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9513*)
- MQ Error monitor - AMQ9526 (Message sequence number error for channel XXXXXXXX) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9526*)
- MQ Error monitor - AMQ9542 (Queue manager is ending) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9542*)
- MQ Error monitor - AMQ9999 (Channel to host ended abnormally) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9999*)
- MQ FFST record (.FDC file) *SAMPLE* - LogFile(/var/adm/syslog) Expression(.+FFST record created in .+)

Process Monitor

Contains the following rules:

- MQ Monitor - Broker worker process (amqfcxba) not active - Type(Process By Name) Process(amqfcxba) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(runmqchi) not active - Type(Process By Name) Process(runmqchi) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(amqrmppa) not active - Type(Process By Name) Process(amqrmppa) Trigger(Does Not Exist)
- MQ Monitor - Channel process manager(amqzmuc0) not active - Type (Process By Name) Process(amqzmuc0) Trigger(Does Not Exist)
- MQ Monitor - Dead letter queue handler(runmqdlq) not active - Type (Process By Name) Process(runmqdlq) Trigger(Does Not Exist)
- MQ Monitor - LQM Agents (amqzlaa0) not active - Type(Process By Name) Process(amqzlaa0) Trigger(Does Not Exist)
- MQ Monitor - LU62 receiver channel and client connection (amqcrs6b) not active - Type(Process By Name) Process(amqcrs6b) Trigger(Does Not Exist)
- MQ Monitor - MQ listener (runmqlsr) not active - Type(Process By Name) Process(runmqlsr) Trigger(Does Not Exist)

- **MQ Monitor - Object Authority Manager (amqzfuma) not active - Type (Process By Name) Process(amqzfuma) Trigger(Does Not Exist)**
- **MQ Monitor -Process controller(amqzmgr0) not active - Type(Process By Name) Process(amqzmgr0) Trigger(Does Not Exist)**
- **MQ Monitor - Processing controller (amqzxma0) not active - Type(Process By Name) Process(amqzxma0) Trigger(Does Not Exist)**
- **MQ Monitor - Publish subscribe process (amqfqpub) not active - Type (Process By Name) Process(amqfqpub) Trigger(Does Not Exist)**
- **MQ Monitor - PubSub restartable utility manager (amqzmuf0) not active - Type(Process By Name) Process(amqzmuf0) Trigger(Does Not Exist)**
- **MQ Monitor - Queue manager agent (amqzsla0) not active - Type(Process By Name) Process(amqzsla0) Trigger(Does Not Exist)**
- **MQ Monitor - Repository process (amqrrmfa) not active - Type(Process By Name) Process(amqrrmfa) Trigger(Does Not Exist)**
- **MQ Monitor - Restartable process manager (amqzmur0) not active - Type (Process By Name) Process(amqzmur0) Trigger(Does Not Exist)**
- **MQ Monitor -TCP/IP-invoked channel responder (amqcrsta) not active - Type(Process By Name) Process(amqcrsta) Trigger(Does Not Exist)**
- **MQ Monitor - The command server (amqpcesa) not active - Type(Process By Name) Process(amqpcesa) Trigger(Does Not Exist)**
- **MQ Monitor - Trigger monitor (runmqtrm) not active - Type(Process By Name) Process(runmqtrm) Trigger(Does Not Exist)**

AIX Oracle JDE EnterpriseOne template

Oracle's JD Edwards EnterpriseOne is an integrated applications suite of comprehensive enterprise resource planning software.

The AIX Oracle JDE EnterpriseOne template contains the following components:

Script Monitor

Contains the following rule:

- **JDE: Monitor Overnight NIGHTOPR Batch Processes - Script(jdejobs nightopr ^([a-zA-Z0-9]+).*)**

File and Folder Monitor

Contains the following rule:

- **JDE: Monitor changes in JDE.INI - File or Folder(JDE_BASE\JDE.INI) Include(*) Trigger(Exists)**

Log File Monitor

Contains the following rule:

- **JDE: Monitor JDE LogFiles - LogFile(/var/log/jde/jde*) Expression(.+)**

> NOTE: Each log file to be monitored must be entered as a separate rule. Use the copy rule facility to save time.

Process Monitor

Contains the following rules:

- **JDE: Execute Submitted Jobs Process Active - Type(Process By Name) Process(runbatch) Trigger(Does Not Exist)**
- **JDE: Kernel Processes Active - Type(Process By Name) Process(jde_k) Trigger(Does Not Exist)**
- **JDE: Kernel Process Count - Type(Process By Name) Process(jde_k) Measure(NumberOfProcesses) Trigger(<4)**
- **JDE: Network Listener Process Active - Type(Process By Name) Process (jde_n) Trigger(Does Not Exist)**
- **JDE: Network Listener Process Count - Type(Process By Name) Process (jde_n) Measure(NumberOfProcesses) Trigger(<3)**

> NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

AIX Temenos T24 template

Temenos T24 is widely used core banking system which provides a technically advanced front-to-back platform for banks in over 120 countries.

T24 is a modular, functionally rich, fully integrated, real-time banking application, that has removed the need for end-of-day processing and enabled 24/7/365 online operation.

The AIX Temenos T24 Template contains rules covering the AIX Script, File & Folder and CPU, Filesystem and Memory Monitors.

AIX Script Monitor

Contains the following rules:

- Agent ARCIB jbase not running - Script(ps - ef | grep "start \-p 7701" ^$)
- Agent BROWSER jbase not running - Script(ps - ef | grep "jbase_agent start \-p 7500" ^$)
- Agent PEGA jbase not running - Script(ps - ef | grep "start \-p 7888" ^$)
- File count DW.EXTRACT <500 files in folder - Script (/var/lib/halcyon/filecount.sh/live/globus/bnk.local/DW.EXTRACT 500 Less.*)
- Phantom DEBIT CARD not running - Script(ps - ef | grep "jsh \-Jz\-c EX EB.PHANTOM.PH OFS.USER DEBIT CARDS" ^$)
- Phantom DELIVERY PRINT CARRIER not running - Script(ps - ef | grep "jsh\-Jz\-c DE.PHANTOM.CALL DE.O.CC.PRINT" ^$)
- Phantom EXSHARE not running - SCript(ps - ef | grep "jsh\-Jz\-c EX EB.PHANTOM.PH EXS.USER EXSHARE" ^$)
- Phantom JBLOADER not running - Script(ps - ef | grep "jsh\-Jz|-c EX EB.PHANTOM.PH OFS.USER JBLOADER" ^$)
- Phantom TIB daemon not running - Script(ps - ef | grep "java\-Xmx512M\-Djava.endorsed.dirs=../lib/endorsed/jaxp13:../lib/endorsed/jax13\-jar ..lib/tcserver.jar" ^S
- Printer queue is down - Script(lpstat | grep DOWN .+)

AIX File and Folder Monitor

Contains the following rules:

- Files older than 12 hours in /Globus/bnk.local/FT.IN.TAPE/BNK.CBACS - File Or Folder(live/globus/bnk.local/FT.IN.TAPE) Include(BNK.CBACS*) Trigger(Exists)
- Files older than 5 minutes in /Swift/In - File(/Swift/IN) Include(*) Trigger (Exists)
- Files older than 5 minutes in /Swift/Out - File(/Swift/Out) Include(8) Trigger(Exists)
- Files older than 6 hours in /Globus/bnk.local/DW.EXTRACT - File Or Folder(/live/globus/bnk.local/DW.EXTRACT) Include(*) Trigger(Exists)
- Files older than 60 minutes in /LocalClearing) Include(*) Trigger(Exists)

CPU, Filesystem and Memory Monitor

Contains the following rules:

- Filesystem /jbase10000t > 80% Used - Group(Filesystem) Volume (/jbase10000) Type(Filesystem Space Used %) Trigger(>80%)

- **Filesystem /jbase1019 > 80% Used - Group(Filesystem) Volume (/jbase10000) Type(Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /live/globus/bnk.arc > 80% Used - Group(Filesystem) Volume (/live/globus/bnk.arc) Type(Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /live/globus/bnk.backup >80% Used - Group(Filesystem) Volume(/live/globus/bnk.backup) Type(Filesystem Space Used %) Trigger (>80%)**
- **Filesystem /live/globus/bnk.data >80% Used - Group(Filesystem) Volume (/live/globus/bnk.data) Type(Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /live/globus/bnk.local >80% Used - Group(Filesystem) Volume (/live/globus/bnk.local) Type(Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /live/globus/jspooler > 80% Used - Group(Filesystem) Volume (/live/globus/jspooler) Type(Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /logs > 80% Used - Group(Filesystem) Volume(/logs) Type (Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /Swift > 80% Used - Group(Filesystem) Volume(/Swift) Type (Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /tmp > 80% Used - Group(Filesystem) Volume(/tmp) Type (Filesystem Space Used %) Trigger(>80%)**
- **Filesystem /tranlogs > 80% Used - Group(Filesystem) Volume (/live/tranlogs) type(Filesystem Space Used %) Trigger(>80%)**
- **Filesystem live/globus > 80% Used - Group(Filesystem) Volume (/live/globus) type(Filesystem Space Used %) trigger(>80%)**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

TIP: For a more detailed overview of these templates, download a copy of the Guide to AIX Temenos T24 templates.

AIX VIOS template

The virtual I/O server (VIOS) is an appliance that provides virtual storage and shared ethernet adapter capability to client logical partitions.it allow a physical adapter with attached disks on the virtual i/o sever partition to be shared by one or more partitions, enabling clients to consolidate and potentially minimize the number of physical adapters required.

The AIX VIOS template contains the following components:

AIX Error Report Monitor

Contains the following rules:

- **Hardware Errors - Errpt(Class=H)**
- **Software Errors - Errpt(Class=S)**

Script Monitor

Contains the following rules:

- **Check for adapter errors - Script(for ERROR in $(lsdev -c adapter | grep -v -w -e Available -e description | awk '{print $1}'); do OCCURS=$(lsdev - l $ERROR); echo $OCCURS; done .+)**
- **Check for maps that are not available (between external disk and client partitions) - Script(result=`/usr/ios/cli/ioscli lsmap -all|grep ^Status|grep -v "Available"|wc -l`;[[$result -ne 0]] && echo $result .+)**

AIX File & Folder Monitor

Contains the following rules:

- **File(/etc/aixmibd.conf) Has Changed - File(/etc/aixmibd.conf) Trigger (Exists)**
- **File(/etc/inetd.conf) Has Changed - File(/etc/inetd.conf) Trigger(exists)**
- **File(/etc/inittab) Has Changed - File(/etc/inittab) Trigger(Exists)**
- **File(/etc/security/login.cfg) Has Changed - File(/etc/security/login.cfg) Trigger(Exists)**
- **File(/var/spool/cron/crontabs/root) Has Changed - File (/var/spool/cron/crontabs/root) Trigger(Exists)**

CPU, Filesystem and Memory Monitor

Contains the following rules:

- **Monitor / filesystem used space - Group(Filesystem) Volume(/) Type (Filesystem Space Used %) Trigger(>=80%)**
- **Monitor /home filesystem used space - Group(Filesystem) Volume(/home) Type(Filesystem Space Used %) Trigger(>=80%)**
- **Monitor /opt filesystem used space - Group(Filesystem) Volume(/opt) Type(Filesystem Space Used %) Trigger(>=80%)**

- **Monitor /usr filesystem used space - Group(Filesystem) Volume(/usr) Type(Filesystem Space Used %) Trigger(>=80%)**
- **Monitor /var filesystem used space - Group(Filesystem) Volume(/var) Type(Filesystem Space Used %) Trigger(>=80%)**
- **Page File Used <30% (Suggests Too Much Paging Space) - Group (Memory) Type(Page File Used %) Trigger(< 30%)**
- **Page File Used > 70% (Suggests Not Enough Paging Space) - Group (Memory) Type(Page File Used %) Trigger(> 70%)**
- **Paging Space >70% - Group(Memory) Type(Page File Used %) Trigger(> 70%)**
- **Sustained CPU .80% - Group(CPU) CPU(0) Type(CPU Load) Trigger (>80%)**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

TIP: For a more detailed overview of these templates, download a copy of the Guide to AIX VIOS templates.

Linux Oracle JDE EnterpriseOne template

Oracle's JD Edwards EnterpriseOne is an integrated applications suite of comprehensive enterprise resource planning software.

The Linux Oracle JDE EnterpriseOne template contains the following components:

Script Monitor

Contains the following rule:

- **JDE: Monitor Overnight NIGHTOPR Batch Processes - Script(jdejobs nightopr ^([a-zA-Z0-9]+).*)**

File and Folder Monitor

Contains the following rule:

- **JDE: Monitor changes in JDE.INI - File or Folder(JDE_BASE\JDE.INI) Include(*) Trigger(Exists)**

Log File Monitor

Contains the following rule:

- **JDE: Monitor JDE LogFiles - LogFile(/var/log/jde/jde*) Expression(.+)**

> NOTE: Each log file to be monitored must be entered as a separate rule. Use the copy rule facility to save time.

Process Monitor

Contains the following rules:

- **JDE: Execute Submitted Jobs Process Active - Type(Process By Name) Process(runbatch) Trigger(Does Not Exist)**
- **JDE: Kernel Processes Active - Type(Process By Name) Process(jde_k) Trigger(Does Not Exist)**
- **JDE: Kernel Process Count - Type(Process By Name) Process(jde_k) Measure(NumberOfProcesses) Trigger(<4)**
- **JDE: Network Listener Process Active - Type(Process By Name) Process (jde_n) Trigger(Does Not Exist)**
- **JDE: Network Listener Process Count - Type(Process By Name) Process (jde_n) Measure(NumberOfProcesses) Trigger(<3)**

> NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux Oracle System Monitoring (Standard) template

The Oracle Linux System Monitoring (Standard) template contains rules covering all of the Linux Monitors with the exception of the System Monitor. The following rules are defined:

Linux Logical Volume Monitor

Contains the following rules:

- **Logical volume (LogVol00) status <> available - Measure(Status) Trigger (<> available)**
- **Logical volume (LogVol01) status <> available - Measure(Status) Trigger (<> available)**

Script Monitor

Contains the following rule:

- **Check for Failed Raid Drives - Script(mdadm -D /dev/md0 | grep Failed Devices 1|2|3)**

File & Folder Monitor

Contains the following rules:

- File (/etc/crontab) Has Changed - File(/etc/crontab) Trigger(Exists)
- File (/etc/inittab) Has Changed - File(/etc/inittab) Trigger(Exists)
- File (/etc/sendmail.cf) Has Changed - File(/etc/sendmail.cf) Trigger (Exists)
- File (/etc/profile) Has Changed - File(/etc/profile) Trigger(Exists)
- File (/etc/xinetd.conf) Has Changed - File(/etc/xinetd.conf) Trigger(Exists)

Log File Monitor

Contains the following rule:

- Monitor for Failed Logins in Secure Log - LogFile(/var/log/secure) Expression (failure)

CPU, Filesystem and Memory Monitor

Contains the following rules:

- Filesystem (/) Disk Space Used >=80% - Group(Filesystem) Volume(/) Type(Filesystem Space Used %) Trigger(>=80%)
- Filesystem (/) Does Not Exist - Group(Filesystem) Volume(/) Trigger(Does Not Exist)
- Filesystem (/) Inode Used >=90% - Group(Filesystem) Volume(/) Type(I-Nodes %) Trigger(>=90%)
- Paging Space >95% - Group(Memory) Type(Page File Used %) Trigger (>95%)
- Sustained CPU >95% - Group(CPU) CPU(0) Type(Load) Trigger(>95%)

Process Monitor

Contains the following rules:

- Critical Process (crond) Does Not Exist - Type(Process By Name) Process (crond) Trigger(DoesNotExist)
- Critical Process (gdm-binary) Does Not Exist - Type(Process By Name) Process(gdm-binary) Trigger(DoesNotExist)
- Critical Process (sshd) Does Not Exist - Type(Process By Name) Process (sshd) Trigger(DoesNotExist)

- **Critical Process (syslogd) Does Not Exist - Type(Process By Name) Process(syslogd) Trigger(DoesNotExist)**
- **Critical Process (xfs) Does Not Exist - Type(Process By Name) Process (xfs) Trigger(DoesNotExist)**
- **Critical Process (xinetd) Does Not Exist - Type(Process By Name) Process(xinetd) Trigger(DoesNotExist)**

Ping Monitor

Contains a single rule:

- **Check Server Can Ping Router - Host(1.2.3.4) Timeout(2000) Attempts(4) Success(50%) TTL(128)**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux Oracle System Monitoring (Advanced) template

The Oracle System Monitoring (Advanced) template contains all of the rules available in the Standard template and adds additional rule coverage.

File & Folder Monitor

Contains the standard plus the following rules:

- **File (/etc/resolv.conf) Has Changed - File(/etc/resolv.conf) Trigger(Exists)**
- **File (/etc/sysconfig/iptables) Has Changed - File(/etc/sysconfig/iptables) Trigger(Exists)**
- **File (/etc/vsftpd.conf) Has Changed - File(/etc/vsftpd.conf) Trigger(Exists)**

Log File Monitor

Contains the standard plus following rules:

- **Monitor for MySQL Errors - LogFile(/var/log/mysqld.log) Expression (error|failure)**
- **Monitor for Samba Errors - LogFile(/var/log/samba/smbd.log) Expression (error|failed)**

CPU, Filesystem and Memory Monitor

Contains the standard rules plus the following rules:

- Filesystem (/boot) Disk Space Used >=80% - Group(Filesystem) Volume (/boot) Type(Filesystem Space Used %) Trigger(>=80%)
- Filesystem (/boot) Does Not Exist - Group(Filesystem) Volume(/boot) Trigger(Does Not Exist)
- Filesystem (/boot) Inode Used >=90% - Group(Filesystem) Volume(/boot) Type(I-Nodes %) Trigger(>=90%)
- PageFile Used <30% (Suggests Too Much Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(<30%)
- PageFile Used >70% (Suggests Not Enough Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(>70%)

Process Monitor

Contains the standard rules plus the following rules:

- Optional Process (httpd) Does Not Exist - Type(Process By Name) Process(httpd) Trigger(DoesNotExist)
- Optional Process (mysqld) Does Not Exist - Type(Process By Name) Process(mysqld) Trigger(DoesNotExist)
- Optional Process (postmaster) Does Not Exist - Type(Process By Name) Process(postmaster) Trigger(DoesNotExist)
- Optional Process (rpc.idmapd) Does Not Exist - Type(Process By Name) Process(rpc.idmapd) Trigger(DoesNotExist)
- Optional Process (rpc.statd) Does Not Exist - Type(Process By Name) Process(rpc.statd) Trigger(DoesNotExist)
- Optional Process (sendmail) Does Not Exist - Type(Process By Name) Process(sendmail) Trigger(DoesNotExist)
- Optional Process (smbd) Does Not Exist - Type(Process By Name) Process(smbd) Trigger(DoesNotExist)
- Optional Process (spamd) Does Not Exist - Type(Process By Name) Process(spamd) Trigger(DoesNotExist)
- Optional Process (squid) Does Not Exist - Type(Process By Name) Process(squid) Trigger(DoesNotExist)
- Optional Process (vsftpd) Does Not Exist - Type(Process By Name) Process(vsftpd) Trigger(DoesNotExist)

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux Oracle MQ Monitor Template

IBM MQ is the most popular system for cross- platform messaging, providing assured delivery of messages across 35 plus IBM and non-IBM platforms, including IBM mainframe and midrange, Windows, AIX and Linux.

Central Configuration Manager contains a Linux Template for managing MQ installations running on Linux Oracle. This contains the following monitors:

Script Monitor

The script monitor is the engine-room of the MQ monitor. Use the script provided to interrogate an MQ environment.

The script is installed to, and must reside in **/var/lib/halcyon**

Configure the hmq.config file to point to the MQ installation namely:

• The location of the **runmqsc** command.

• The location of the **mqs.ini** file.

Contains the following rules:

- **MQ *SAMPLE* - Channel indicator running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CHINIT .+)**
- **MQ *SAMPLE* - Channel is RUNNING? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgqr LNX100.QM -monitor CHANNEL -name HALAIX61.HALAIX71 .+)**
- **MQ *SAMPLE* - Command Server running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CMDSERV .+)**
- **MQ *SAMPLE* - Connection count - Script(/bin/ksh /var/lib/halcyon/hq.sh -qmgr LNX100.QM -monitor CONNS -ge 20 .+)**
- **MQ *SAMPLE* - Dead Letter queue CURDEPTH > 0 - Script/bin.ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.DEAD.LETTER.QUEUE -gt 0 .+)**
- **MQ *SAMPLE* - Listener status - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LISTENER -name SYSTEM.DEFAULT.LISTENER.TCP .+)**
- **MQ *SAMPLE* - Message age test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor MSGAGE -name LNX100.QUEUE1 -ge 120 .+)**
- **MQ *SAMPLE* - Monitor the number of handles that are currently open for input for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr**

jupiter.queue.manager -monitor IPPROCS -name TEST.SEND.QUEUE -ge 25 .+)

- MQ *SAMPLE* - Monitor the number of handles that are currently open for output for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor OPPROCS -name TEST.SEND.QUEUE -ge 25 .+)
- MQ *SAMPLE* - QMGR Performance Events not enabled? - Script (/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor QMGR -name PERFMEV -value ENABLED .+)
- MQ *SAMPLE* - Queue depth percentage test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor QDEPTHCT -name TEST.SEND.QUEUE -ge 75 .+)
- MQ *SAMPLE* - Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name LNX100.QUEUE1 -ge 3 .+)
- MQ *SAMPLE* - Queue LASTGET test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 -ge120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 - ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE uncommitted message count - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor UNCOM -name TEST.SEND.QUEUE -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CHANNEL.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.CHANNEL.EVENT -ne 0 .+)

- MQ *SAMPLE* - SYSTEM.ADMIN.COMMAND.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.COMMAND.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CONFIG.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.CONFIG.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.LOGGER.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.LOGGER.EVENT -ne 0 .+)
- MQ *SAMPLE - SYSTEM.ADMIN.PERFM.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.PERFM.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.PUBSUB.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.PUBSUB.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.QMGR.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name SYSTEM.ADMIN.QMGR.EVENT -ne 0 .+)
- MQ *TEST* - Queue with wrong name - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor CURDEPTH -name HALAIX61.SEND.QPO -gt 10 .+)

File & Folder Monitor

Contains the following rules:

- *SAMPLE* MQ - Queue Manager .ini file permissions and ownership check. - File(/var/mqm/qmgrs/jupiter!queue!manager) Include(qm.ini) Trigger(Does Not Exist)
- *SAMPLE* Queue Manager Error log ownership and permissions - File (/var/mqm/qmgrs/jupiter!queue!Manager/errors) Include(AMQERR*.LOG) Trigger(Does Not Exist)
- MQ - /var/mqm directory permissions an ownership check. - Folder(/var) Include(mqm) Trigger(Does Not Exist)
- MQ - /var/mqm/config directory permissions and ownership check. - Folder(/var/mqm) Include(config) Trigger(Does Not Exist)
- MQ - /var/mqm/conv directory permissions and ownership check. - Folder (/var/mqm) Include(conv) Trigger(Does Not Exist)
- MQ - /var/mqm/errors directory permissions and ownership check. - Folder(/var/mqm) Include(errors) Trigger(Does Not Exist)

- MQ - /var/mqm/errors/*.FDC file(s) found - File(/var/mqm/errors) Include (*.FDC) Trigger(Exists)
- MQ - /var/mqm/exits directory permissions and ownership check. - Folder (/var/mqm) Include(exits) Trigger(Does Not Exist)
- MQ - /var/mqm/exits64 directory permissions and ownership check. - Folder(/var/mqm) Include(exits64) Trigger(Does Not Exist)
- MQ - /var/mqm/log directory permissions and ownership check. - Folder (/var/mqm) Include(log) Trigger(Does Not Exist)
- MQ - /var/mqm/mqft directory permissions and ownership check. - Folder (/var/mqm) Include(Mqft) Trigger(Does Not Exist)
- MQ - /var/mqm/mqs.ini file permissions, ownership and changed check. - (Mulitple Criteria Defined)
- MQ - /var/mqm/qmgrs directory permissions and ownership check. - Folder(/var/mqm) Include(qmgrs) Trigger(Does Not Exist)
- MQ - /var/mqm/shared directory permissions and ownership check. - Folder(/var/mqm) Include(shared) Trigger(Does Not Exist)
- MQ - /var/mqm/sockets directory permissions and ownership check. - Folder(/var/mqm) Include(sockets) Trigger(Does Not Exist)
- MQ - /var/mqm/trace directory permissions and ownership check. - Folder (/var/mqm) Include(trace) Trigger(Does Not Exist)

Log File Monitor

Contains the following rules:

- MQ Error monitor - AMQ5027 (The Listener has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5027*)
- MQ Error monitor - AMQ5041 (The queue manager task has ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQER01.LOG) Expression(^AMQ5041*)
- MQ Error monitor - AMQ5976 (WebSphere MQ Distributed Pub/Sub has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5976*)
- MQ Error monitor - AMQ6090 (WebSphere MQ was unable to display an error message) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6090*)

- MQ Error monitor - AMQ6119 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6119*)
- MQ Error monitor - AMQ6125 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6125*)
- MQ Error monitor - AMQ6183 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6183*)
- MQ Error monitor - AMQ6184 (An internal WebSphere MQ error has occurred on queue manager) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6184*)
- MQ Error monitor - AMQ7469 (Transactions rolled back to release log space) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ7469*)
- MQ Error monitor - AMQ8004 (WebSphere MQ queue manager ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8004*)
- MQ Error monitor - AMQ8101 (WebSphere MQ error (XXXXXXX) has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8101*)
- MQ Error monitor - AMQ8420 (Channel status not found) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8420*)
- MQ Error monitor - AMQ9001 (Channel ended normally) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9001*)
- MQ Error monitor - AMQ9202 (Remote host not available, retry) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9202*)
- MQ Error monitor - AMQ9208 (Error on receive from host) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9208*)

- MQ Error monitor - AMQ9209 (Connection to host XXXXXXXX closed) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9209*)
- MQ Error monitor - AMQ9213 (A communications error for XXXXXXXX occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9213*)
- MQ Error monitor - AMQ9218 (The TCP/IP listener program could not bind to port number) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9218*)
- MQ Error monitor - AMQ9228 (The XXXXXXXX responder program could not be started) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9228*)
- MQ Error monitor - AMQ9503 (Channel negotiation failed) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9503*)
- MQ Error monitor - AMQ9513 (Maximum number of channels reached) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9513*)
- MQ Error monitor - AMQ9526 (Message sequence number error for channel XXXXXXXX) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9526*)
- MQ Error monitor - AMQ9542 (Queue manager is ending) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9542*)
- MQ Error monitor - AMQ9999 (Channel to host ended abnormally) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9999*)
- MQ FFST record (.FDC file) *SAMPLE* - LogFile(/var/adm/syslog) Expression(.+FFST record created in .+)

Process Monitor

Contains the following rules:

- MQ Monitor - Broker worker process (amqfcxba) not active - Type(Process By Name) Process(amqfcxba) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(runmqchi) not active - Type(Process By Name) Process(runmqchi) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(amqrmppa) not active - Type(Process By Name) Process(amqrmppa) Trigger(Does Not Exist)
- MQ Monitor - Channel process manager(amqzmuc0) not active - Type (Process By Name) Process(amqzmuc0) Trigger(Does Not Exist)
- MQ Monitor - Dead letter queue handler(runmqdlq) not active - Type (Process By Name) Process(runmqdlq) Trigger(Does Not Exist)
- MQ Monitor - LQM Agents (amqzlaa0) not active - Type(Process By Name) Process(amqzlaa0) Trigger(Does Not Exist)
- MQ Monitor - LU62 receiver channel and client connection (amqcrs6b) not active - Type(Process By Name) Process(amqcrs6b) Trigger(Does Not Exist)
- MQ Monitor - MQ listener (runmqlsr) not active - Type(Process By Name) Process(runmqlsr) Trigger(Does Not Exist)
- MQ Monitor - Object Authority Manager (amqzfuma) not active - Type (Process By Name) Process(amqzfuma) Trigger(Does Not Exist)
- MQ Monitor -Process controller(amqzmgr0) not active - Type(Process By Name) Process(amqzmgr0) Trigger(Does Not Exist)
- MQ Monitor - Processing controller (amqzxma0) not active - Type(Process By Name) Process(amqzxma0) Trigger(Does Not Exist)
- MQ Monitor - Publish subscribe process (amqfqpub) not active - Type (Process By Name) Process(amqfqpub) Trigger(Does Not Exist)
- MQ Monitor - PubSub restartable utility manager (amqzmuf0) not active - Type(Process By Name) Process(amqzmuf0) Trigger(Does Not Exist)
- MQ Monitor - Queue manager agent (amqzsla0) not active - Type(Process By Name) Process(amqzsla0) Trigger(Does Not Exist)
- MQ Monitor - Repository process (amqrrmfa) not active - Type(Process By Name) Process(amqrrmfa) Trigger(Does Not Exist)
- MQ Monitor - Restartable process manager (amqzmur0) not active - Type (Process By Name) Process(amqzmur0) Trigger(Does Not Exist)
- MQ Monitor -TCP/IP-invoked channel responder (amqcrsta) not active - Type(Process By Name) Process(amqcrsta) Trigger(Does Not Exist)

- MQ Monitor - The command server (amqpcesa) not active - Type(Process By Name) Process(amqpcesa) Trigger(Does Not Exist)
- MQ Monitor - Trigger monitor (runmqtrm) not active - Type(Process By Name) Process(runmqtrm) Trigger(Does Not Exist)

Linux RED HAT System Monitoring (Standard) template

The RED HAT System Monitoring (Standard) template contains rules covering all of the Linux Monitors with the exception of the System Monitor. The following rules are defined:

Linux Logical Volume Monitor

Contains the following rules:

- **Logical volume (LogVol00) status <> available - Measure(Status) Trigger (<> available)**
- **Logical volume (LogVol01) status <> available - Measure(Status) Trigger (<> available)**

Script Monitor

Contains the following rules:

- **Check for Failed Raid Drives - Script(mdadm -D /dev/md0 | grep Failed Devices 1|2|3)**
- **Zombie process - Report on all - Script(ps -eo stat,pid | egrep “^Z” | awk ‘{print $2}’ ^[^$])**
- **Zombie process count - Script(ps -eo stat,pid | egrep “^Z” | wc -l ^[^0])**

File & Folder Monitor

Contains the following rules:

- **File (/etc/crontab) Has Changed - File(/etc/crontab) Trigger(Exists)**
- **File (/etc/inittab) Has Changed - File(/etc/inittab) Trigger(Exists)**
- **File (/etc/sendmail.cf) Has Changed - File(/etc/mail/sendmail.cf) Trigger (Exists)**
- **File (/etc/profile) Has Changed - File(/etc/profile) Trigger(Exists)**
- **File (/etc/xinetd.conf) Has Changed - File(/etc/xinetd.conf) Trigger(Exists)**

Log File Monitor

Contains the following rule:

- **Monitor for Failed Logins in Secure Log - LogFile(/var/log/secure) Expression (failure)**

CPU, Filesystem and Memory Monitor

Contains the following rules:

- Filesystem (/) Disk Space Used >=80% - Group(Filesystem) Volume(/) Type(Filesystem Space Used %) Trigger(>=80%)
- Filesystem (/) Does Not Exist - Group(Filesystem) Volume(/) Trigger(Does Not Exist)
- Filesystem (/) Inode Used >=90% - Group(Filesystem) Volume(/) Type(I-Nodes %) Trigger(>=90%)
- Paging Space >95% - Group(Memory) Type(Page File Used %) Trigger (>95%)
- Sustained CPU >95% - Group(CPU) CPU(0) Type(Load) Trigger(>95%)

Process Monitor

Contains the following rules:

- **Critical Process (crond) Does Not Exist - Type(Process By Name) Process (crond) Trigger(DoesNotExist)**
- **Critical Process (gdm-binary) Does Not Exist - Type(Process By Name) Process(gdm-binary) Trigger(DoesNotExist)**
- **Critical Process (sshd) Does Not Exist - Type(Process By Name) Process (sshd) Trigger(DoesNotExist)**
- **Critical Process (syslogd) Does Not Exist - Type(Process By Name) Process(syslogd) Trigger(DoesNotExist)**
- **Critical Process (xfs) Does Not Exist - Type(Process By Name) Process (xfs) Trigger(DoesNotExist)**
- **Critical Process (xinetd) Does Not Exist - Type(Process By Name) Process(xinetd) Trigger(DoesNotExist)**

Ping Monitor

Contains a single rule:

- **Check Server Can Ping Router - Host(1.2.3.4) Timeout(2000) Attempts(4) Success(50%) TTL(128)**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux RED HAT System Monitoring (Advanced) template

The Linux RED HAT System Monitoring (Advanced) template contains all of the rules available in the Standard template and adds additional rule coverage.

File & Folder Monitor

Contains the standard rules plus these rules:

- **File (/etc/resolv.conf) Has Changed - File(/etc/) Trigger(Exists)**
- **File (/etc/sysconfig/iptables) Has Changed - File(/etc/sysconfig) Trigger (Exists)**
- **File (/etc/vsftpd.conf) Has Changed - File(/etc/vsftpd) Trigger(Exists)**

Log File Monitor

Contains the standard rule plus these rules:

- Monitor for MySQL Errors - LogFile(/var/log/mysqld.log) Expression (error|failure)
- Monitor for Samba Errors - LogFile(/var/log/samba/smbd.log) Expression (error|failed)

CPU, Filesystem and Memory Monitor

Contains the standard rules plus these rules:

- **Filesystem (/boot) Disk Space Used >=80% - Group(Filesystem) Volume (/boot) Type(Filesystem Space Used %) Trigger(>=80%)**
- **Filesystem (/boot) Does Not Exist - Group(Filesystem) Volume(/boot) Trigger(Does Not Exist)**
- **Filesystem (/boot) Inode Used >=90% - Group(Filesystem) Volume(/boot) Type(I-Nodes %) Trigger(>=90%)**
- **PageFile Used <30% (Suggests Too Much Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(<30%)**
- **PageFile Used >70% (Suggests Not Enough Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(>70%)**

Process Monitor

Contains the standard rules plus these rules:

- **Optional Process (httpd) Does Not Exist - Type(Process By Name) Process(httpd) Trigger(DoesNotExist)**
- **Optional Process (mysqld) Does Not Exist - Type(Process By Name) Process(mysqld) Trigger(DoesNotExist)**
- **Optional Process (postmaster) Does Not Exist - Type(Process By Name) Process(postmaster) Trigger(DoesNotExist)**
- **Optional Process (rpc.idmapd) Does Not Exist - Type(Process By Name) Process(rpc.idmapd) Trigger(DoesNotExist)**
- **Optional Process (rpc.statd) Does Not Exist - Type(Process By Name) Process(rpc.statd) Trigger(DoesNotExist)**
- **Optional Process (sendmail) Does Not Exist - Type(Process By Name) Process(sendmail) Trigger(DoesNotExist)**
- **Optional Process (smbd) Does Not Exist - Type(Process By Name) Process(smbd) Trigger(DoesNotExist)**
- **Optional Process (spamd) Does Not Exist - Type(Process By Name) Process(spamd) Trigger(DoesNotExist)**
- **Optional Process (squid) Does Not Exist - Type(Process By Name) Process(squid) Trigger(DoesNotExist)**
- **Optional Process (vsftpd) Does Not Exist - Type(Process By Name) Process(vsftpd) Trigger(DoesNotExist)**

NOTE: All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux Red Hat MQ Monitor Template

IBM MQ is the most popular system for cross- platform messaging, providing assured delivery of messages across 35 plus IBM and non-IBM platforms, including IBM mainframe and midrange, Windows, AIX and Linux.

Central Configuration Manager contains a Linux Template for managing MQ installations running on Linux Red Hat. This contains the following monitors:

Script Monitor

The script monitor is the engine-room of the MQ monitor. Use the script provided to interrogate an MQ environment.

The script is installed to, and must reside in **/var/lib/halcyon**

Configure the hmq.config file to point to the MQ installation namely:

• The location of the **runmqsc** command.

• The location of the **mqs.ini** file.

Contains the following rules:

- **MQ *SAMPLE* - Channel indicator running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CHINIT .+)**
- **MQ *SAMPLE* - Channel is RUNNING? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgqr LNX100.QM -monitor CHANNEL -name HALAIX61.HALAIX71 .+)**
- **MQ *SAMPLE* - Command Server running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CMDSERV .+)**
- **MQ *SAMPLE* - Connection count - Script(/bin/ksh /var/lib/halcyon/hq.sh -qmgr LNX100.QM -monitor CONNS -ge 20 .+)**
- **MQ *SAMPLE* - Dead Letter queue CURDEPTH > 0 - Script/bin.ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.DEAD.LETTER.QUEUE -gt 0 .+)**
- **MQ *SAMPLE* - Listener status - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LISTENER -name SYSTEM.DEFAULT.LISTENER.TCP .+)**

- MQ *SAMPLE* - Message age test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor MSGAGE -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - Monitor the number of handles that are currently open for input for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor IPPROCS -name TEST.SEND.QUEUE -ge 25 .+)
- MQ *SAMPLE* - Monitor the number of handles that are currently open for output for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor OPPROCS -name TEST.SEND.QUEUE -ge 25 .+)
- MQ *SAMPLE* - QMGR Performance Events not enabled? - Script (/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor QMGR -name PERFMEV -value ENABLED .+)
- MQ *SAMPLE* - Queue depth percentage test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor QDEPTHCT -name TEST.SEND.QUEUE -ge 75 .+)
- MQ *SAMPLE* - Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name LNX100.QUEUE1 -ge 3 .+)
- MQ *SAMPLE* - Queue LASTGET test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 -ge120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 - ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)

- MQ *SAMPLE* - QUEUE uncommitted message count - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor UNCOM -name TEST.SEND.QUEUE -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CHANNEL.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.CHANNEL.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.COMMAND.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.COMMAND.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CONFIG.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.CONFIG.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.LOGGER.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.LOGGER.EVENT -ne 0 .+)
- MQ *SAMPLE - SYSTEM.ADMIN.PERFM.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.PERFM.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.PUBSUB.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.PUBSUB.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.QMGR.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name SYSTEM.ADMIN.QMGR.EVENT -ne 0 .+)
- MQ *TEST* - Queue with wrong name - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor CURDEPTH -name SYSTEM.DEFAULT.SEND.QPO -gt 10 .+)

File & Folder Monitor

Contains the following rules:

- *SAMPLE* MQ - Queue Manager .ini file permissions and ownership check. - File(/var/mqm/qmgrs/jupiter!queue!manager) Include(qm.ini) Trigger(Does Not Exist)
- *SAMPLE* Queue Manager Error log ownership and permissions - File (/var/mqm/qmgrs/jupiter!queue!Manager/errors) Include(AMQERR*.LOG) Trigger(Does Not Exist)
- MQ - /var/mqm directory permissions an ownership check. - Folder(/var) Include(mqm) Trigger(Does Not Exist)
- MQ - /var/mqm/config directory permissions and ownership check. - Folder(/var/mqm) Include(config) Trigger(Does Not Exist)
- MQ - /var/mqm/conv directory permissions and ownership check. - Folder (/var/mqm) Include(conv) Trigger(Does Not Exist)
- MQ - /var/mqm/errors directory permissions and ownership check. - Folder(/var/mqm) Include(errors) Trigger(Does Not Exist)
- MQ - /var/mqm/errors/*.FDC file(s) found - File(/var/mqm/errors) Include (*.FDC) Trigger(Exists)
- MQ - /var/mqm/exits directory permissions and ownership check. - Folder (/var/mqm) Include(exits) Trigger(Does Not Exist)
- MQ - /var/mqm/exits64 directory permissions and ownership check. - Folder(/var/mqm) Include(exits64) Trigger(Does Not Exist)
- MQ - /var/mqm/log directory permissions and ownership check. - Folder (/var/mqm) Include(log) Trigger(Does Not Exist)
- MQ - /var/mqm/mqft directory permissions and ownership check. - Folder (/var/mqm) Include(Mqft) Trigger(Does Not Exist)
- MQ - /var/mqm/mqs.ini file permissions, ownership and changed check. - (Mulitple Criteria Defined)
- MQ - /var/mqm/qmgrs directory permissions and ownership check. - Folder(/var/mqm) Include(qmgrs) Trigger(Does Not Exist)
- MQ - /var/mqm/shared directory permissions and ownership check. - Folder(/var/mqm) Include(shared) Trigger(Does Not Exist)
- MQ - /var/mqm/sockets directory permissions and ownership check. - Folder(/var/mqm) Include(sockets) Trigger(Does Not Exist)
- MQ - /var/mqm/trace directory permissions and ownership check. - Folder (/var/mqm) Include(trace) Trigger(Does Not Exist)

Log File Monitor

Contains the following rules:

- MQ Error monitor - AMQ5027 (The Listener has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5027*)
- MQ Error monitor - AMQ5041 (The queue manager task has ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQER01.LOG) Expression(^AMQ5041*)
- MQ Error monitor - AMQ5976 (WebSphere MQ Distributed Pub/Sub has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5976*)
- MQ Error monitor - AMQ6090 (WebSphere MQ was unable to display an error message) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6090*)
- MQ Error monitor - AMQ6119 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6119*)
- MQ Error monitor - AMQ6125 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6125*)
- MQ Error monitor - AMQ6183 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6183*)
- MQ Error monitor - AMQ6184 (An internal WebSphere MQ error has occurred on queue manager) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6184*)
- MQ Error monitor - AMQ7469 (Transactions rolled back to release log space) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ7469*)
- MQ Error monitor - AMQ8004 (WebSphere MQ queue manager ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8004*)

- MQ Error monitor - AMQ8101 (WebSphere MQ error (XXXXXXX) has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8101*)
- MQ Error monitor - AMQ8420 (Channel status not found) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8420*)
- MQ Error monitor - AMQ9001 (Channel ended normally) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9001*)
- MQ Error monitor - AMQ9202 (Remote host not available, retry) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9202*)
- MQ Error monitor - AMQ9208 (Error on receive from host) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9208*)
- MQ Error monitor - AMQ9209 (Connection to host XXXXXXXX closed) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9209*)
- MQ Error monitor - AMQ9213 (A communications error for XXXXXXXX occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9213*)
- MQ Error monitor - AMQ9218 (The TCP/IP listener program could not bind to port number) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9218*)
- MQ Error monitor - AMQ9228 (The XXXXXXXX responder program could not be started) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9228*)
- MQ Error monitor - AMQ9503 (Channel negotiation failed) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9503*)
- MQ Error monitor - AMQ9513 (Maximum number of channels reached) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9513*)
- MQ Error monitor - AMQ9526 (Message sequence number error for channel XXXXXXXX) - LogFile

(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9526*)

- MQ Error monitor - AMQ9542 (Queue manager is ending) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9542*)
- MQ Error monitor - AMQ9999 (Channel to host ended abnormally) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9999*)
- MQ FFST record (.FDC file) *SAMPLE* - LogFile(/var/adm/syslog) Expression(.+FFST record created in .+)

Process Monitor

Contains the following rules:

- MQ Monitor - Broker worker process (amqfcxba) not active - Type(Process By Name) Process(amqfcxba) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(runmqchi) not active - Type(Process By Name) Process(runmqchi) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(amqrmppa) not active - Type(Process By Name) Process(amqrmppa) Trigger(Does Not Exist)
- MQ Monitor - Channel process manager(amqzmuc0) not active - Type (Process By Name) Process(amqzmuc0) Trigger(Does Not Exist)
- MQ Monitor - Dead letter queue handler(runmqdlq) not active - Type (Process By Name) Process(runmqdlq) Trigger(Does Not Exist)
- MQ Monitor - LQM Agents (amqzlaa0) not active - Type(Process By Name) Process(amqzlaa0) Trigger(Does Not Exist)
- MQ Monitor - LU62 receiver channel and client connection (amqcrs6b) not active - Type(Process By Name) Process(amqcrs6b) Trigger(Does Not Exist)
- MQ Monitor - MQ listener (runmqlsr) not active - Type(Process By Name) Process(runmqlsr) Trigger(Does Not Exist)
- MQ Monitor - Object Authority Manager (amqzfuma) not active - Type (Process By Name) Process(amqzfuma) Trigger(Does Not Exist)
- MQ Monitor -Process controller(amqzmgr0) not active - Type(Process By Name) Process(amqzmgr0) Trigger(Does Not Exist)
- MQ Monitor - Processing controller (amqzxma0) not active - Type(Process By Name) Process(amqzxma0) Trigger(Does Not Exist)
- MQ Monitor - Publish subscribe process (amqfqpub) not active - Type (Process By Name) Process(amqfqpub) Trigger(Does Not Exist)

- MQ Monitor - PubSub restartable utility manager (amqzmuf0) not active - Type(Process By Name) Process(amqzmuf0) Trigger(Does Not Exist)
- MQ Monitor - Queue manager agent (amqzsla0) not active - Type(Process By Name) Process(amqzsla0) Trigger(Does Not Exist)
- MQ Monitor - Repository process (amqrrmfa) not active - Type(Process By Name) Process(amqrrmfa) Trigger(Does Not Exist)
- MQ Monitor - Restartable process manager (amqzmur0) not active - Type (Process By Name) Process(amqzmur0) Trigger(Does Not Exist)
- MQ Monitor -TCP/IP-invoked channel responder (amqcrsta) not active - Type(Process By Name) Process(amqcrsta) Trigger(Does Not Exist)
- MQ Monitor - The command server (amqpcesa) not active - Type(Process By Name) Process(amqpcesa) Trigger(Does Not Exist)
- MQ Monitor - Trigger monitor (runmqtrm) not active - Type(Process By Name) Process(runmqtrm) Trigger(Does Not Exist)

Linux SUSE System Monitoring (Standard) template

The Linux SUSE System Monitoring (Standard) template contains rules covering all of the Linux Monitors with the exception of the System Monitor. The following rules are defined:

Linux Logical Volume Monitor

Contains the following rules:

- Logical volume (LogVol00) status <> available - Measure(Status) Trigger (<> available)
- Logical volume (LogVol01) status <> available - Measure(Status) Trigger (<> available)

Script Monitor

Contains the following rules:

- Check for Failed Raid Drives - Script(mdadm -D /dev/md0 | grep Failed Devices 1|2|3)
- Zombie process - Report on all - Script(ps -eo stat,pid | egrep “^Z” | awk ‘{print $2}’ ^[^$])
- Zombie process count - Script(ps -eo stat,pid | egrep “^Z” | wc -l ^[^0])

File & Folder Monitor

Contains the following rules:

- File (/etc/crontab) Has Changed - File(/etc/) Trigger(Exists)
- File (/etc/inittab) Has Changed - File(/etc/) Trigger(Exists)
- File (/etc/sendmail.cf) Has Changed - File(/etc/mail) Trigger(Exists)
- File (/etc/profile) Has Changed - File(/etc/) Trigger(Exists)
- File (/etc/xinetd.conf) Has Changed - File(/etc/) Trigger(Exists)

Log File Monitor

Contains the following rule:

- Monitor for Failures in Messages Log - LogFile(/var/log/messages) Expression (error|fail)

CPU, Filesystem and Memory Monitor

Contains the following rules:

- Filesystem (/) Disk Space Used >=80% - Group(Filesystem) Volume(/) Type(Filesystem Space Used %) Trigger(>=80%)
- Filesystem (/) Does Not Exist - Group(Filesystem) Volume(/) Trigger(Does Not Exist)
- Filesystem (/) Inode Used >=90% - Group(Filesystem) Volume(/) Type(I-Nodes %) Trigger(>=90%)
- Paging Space >95% - Group(Memory) Type(Page File Used %) Trigger (>95%)
- Sustained CPU >95% - Group(CPU) CPU(0) Type(Load) Trigger(>95%)

Process Monitor

Contains the following rules:

- Critical Process (crond) Does Not Exist - Type(Process By Name) Process (crond) Trigger(DoesNotExist)
- Critical Process (gdm-binary) Does Not Exist - Type(Process By Name) Process(gdm-binary) Trigger(DoesNotExist)
- Critical Process (sshd) Does Not Exist - Type(Process By Name) Process (sshd) Trigger(DoesNotExist)
- Critical Process (syslogd) Does Not Exist - Type(Process By Name) Process(syslogd) Trigger(DoesNotExist)
- Critical Process (xfs) Does Not Exist - Type(Process By Name) Process (xfs) Trigger(DoesNotExist)

- **Critical Process (xinetd) Does Not Exist - Type(Process By Name) Process(xinetd) Trigger(DoesNotExist)**

Ping Monitor

Contains a single rule:

- **Check Server Can Ping Router - Host(1.2.3.4) Timeout(2000) Attempts(4) Success(50%) TTL(128)**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux SUSE System Monitoring (Advanced) template

The Linux SUSE System Monitoring (Advanced) template contains all of the rules available in the Standard template and adds additional rule coverage.

File & Folder Monitor

Contains the standard rules plus these rules:

- **File (/etc/resolv.conf) Has Changed - File(/etc/) Trigger(Exists)**
- **File (/etc/sysconfig/iptables) Has Changed - File(/etc/sysconfig) Trigger (Exists)**
- **File (/etc/vsftpd.conf) Has Changed - File(/etc/vsftpd) Trigger(Exists)**

Log File Monitor

Contains the standard rule plus these rules:

- **Monitor for MySQL Errors - LogFile(/var/log/mysqld.log) Expression (error|failure)**
- **Monitor for Samba Errors - LogFile(/var/log/samba/smbd.log) Expression (error|failed)**

CPU, Filesystem and Memory Monitor

Contains the standard rules plus these five rules:

- **Filesystem (/boot) Disk Space Used >=80% - Group(Filesystem) Volume (/boot) Type(Filesystem Space Used %) Trigger(>=80%)**
- **Filesystem (/boot) Does Not Exist - Group(Filesystem) Volume(/boot) Trigger(Does Not Exist)**

- **Filesystem (/boot) Inode Used >=90% - Group(Filesystem) Volume(/boot) Type(I-Nodes %) Trigger(>=90%)**
- **PageFile Used <30% (Suggests Too Much Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(<30%)**
- **PageFile Used >70% (Suggests Not Enough Paging Space) - Group (Memory) Type(UsedPageFilePercent) Trigger(>70%)**

Process Monitor

Contains the standard rules plus these additional rules:

- **Optional Process (httpd) Does Not Exist - Type(Process By Name) Process(httpd) Trigger(DoesNotExist)**
- **Optional Process (mysqld) Does Not Exist - Type(Process By Name) Process(mysqld) Trigger(DoesNotExist)**
- **Optional Process (postmaster) Does Not Exist - Type(Process By Name) Process(postmaster) Trigger(DoesNotExist)**
- **Optional Process (rpc.idmapd) Does Not Exist - Type(Process By Name) Process(rpc.idmapd) Trigger(DoesNotExist)**
- **Optional Process (rpc.statd) Does Not Exist - Type(Process By Name) Process(rpc.statd) Trigger(DoesNotExist)**
- **Optional Process (sendmail) Does Not Exist - Type(Process By Name) Process(sendmail) Trigger(DoesNotExist)**
- **Optional Process (smbd) Does Not Exist - Type(Process By Name) Process(smbd) Trigger(DoesNotExist)**
- **Optional Process (spamd) Does Not Exist - Type(Process By Name) Process(spamd) Trigger(DoesNotExist)**
- **Optional Process (squid) Does Not Exist - Type(Process By Name) Process(squid) Trigger(DoesNotExist)**
- **Optional Process (vsftpd) Does Not Exist - Type(Process By Name) Process(vsftpd) Trigger(DoesNotExist)**

> **NOTE:** All actions for each of the above rules within this template are set to a default of sending an alert to the Enterprise Console. You must manually change this setting if you require an alternative action to be taken upon the generation of an alert.

Linux SUSE MQ Monitor Template

IBM MQ is the most popular system for cross- platform messaging, providing assured delivery of messages across 35 plus IBM and non-IBM platforms, including IBM mainframe and midrange, Windows, AIX and Linux.

Central Configuration Manager contains a Linux Template for managing MQ installations running on Linux SUSE. This contains the following monitors:

Script Monitor

The script monitor is the engine-room of the MQ monitor. Use the script provided to interrogate an MQ environment.

The script is installed to, and must reside in **/var/lib/halcyon**

Configure the hmq.config file to point to the MQ installation namely:

• The location of the **runmqsc** command.

• The location of the **mqs.ini** file.

Contains the following rules:

- **MQ *SAMPLE* - Channel indicator running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CHINIT .+)**
- **MQ *SAMPLE* - Channel is RUNNING? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgqr LNX100.QM -monitor CHANNEL -name HALAIX61.HALAIX71 .+)**
- **MQ *SAMPLE* - Command Server running? - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CMDSERV .+)**
- **MQ *SAMPLE* - Connection count - Script(/bin/ksh /var/lib/halcyon/hq.sh -qmgr LNX100.QM -monitor CONNS -ge 20 .+)**
- **MQ *SAMPLE* - Dead Letter queue CURDEPTH > 0 - Script/bin.ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.DEAD.LETTER.QUEUE -gt 0 .+)**
- **MQ *SAMPLE* - Listener status - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LISTENER -name SYSTEM.DEFAULT.LISTENER.TCP .+)**
- **MQ *SAMPLE* - Message age test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor MSGAGE -name LNX100.QUEUE1 -ge 120 .+)**
- **MQ *SAMPLE* - Monitor the number of handles that are currently open for input for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor IPPROCS -name TEST.SEND.QUEUE -ge 25 .+)**

- MQ *SAMPLE* - Monitor the number of handles that are currently open for output for the queue - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor OPPROCS -name TEST.SEND.QUEUE -ge 25 .+)
- MQ *SAMPLE* - QMGR Performance Events not enabled? - Script (/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor QMGR -name PERFMEV -value ENABLED .+)
- MQ *SAMPLE* - Queue depth percentage test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor QDEPTHCT -name TEST.SEND.QUEUE -ge 75 .+)
- MQ *SAMPLE* - Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name LNX100.QUEUE1 -ge 3 .+)
- MQ *SAMPLE* - Queue LASTGET test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 -ge120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - Queue LASTGET test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTGET -name LNX100.QUEUE1 - ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (All day) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Daytime) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE LASTPUT test (Overnight) - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor LASTPUT -name LNX100.QUEUE1 -ge 120 .+)
- MQ *SAMPLE* - QUEUE uncommitted message count - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor UNCOM -name TEST.SEND.QUEUE -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.CHANNEL.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.CHANNEL.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.COMMAND.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.COMMAND.EVENT -ne 0 .+)

- MQ *SAMPLE* - SYSTEM.ADMIN.CONFIG.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.CONFIG.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.LOGGER.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.LOGGER.EVENT -ne 0 .+)
- MQ *SAMPLE - SYSTEM.ADMIN.PERFM.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.PERFM.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.PUBSUB.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM -monitor CURDEPTH -name SYSTEM.ADMIN.PUBSUB.EVENT -ne 0 .+)
- MQ *SAMPLE* - SYSTEM.ADMIN.QMGR.EVENT Queue depth test - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr jupiter.queue.manager -monitor CURDEPTH -name SYSTEM.ADMIN.QMGR.EVENT -ne 0 .+)
- MQ *TEST* - Queue with wrong name - Script(/bin/ksh /var/lib/halcyon/hmq.sh -qmgr LNX100.QM - monitor CURDEPTH -name HALAIX61.SEND.QPO -gt 10 .+)

File & Folder Monitor

Contains the following rules:

- *SAMPLE* MQ - Queue Manager .ini file permissions and ownership check. - File(/var/mqm/qmgrs/jupiter!queue!manager) Include(qm.ini) Trigger(Does Not Exist)
- *SAMPLE* Queue Manager Error log ownership and permissions - File (/var/mqm/qmgrs/jupiter!queue!Manager/errors) Include(AMQERR*.LOG) Trigger(Does Not Exist)
- MQ - /var/mqm directory permissions an ownership check. - Folder(/var) Include(mqm) Trigger(Does Not Exist)
- MQ - /var/mqm/config directory permissions and ownership check. - Folder(/var/mqm) Include(config) Trigger(Does Not Exist)
- MQ - /var/mqm/conv directory permissions and ownership check. - Folder (/var/mqm) Include(conv) Trigger(Does Not Exist)
- MQ - /var/mqm/errors directory permissions and ownership check. - Folder(/var/mqm) Include(errors) Trigger(Does Not Exist)
- MQ - /var/mqm/errors/*.FDC file(s) found - File(/var/mqm/errors) Include (*.FDC) Trigger(Exists)
- MQ - /var/mqm/exits directory permissions and ownership check. - Folder (/var/mqm) Include(exits) Trigger(Does Not Exist)

- MQ - /var/mqm/exits64 directory permissions and ownership check. - Folder(/var/mqm) Include(exits64) Trigger(Does Not Exist)
- MQ - /var/mqm/log directory permissions and ownership check. - Folder (/var/mqm) Include(log) Trigger(Does Not Exist)
- MQ - /var/mqm/mqft directory permissions and ownership check. - Folder (/var/mqm) Include(Mqft) Trigger(Does Not Exist)
- MQ - /var/mqm/mqs.ini file permissions, ownership and changed check. - (Mulitple Criteria Defined)
- MQ - /var/mqm/qmgrs directory permissions and ownership check. - Folder(/var/mqm) Include(qmgrs) Trigger(Does Not Exist)
- MQ - /var/mqm/shared directory permissions and ownership check. - Folder(/var/mqm) Include(shared) Trigger(Does Not Exist)
- MQ - /var/mqm/sockets directory permissions and ownership check. - Folder(/var/mqm) Include(sockets) Trigger(Does Not Exist)
- MQ - /var/mqm/trace directory permissions and ownership check. - Folder (/var/mqm) Include(trace) Trigger(Does Not Exist)

Log File Monitor

Contains the following rules:

- MQ Error monitor - AMQ5027 (The Listener has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5027*)
- MQ Error monitor - AMQ5041 (The queue manager task has ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQER01.LOG) Expression(^AMQ5041*)
- MQ Error monitor - AMQ5976 (WebSphere MQ Distributed Pub/Sub has ended) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ5976*)
- MQ Error monitor - AMQ6090 (WebSphere MQ was unable to display an error message) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6090*)
- MQ Error monitor - AMQ6119 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6119*)

- MQ Error monitor - AMQ6125 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6125*)
- MQ Error monitor - AMQ6183 (An internal WebSphere MQ error has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6183*)
- MQ Error monitor - AMQ6184 (An internal WebSphere MQ error has occurred on queue manager) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ6184*)
- MQ Error monitor - AMQ7469 (Transactions rolled back to release log space) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ7469*)
- MQ Error monitor - AMQ8004 (WebSphere MQ queue manager ended) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8004*)
- MQ Error monitor - AMQ8101 (WebSphere MQ error (XXXXXXX) has occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8101*)
- MQ Error monitor - AMQ8420 (Channel status not found) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ8420*)
- MQ Error monitor - AMQ9001 (Channel ended normally) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9001*)
- MQ Error monitor - AMQ9202 (Remote host not available, retry) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9202*)
- MQ Error monitor - AMQ9208 (Error on receive from host) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9208*)
- MQ Error monitor - AMQ9209 (Connection to host XXXXXXXX closed) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9209*)

- MQ Error monitor - AMQ9213 (A communications error for XXXXXXXX occurred) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9213*)
- MQ Error monitor - AMQ9218 (The TCP/IP listener program could not bind to port number) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9218*)
- MQ Error monitor - AMQ9228 (The XXXXXXXX responder program could not be started) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9228*)
- MQ Error monitor - AMQ9503 (Channel negotiation failed) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9503*)
- MQ Error monitor - AMQ9513 (Maximum number of channels reached) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9513*)
- MQ Error monitor - AMQ9526 (Message sequence number error for channel XXXXXXXX) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9526*)
- MQ Error monitor - AMQ9542 (Queue manager is ending) - LogFile (/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9542*)
- MQ Error monitor - AMQ9999 (Channel to host ended abnormally) - LogFile(/var/mqm/qmgrs/jupiter!queue!manager/errors/AMQERR01.LOG) Expression(^AMQ9999*)
- MQ FFST record (.FDC file) *SAMPLE* - LogFile(/var/adm/syslog) Expression(.+FFST record created in .+)

Process Monitor

Contains the following rules:

- MQ Monitor - Broker worker process (amqfcxba) not active - Type(Process By Name) Process(amqfcxba) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(runmqchi) not active - Type(Process By Name) Process(runmqchi) Trigger(Does Not Exist)
- MQ Monitor - Channel initiator(amqrmppa) not active - Type(Process By Name) Process(amqrmppa) Trigger(Does Not Exist)

- MQ Monitor - Channel process manager(amqzmuc0) not active - Type (Process By Name) Process(amqzmuc0) Trigger(Does Not Exist)
- MQ Monitor - Dead letter queue handler(runmqdlq) not active - Type (Process By Name) Process(runmqdlq) Trigger(Does Not Exist)
- MQ Monitor - LQM Agents (amqzlaa0) not active - Type(Process By Name) Process(amqzlaa0) Trigger(Does Not Exist)
- MQ Monitor - LU62 receiver channel and client connection (amqcrs6b) not active - Type(Process By Name) Process(amqcrs6b) Trigger(Does Not Exist)
- MQ Monitor - MQ listener (runmqlsr) not active - Type(Process By Name) Process(runmqlsr) Trigger(Does Not Exist)
- MQ Monitor - Object Authority Manager (amqzfuma) not active - Type (Process By Name) Process(amqzfuma) Trigger(Does Not Exist)
- MQ Monitor -Process controller(amqzmgr0) not active - Type(Process By Name) Process(amqzmgr0) Trigger(Does Not Exist)
- MQ Monitor - Processing controller (amqzxma0) not active - Type(Process By Name) Process(amqzxma0) Trigger(Does Not Exist)
- MQ Monitor - Publish subscribe process (amqfqpub) not active - Type (Process By Name) Process(amqfqpub) Trigger(Does Not Exist)
- MQ Monitor - PubSub restartable utility manager (amqzmuf0) not active - Type(Process By Name) Process(amqzmuf0) Trigger(Does Not Exist)
- MQ Monitor - Queue manager agent (amqzsla0) not active - Type(Process By Name) Process(amqzsla0) Trigger(Does Not Exist)
- MQ Monitor - Repository process (amqrrmfa) not active - Type(Process By Name) Process(amqrrmfa) Trigger(Does Not Exist)
- MQ Monitor - Restartable process manager (amqzmur0) not active - Type (Process By Name) Process(amqzmur0) Trigger(Does Not Exist)
- MQ Monitor -TCP/IP-invoked channel responder (amqcrsta) not active - Type(Process By Name) Process(amqcrsta) Trigger(Does Not Exist)
- MQ Monitor - The command server (amqpcesa) not active - Type(Process By Name) Process(amqpcesa) Trigger(Does Not Exist)
- MQ Monitor - Trigger monitor (runmqtrm) not active - Type(Process By Name) Process(runmqtrm) Trigger(Does Not Exist)

Creating Bespoke Templates

Open Central Configuration Manager and select the **Templates** tab from the left navigation panel.

Select the top level of the operating system (Windows, AIX or Linux) for which the template is being created.

Click **Add Template** on the Central Configuration Manager menu ribbon to display the **Add Template** dialog.

Templates require a name and description to be applied and it is good practice to choose labels that are meaningful and identify the tasks that the template undertakes. From the Template selection screen it is possible to select the monitors and rules that form the basis of the template.

> NOTE: It is only possible to open the rule dialog of the monitor from the **Templates** tab. The monitor settings option is only accessible from the **Systems** tab. This means that it is not possible to apply the 'Hold' monitor status (or other monitor settings) to a template. This must be done on an individual system basis after the template has been applied.

Monitor rules are created in templates in the same way as in 'standalone' monitors, (please refer to the section Working with Monitors for more information on monitors) with the following exceptions:

- **Event Log Monitors**: When adding criteria and using the Browse facility, you must first select an Example Device from which to select the specific event that you wish to monitor. If the template is applied to a system that does not run the event, the rule is ignored.
- **Performance Monitors**: When adding criteria, an Example Device must be selected prior to selection of the actual criteria. If selecting Generic Performance criteria directly from the Browse facility on the Example Device, it is the current settings on this device that is applied to the template.
- **System Monitors (Service)**: When adding criteria, first select an Example Device from which to select the specific service to be monitored. If the template is applied to a system that does not run the service, the rule is ignored.

When a template rule has been created, the associated monitor is shown in bold type as it does in the **Systems** dialog. The number of rules applied per monitor is also shown in both panes of the **Template** dialog.

Reporting

Network Server Suite includes a reporting function that captures performance data allowing you to generate summarized or detailed reports based on the performance of monitored systems in your enterprise. Reporting is activated at system level rather than across the entire enterprise so it is possible to select which systems to include.

Performance data can then be fed into Advanced Reporting Suite[1] from where performance reports can be designed, generated and distributed.

> **NOTE:** Advanced Reporting Suite is an additional product that requires a separate license from Network Server Suite in order to run.

Please refer to the Advanced Reporting Suite Installation Guide and Advanced Reporting Suite Report Designer User Reference manuals for more information on how to use performance data from Network Server Suite within Advanced Reporting Suite.

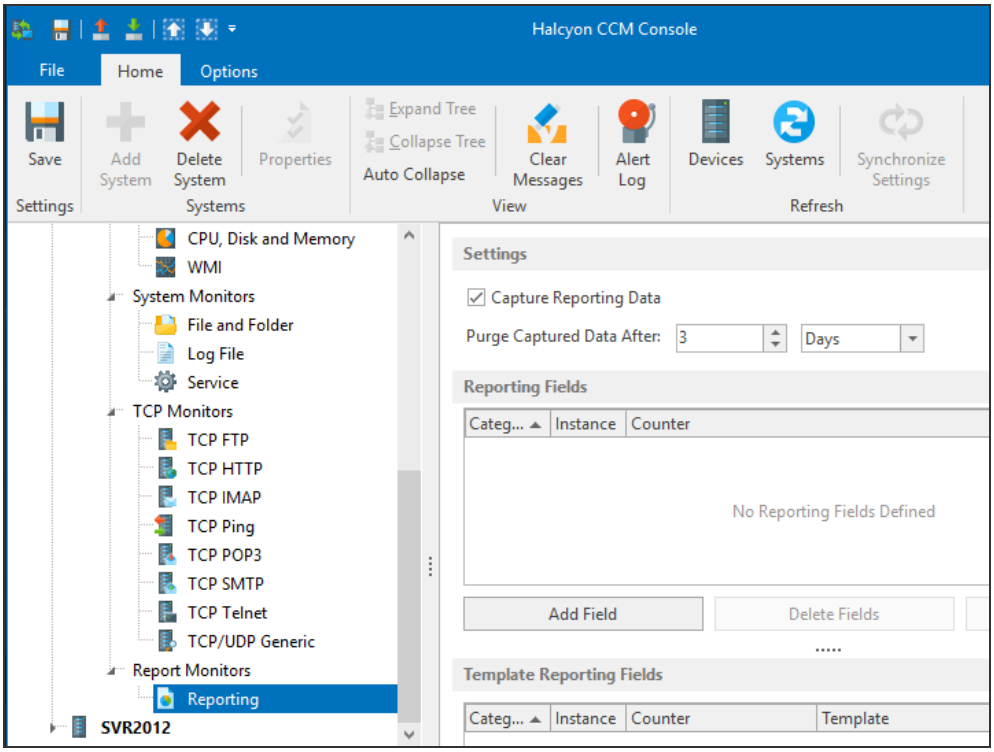
[1] Halcyon's custom performance and SLA reporting software for Windows, Linux, AIX, and IBM i

Applying the Reporting Monitor to a System

Providing Advanced Reporting Suite is installed and the selected system configured within, applying the Reporting Monitor to a system in Central Configuration Manager allows the collection of Performance Data.

To apply Performance Monitoring to a system

1. From within the Central Configuration Manager, in the left-hand navigation panel, expand the view of the system to which you want to apply the performance reporting.
2. Expand **Report Monitors** and select **Reporting**.
3. In the **Reporting Panel**, **Settings** section, click **Capture Reporting Data**.



NOTE: Even though the report monitor has been applied to the system, this system must still be added in the Web Interface of the Advanced Reporting Suite in order that the performance data is collected. Please refer to the Advanced Reporting Suite Installation Guide for more information on how to do this.

4. Click **Save** to apply the reporting settings to this system.

NOTE: Performance Reporting is automatically applied across all disks installed on the system. You do not need to specify each disk separately.

Purging Performance Data

To prevent historic performance data from taking up excessive storage space, define a period of time after which this data is deleted from the system. This means that after this time period, the data is unavailable for collection by the Halcyon Data Collector Service within the Advanced Reporting Suite. Data can be purged after a defined period of Hours or Days.

Setting the Purge Time Period

1. From within the Central Configuration Manager, in the left-hand navigation panel, expand the view of the system to which you want to apply the performance reporting.
2. Expand **Report Monitors** and select **Reporting**.
3. In the **Reporting Panel** in the **Settings** section, set the **Purge Captured Data After** option to the number of hours or days that you wish to retain the information.
4. Select whether the time period is in **Hours** or **Days**.
5. Click **Save** to apply the purge settings to this system.

Adding Reporting Fields

For Windows systems

The quickest way to add reporting fields to a Windows system is to apply the Advanced Reporting (Data Warehouse) Reporting template which contains five pre-defined, commonly-used performance reporting fields:

- **Processor**: % Processor Time
- **Win32_LogicalDisk**: FreeSpace
- **Win32_LogicalDisk**: Size
- **Win32_PageFileUsage**: AllocatedBaseSize
- **Win32_PageFileUsage**: CurrentUsage

> **NOTE:** See Reporting Templates for more information.

Reporting fields are used to determine what performance data should be collected from each system in order to form the basis of performance reporting for this device. The available fields are based upon the Windows Management Instrumentation (WMI) Monitor. An unlimited number of user-defined fields can be added for each system.

To Add a Reporting Field:

1. From the **Reporting Panel**, click **Add Field**. The **Select Example Device** dialog is displayed.
2. Select a device to use as the example device on which the Performance Monitoring data used for the basis of the report is based. The **WMI Reporting Data** dialog is displayed.

NOTE: See WMI (Windows Management Instrumentation) Monitor for more information relating to the options on this dialog.

For AIX and Linux systems

The quickest way to add reporting fields to a Windows system is to apply the AIX Advanced Reporting (Data Warehouse) template and Linux Advanced Reporting (Data Warehouse) template which contain five pre-defined, commonly-used performance reporting fields:

- **CPU**: CPU Load
- **Filesystem**: Filesystem Space Used %
- **Memory**: Page File Used %
- **Memory**: Physical Memory Used %
- **Process By Name**: CPU Usage %

Reporting fields are used to determine the performance data to be collected from each system in order to form the basis of performance reporting for this device. The available default fields are based upon the CPU, Filesystem and Memory Monitor. An unlimited number of user-defined fields can be added for each system and can also include Volume and Process Reporting options.

To Add a Reporting Field:

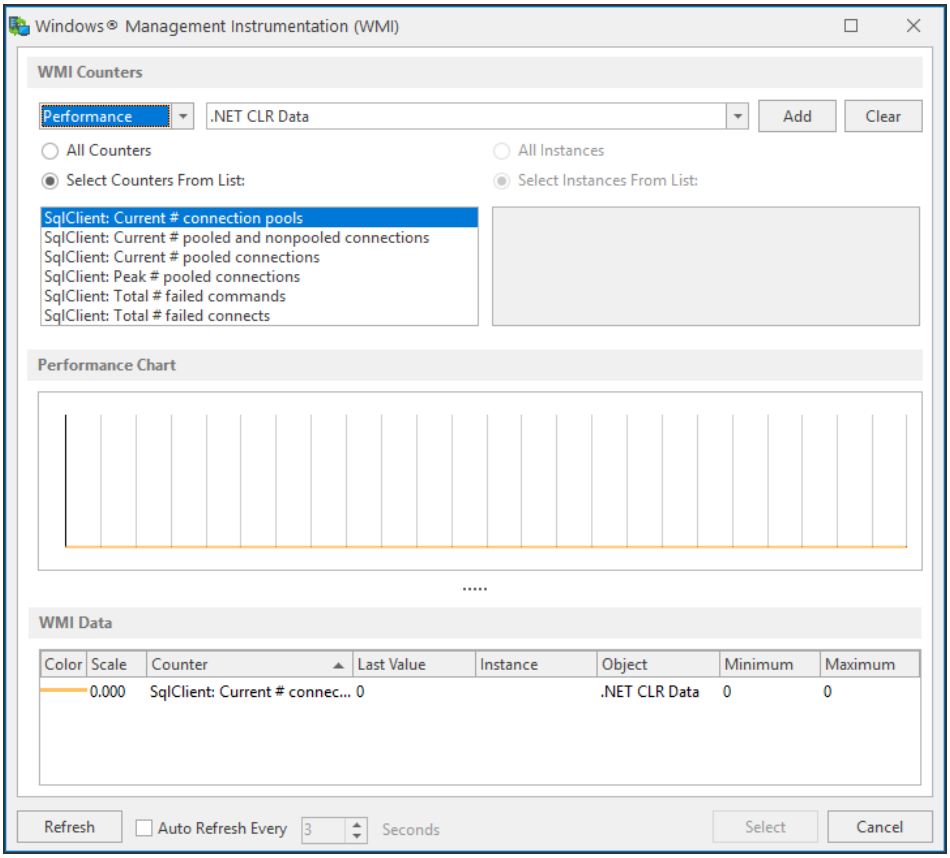
1. From the **Reporting Panel**, click **Add Field**. The **Select Category** dialog is displayed.
2. Select a Performance Category from any of the following options:
   - CPU
   - Filesystem
   - Memory
   - Volume Group
   - Physical Volume
   - Logical Volume
   - Process

   The **Select Example Device** dialog is displayed

3. Select a device to use as the example device on which the Performance Monitoring data used for the basis of the report is based.

Defining Windows Reporting Fields

The simplest way to define a specific Windows reporting field is to use the **Browse** option from the **WMI Reporting Option** dialog (accessed when adding a new reporting field) to scan the current system for the generic performance object on which data is collected.



Performance data is added using a series of drop-down menu options and choice buttons.

Category drop-down

Select whether you are going to check for the **Performance** or **Non-Performance** of the intended data object.

Object drop-down

Use the drop-down menu to select the WMI Object for which the performance data is to be reported. Use the vertical scroll-bar to see further options that are not initially displayed. Click on an object in the list to select it.

Counters/Instances

Depending on the chosen object you now have the ability to select individual counters and instances unique to the object type or select all (or a combination of one counter and all instances or all counters and one instance).

1. Click **Add** to begin generating Performance Data on the chosen counters/instances which are listed in the data field together with their corresponding graphical color representation.

   Auto-Refresh
   Data can be automatically refreshed every 3 seconds, by default, by clicking the **Auto-Refresh** option. The period of time between refreshing can be increased or decreased as required.
2. Once the choices have been made, highlight the entry in the WMI field data panel at the bottom of this dialog. The **Select** button is now enabled.
3. Click **Select** to re-open the WMI Reporting Data dialog. All fields on this dialog are auto-filled with the selected WMI performance data.
4. Click **OK** to add the WMI definition to the reporting fields in the selected field slot.
5. Continue to add further WMI Reporting data as required for this system.
6. When all the required performance data fields have been added, click  **Save** to apply the changes to this system.

The selected fields (providing that they do not contain a null data value) are now available for inclusion in a Performance Data report for this system that can be generated using the Advanced Reporting Suite Report Designer and Web Interface components.

SLA Statistic Reporting

Setting SLA Flags In Rule Criteria

Aside from using the Report Monitoring tool to check for performance data on a system, it is also possible to set Service Level Agreement (SLA) flags against most other system monitors when setting rule criteria. These SLA flags can then be reported against in the Advanced Reporting Suite using a pre-defined report template that is shipped with the product.

SLA flags can be set for rule criteria within the following Windows monitors:

- Web Application Monitor (if installed)
- CPU, Disk and Memory Monitor
- WMI Monitor
- Service Monitor
- TCP FTP Monitor
- TCP HTTP Monitor
- TCP NNTP Monitor
- TCP Ping Monitor
- TCP POP3 Monitor
- TCP SMTP Monitor
- TCP Telnet Monitor
- TCP/UDP Generic

NOTE: SLA reporting is not currently available for AIX or Linux systems.

To set a SLA Flag from within Rule criteria

Create the monitor rule as you would do normally (see Adding Rule Criteria for more information).

From the **Criteria** dialog for the required monitor, select the **Advanced** page.

1. Click the **SLA Statistic** field so that it is enabled. The SLA flag is measured against the specific criteria defined for this rule.

> **NOTE:** If setting multiple SLA flags for different criteria and/or monitors, we recommend that a Send Enterprise Console Alert action is used to determine which of the SLA criteria has failed.

2. Providing that all the other information required to create the rule has been entered, click **OK** to save this rule criteria as an SLA flag. Click **OK** again on the **Add Rule Detail** dialog to save this rule.
3. Click **Save**to apply the rule to this system.

> **NOTE:** SLA Statistic checking is not affected by the suspension of the rule, (SLA data is still gathered even if the rule is suspended) but is dependent on the time period when the rule is active (SLA data is not gathered outside the times when the rule is active).

> **NOTE:** We recommend that when creating SLA flags within rules, that all SLA criteria are kept together in the same rule that use the 'Perform Actions For Each Criteria That Triggers option, otherwise SLA failures may or may not be indicated correctly.

> **NOTE:** System performance against the specified SLA flags can then be viewed on the SLA Statistics report (automatically included as a Report Template within Advanced Reporting Suite) for this system.

Reporting Templates

Reporting templates allow you to apply the same reporting criteria across multiple systems in your enterprise. By using a reporting template you ensure that you are generating like-for-like reports across the same generic performance measurements of your systems. As with rule templates, a change made at rule level is reflected across all systems where that rule is implemented.

A basic reporting template, Advanced Reporting (Data Warehouse) covering Windows performance measurements is shipped with Network Server Suite as standard. An additional template, IIS (Data Warehouse) adds 3 further Web Service performance measurements for reporting purposes.

For AIX and Linux Systems, the **Advanced Reporting (Data Warehouse)** template is available.

Applying a Reporting Template

Reporting templates are created by adding a new template to the Templates tab of the Central Configuration Manager. It is good practice to give a reporting template an identification label that distinguishes it from any rule templates that may already exist.

> **NOTE:** See Defining Reporting Fields for more information on how to add Performance Data fields to the default or your own Report Templates.

Report templates are applied from the Systems tab of the Central Configuration Manager at Server Manager level. The reporting template is assigned from the Reporting Templates section. Note that all templates (Rules and Reporting appear in the drop-down choice menu so be careful when making your selection). The default Reporting template is called Advanced Reporting (Data Warehouse).

Repeat the process for each server manager on which the reporting template is to be installed. The Performance Data for the specified fields in the assigned Report Template can now be sent to a report from within Advanced Reporting Suite.

> **NOTE:** Server Manager Reporting is configured independently of Reporting Templates.

Advanced Reporting (Data Warehouse) Template (for Windows)

This Windows template includes the following File & Folder Monitor rule:

File & Folder Monitor

The File and Folder Monitor within the Advanced Reporting (Data Warehouse) template contains a single rule.

- **Monitor C:\ProgramFiles(x86)\Halcyon\Server Manager\Data\SMData.sdf in case >128MB - Path(C:\ProgramFiles(x86)\Halcyon\Server Manager\Data\) TriggerOn (First Matching Matching File) Thresholds(Size)**

This rule is a Halcyon self-checking entry to ensure that data for the Advanced Reporting template is being collected regularly. If the advreport.dat file is bigger than 128MB, an alert is raised warning that data may not be being collected as expected.

Windows Reporting fields

The Advanced Reporting (Data Warehouse) template contains the following reporting fields:

- **Processor (% Processor Time)**
- **Win32_PageFileUsage (Allocated Base Size)**
- **Win32_PageFileUsage (Current Usage)**
- **Win32_Volume (Capacity)**
- **Win32_Volume (Free Space)**

IIS (Data Warehouse) Template (for Windows)

This reporting template contains the following reporting fields based around the performance of Internet Information Services (IIS) (required for interaction between Network Server Suite and Advanced Reporting Suite):

Windows Web Service rules:

- **Web Service _Total Bytes Total/Sec**
- **Web Service _Total Current Connections**
- **Web Service _Total Get Requests/sec**

AIX Advanced Reporting (Data Warehouse) Template

This AIX template includes the following File & Folder Monitor rule:

File & Folder Monitor

The File and Folder Monitor within the AIX Advanced Reporting (Data Warehouse) template contains a single rule.

- **Monitor /var/lib/halcyon/advreport.dat in case >128MB - File(/var/lib/halcyon) Include(advreport.dat) Trigger(Exists)**

This rule is a Halcyon self-checking entry to ensure that data for the Advanced Reporting template is being collected regularly. If the advreport.dat file is bigger than 128MB, an alert is raised to warn you that data may not be being collected as expected.

AIX Reporting fields

This AIX reporting template contains the following reporting fields:

- **CPU: CPU Load**
- **FilesystemL Filesystem Space Used %**
- **Memory: Page File Used %**
- **Memory: Physical Memory Used %**
- **Process By Name: CPU Usage %**

Linux Advanced Reporting (Data Warehouse) Template

This Linux template includes the following File & Folder Monitor rule:

File & Folder Monitor

The File and Folder Monitor within the Linux Advanced Reporting (Data Warehouse) template contains a single rule.

- **Monitor /var/lib/halcyon/advreport.dat in case >128MB - File(/var/lib/halcyon) Include(advreport.dat) Trigger(Exists)**

This rule is a Halcyon self-checking entry to ensure that data for the Advanced Reporting template is being collected regularly. If the advreport.dat file is bigger than 128MB, an alert is raised to warn you that data may not be being collected as expected.

Linux Reporting fields

This Linux reporting template contains the following reporting fields:

- **CPU: CPU Load**
- **Filesystem: Filesystem Space Used %**

- Memory: Page File Used %
- Memory: Physical Memory Used %
- Process By Name: CPU Usage %

AIX Reporting

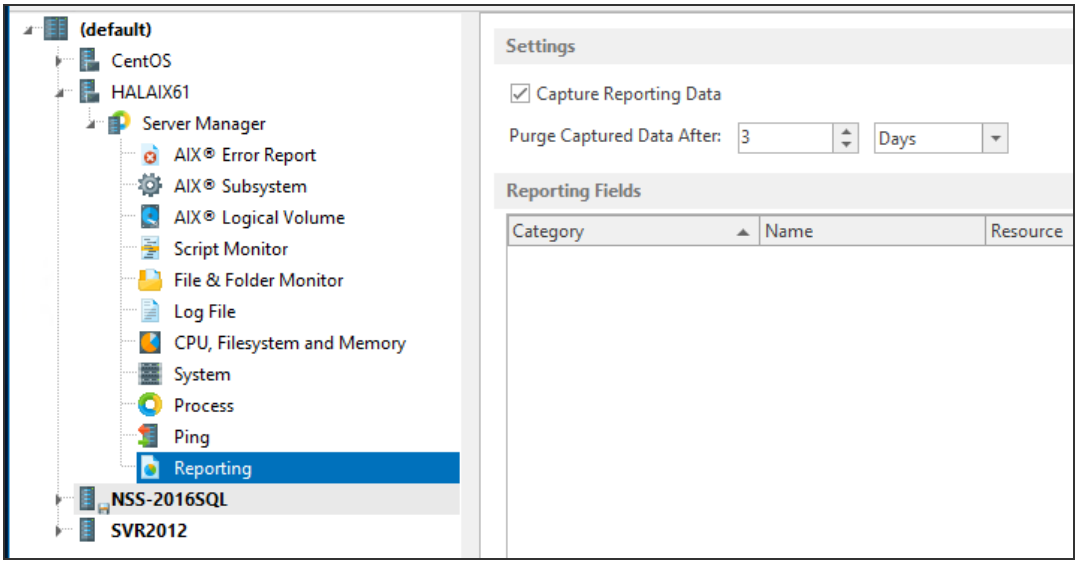
Specific field data from the following options are available for the purposes of AIX Reporting:

- CPU
- Filesystem
- Memory
- Volume Group
- Physical Volume
- Logical Volume
- Process

Getting Started

In order to begin gathering data on which to report, ensure that the **Capture Reporting Data** setting is enabled within the **Reporting Settings** panel.

1. From the left hand-navigation panel, select the **Systems** tab.
2. Expand the system view for the **AIX device**.
3. From the **AIX System** drop-down menu, select **Reporting**.



4. In the **Reporting** panel, **Settings** section click **Capture Reporting Data** to enable this setting.

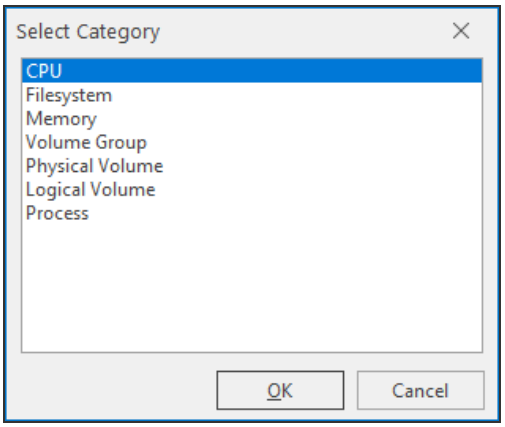
NOTE: By default, any captured data is purged after three days. See Purging Performance Data for more information on setting this parameter.

Once these settings have been specified, specific field data can be added to the AIX Reporting monitor.

Specifying The Reporting Fields

To start adding reporting fields to the AIX Reporting Monitor:

1. Click the **Add Field** button at the bottom of the **Reporting** panel.
   The **Select Category** dialog is displayed.

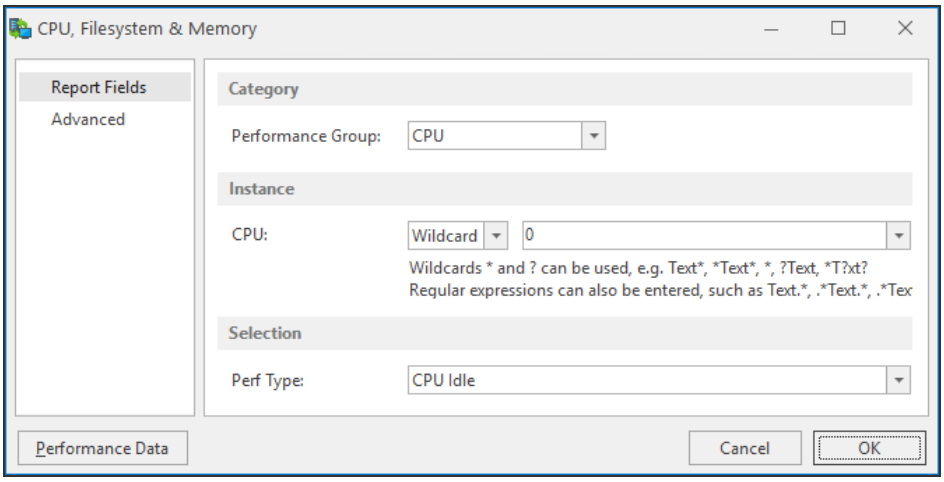


2. Click on an entry in this list followed by **OK** to be able to set specific reporting criteria for the selected category.

AIX CPU Reporting

AIX CPU Reporting provides reporting on the Idle or Load performance statistics of the CPU of the system on which the AIX Agent is installed.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **CPU**.
   This opens the **CPU, Filesystem and Memory** reporting dialog at the **CPU** Performance Group.



Category section

Performance Group

Leave this parameter set to the default setting of **CPU**.

Instance section

CPU Instance

For most CPU reporting purposes the **Wildcard** and **Regular Expressions (Regex)** options can be ignored for this parameter.

From the second drop-down choice menu, select the **CPU instance** on which reporting is required. Alternatively, select **Total** to report across the total of all CPU performance on this system.

Selection section

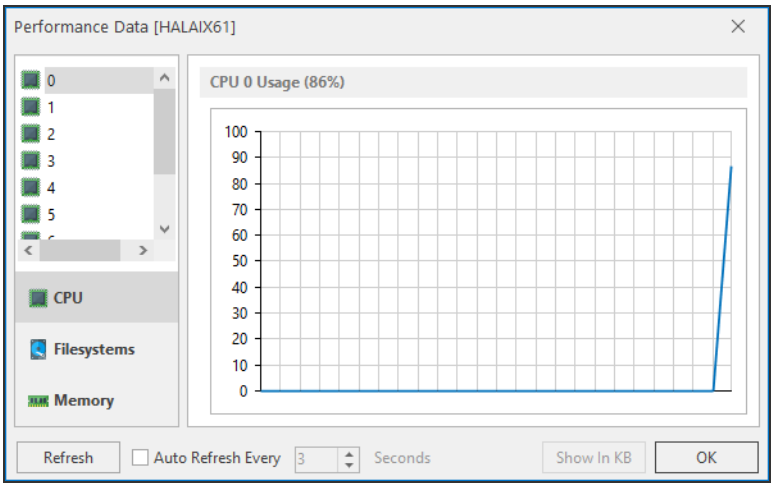
Performance Type

From the drop-down choice menu select one of the following options:

- **CPU Idle**: Reports the Idle levels for either the selected CPU instance or the Total CPU dependent on the selection within the Instance parameter. The higher the figure, the less work the CPU is doing.
- **CPU Load**: Reports the Load levels for either the selected CPU instance or the Total CPU dependent on the selection within the Instance parameter. The higher the figure, the more work the CPU is having to do

CPU Performance Data

Click **Performance Data** on this dialog to display the current CPU, Filesystem and Memory Performance Data for this system.



This dialog shows a view of the current performance data by individual CPU or as a Total.

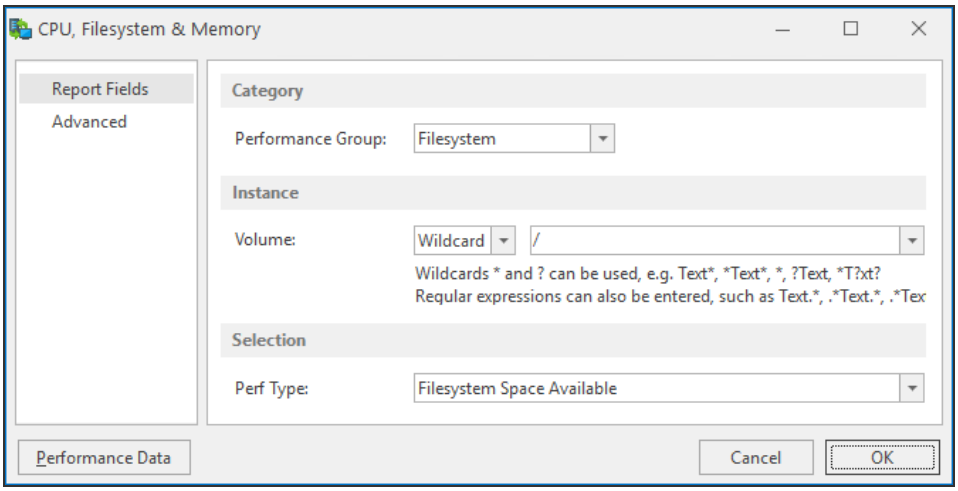
3. Click the **Refresh** button to refresh the data display or click **Auto-Refresh Every** and specify a time interval in seconds to automatically update the information.
4. Click **OK** to exit this display and return to the **CPU, Filesystem & Memory** dialog.

AIX Filesystem Reporting

AIX Filesystem Reporting provides reporting on a variety of Filesystem characteristics of the system on which the AIX Agent is installed.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Filesystem**.

   This opens the **CPU, Filesystem and Memory** reporting dialog at the **Filesystem** Performance Group.



Category section

Performance Group

Leave this parameter set to the default setting of **Filesystem**.

Instance section

Volume Instance

For most Filesystem reporting purposes the **Wildcard** and **Regular Expressions (Regex)** options can be ignored for this parameter.

From the second drop-down choice menu, select the **Volume** instance on which reporting is required.

Performance Type

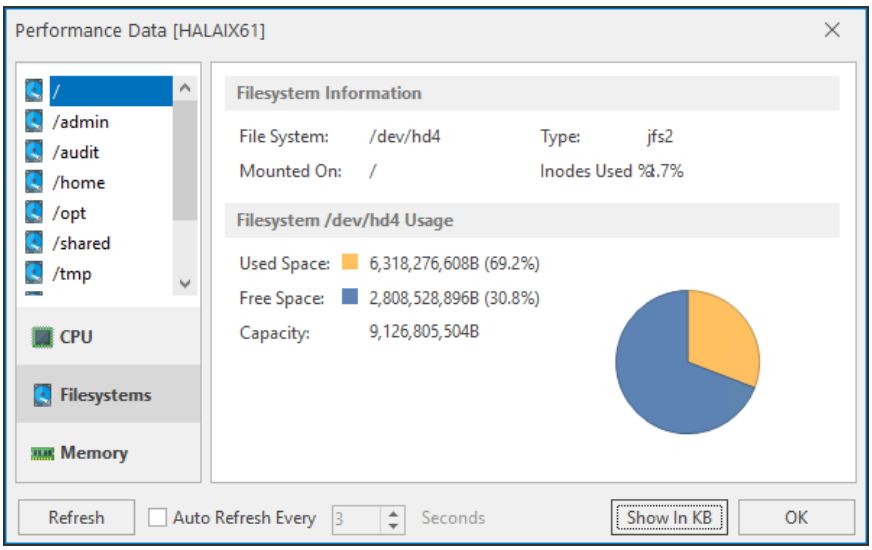
From the drop-down choice menu select one of the following options:

- **Filesystem Space Available**: Reports on the actual space available on the selected volume
- **Filesystem Space Available %**: Reports the space available on the selected volume as a percentage
- **Filesystem Space Total**: Reports on the total space available on the selected volume
- **Filesystem Space Used**: Reports on the actual amount of space used on the selected volume
- **Filesystem Space Used %**: Reports on the amount of space used on the selected volume as a percentage

- **Inodes Available**: Reports on the number of inodes available on the selected volume
- **Inodes Available %**: Reports on the inodes available on the selected volume
- **Inodes Total**: Reports on the total number of inodes on the selected volume
- **Inodes Used**: Reports on the number of inodes used on the selected volume
- **Inodes Used %**: Reports on the number of inodes used on the selected volume as a percentage

Filesystem Performance Data

Click **Performance Data** on this dialog to display the current CPU, Filesystem and Memory Performance Data for this system.



This dialog allows you to view the current Filesystem information by volume.

3. Click the **Refresh** button to refresh the data display or click **Auto-Refresh Every** and specify a time interval in seconds to automatically update the information.
4. Click the **Show In...** button to change the display measurements of the selected Filesystem. The available size options are:

- **B**
- **KB**
- **MB**
- **GB**

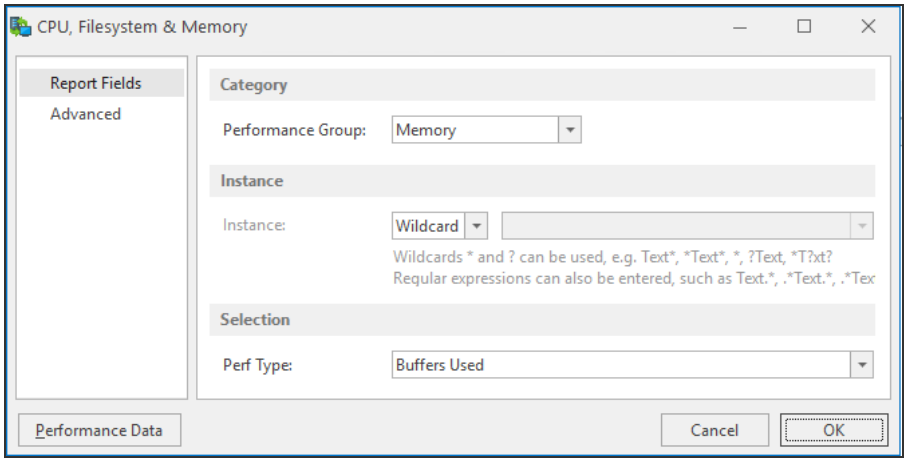
5. Click **OK** to exit this display and return to the CPU, Filesystem & Memory Reporting Selection dialog.

AIX Memory Reporting

AIX Memory Reporting provides reporting on a variety of memory characteristics of the system on which the AIX Agent is installed.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Memory.**

This opens the **CPU, Filesystem and Memory** reporting dialog at the **Memory Performance** Group.



Category section

Performance Group

Leave this parameter set to the default setting of **Memory**.

Instance section

Instance

For the purpose of Memory Reporting, the Instance parameter is unavailable.

Selection section

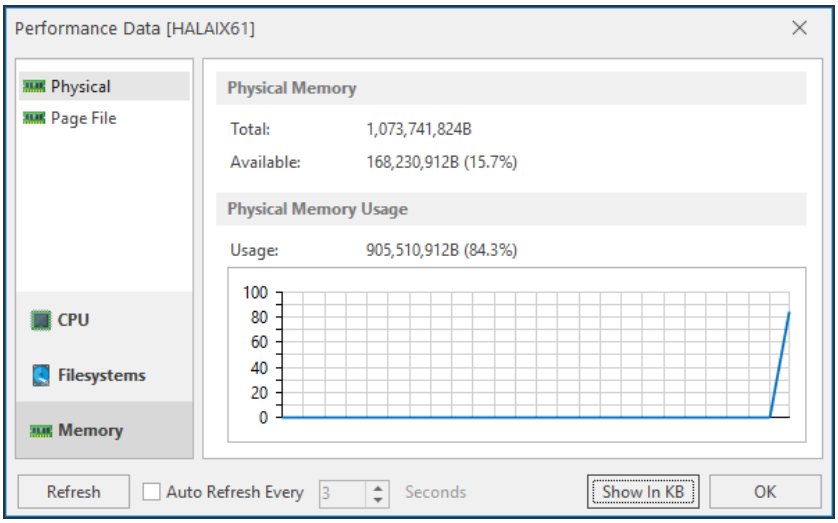
Performance Type

From the drop-down choice menu select one of the following options:

- **Buffers Used**: Reports on the number of buffers used on this system
- **Memory Load**: Reports on the loading of the available memory on this system
- **Page File Available**: Reports on the amount of Page File memory available on this system
- **Page File Available %**: Reports on the amount of Page File memory available on this system as a percentage value
- **Page File Total**: Reports on the total Page File memory available on this system
- **Page File Used**: Reports on the amount of Page File Memory used on this system
- **Page File Used %**: Reports on the amount of Page File Memory used on this system as a percentage value
- **Physical Memory Available**: Reports on the actual amount of Physical Memory available on this system
- **Physical Memory Available %**: Reports on the actual amount of Physical Memory available on this system as a percentage value
- **Physical Memory Total**: Reports on the total amount of Physical Memory available on this system
- **Physical Memory Used**: Reports on the amount of Physical Memory used on this system
- **Physical Memory Used %**: Reports on the amount of Physical Memory used on this system as a percentage value
- **Virtual Memory Total**: Reports on the total amount of Virtual Memory available on this system
- **Virtual Memory Available**: Reports on the actual amount of Virtual Memory available on this system
- **Virtual Memory Used**: Reports on the amount of Virtual Memory used on this system

Memory Performance Data

Click **Performance Data** on this dialog to display the current CPU, Filesystem and Memory Performance Data for this system.



This dialog allows you to view the current memory information by physical or page file attributes.

3. Click **Refresh** to refresh the data display or click **Auto-Refresh Every** and specify a time interval in seconds to automatically update the information.
4. Click **Show In...** to change the display measurements of the selected memory attribute. The available size options are:

- **B**
- **KB**
- **MB**
- **GB**

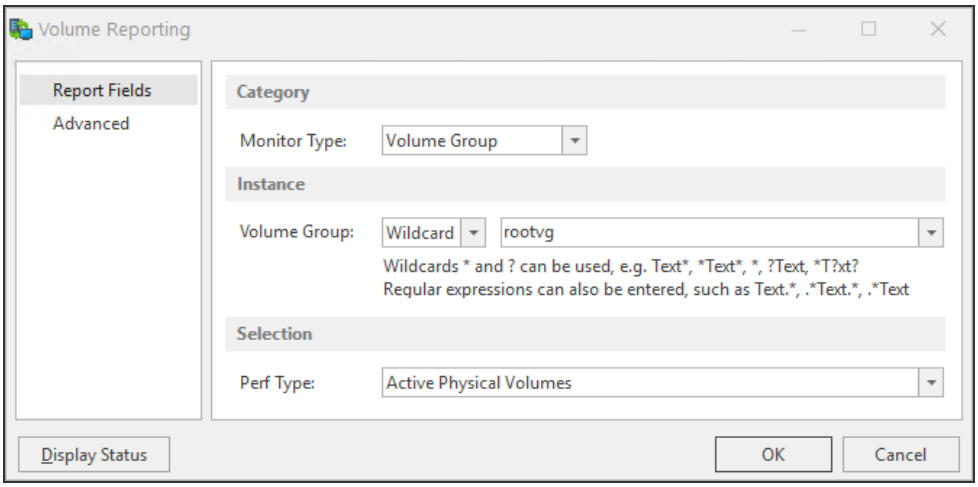
5. Click **OK** to exit this display and return to the CPU, Filesystem & Memory Reporting Selection dialog.

AIX Volume Group Reporting

AIX Volume Group Reporting provides reporting on the Volume Groups of an AIX system.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Volume Group**.

This opens the **Volume Reporting** reporting dialog at the **Volume Group** Monitor Type.



Category section

Monitor Type

Leave this parameter set to the default setting of **Volume Group**.

Instance section

Volume Group

Either select the name of the **Volume Group** from the drop-down choice menu or use **Wildcards** or **Regular Expressions (Regex)** to define the name of the Volume Group on which reporting is required.

Selection section

Performance Type

From the drop-down choice menu select one of the following options:

- **Actual Physical Volumes**: Reports on the number of actual physical volumes within the selected volume group
- **Allocated Physical Extents**: Reports on the number of allocated physical extents within the selected volume group
- **Allocated Size**: Reports on the disk space allocated to accommodate the selected volume group
- **Current Logical Volumes**: Reports on the number of current logical volumes within the selected volume group

- **Current Physical Volumes**: Reports on the number of current physical volumes within the selected volume group
- **Free Physical Extents**: Reports on the number of free physical extents within the selected volume group
- **Free Size**: Reports on the free space left within the selected volume group
- **Maximum Logical Volumes**: Reports on the maximum number of logical volumes available within the selected volume group
- **Maximum Physical Volumes**: Reports on the maximum number of physical volumes available within the selected volume group
- **Meta Sequence Number**: Reports on the Meta Sequence Number of the selected volume group
- **Metadata Areas**: Reports on the number of Metadata Areas within the selected volume group
- **Open Logical Volumes**: Reports on the number of Open Logical Volumes within this selected volume group
- **Physical Extent Size**: Reports on the size of the Physical Extent within the selected volume group
- **Total Physical Extents**: Reports on the total number of Physical Extents within the selected volume groups
- **Volume Group Size**: Reports on the total size of the selected volume group

Volume Group Display Status

3. Click **Display Status** on the **Volume Reporting** dialog to display the current **Volume Group Information** for this system.
4. Click the **Show In...** button to amend the view by which the partition size measurements are displayed. The possible display options are:

- **B**: Byte
- **KB**: Kilobyte
- **MB**: Megabyte
- **GB**: Gigabyte
- **TB**: Terabyte
- **PB**: Petabyte
- **EB**: Exabyte

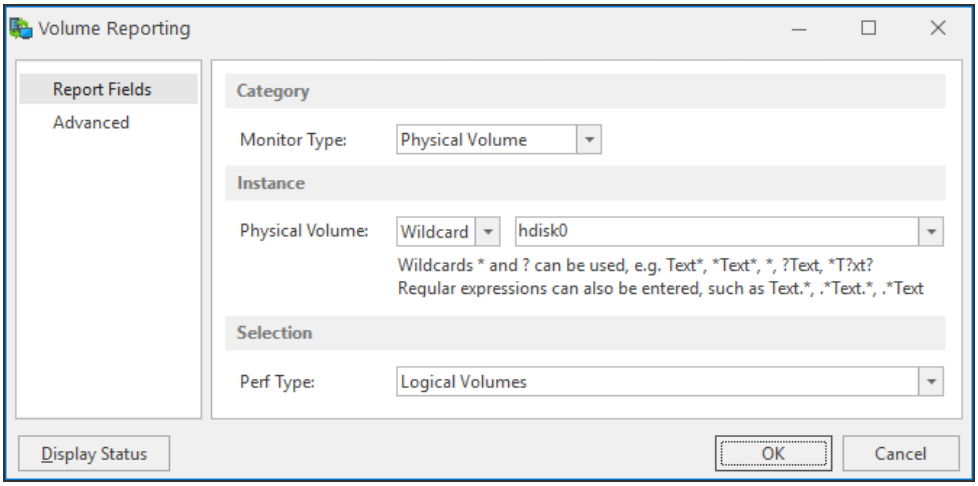
5. Click **OK** to exit this display and return to the **Volume Group Reporting** dialog.

AIX Physical Volume Reporting

AIX Physical Volume Reporting provides reporting on the Physical Volumes of an AIX system.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Physical Volume**.

This opens the **Volume Reporting** reporting dialog at the **Physical Volume** Monitor Type.



Category section

Monitor Type

Leave this parameter set to the default setting of **Physical Volume**.

Instance section

Physical Volume

Either select the name of the **Physical Volume** from the drop-down choice menu or use **Wildcards** or **Regular Expressions** (Regex) to define the name of the Physical Volume on which reporting is required.

Selection section

Performance Type

From the drop-down choice menu select one of the following options:

- **Allocated Physical Extents**: Reports on the number of Allocated Physical Extents within the selected physical volume

- **Free Physical Extents**: Reports on the number of free Physical Extents within the selected physical volume
- **Physical Extent Size**: Reports on the size of the Physical Extent within the selected physical volume
- **Physical Volume Size**: Reports on the size of the selected physical volume
- **Total Physical Extents**: Reports on the total number of Physical Extents on the selected physical volume

Physical Volume Display Status

3. Click **Display Status** on the **Volume Reporting** dialog to display the current **Physical Volume Information** for this system.
4. Click **Show In...** to amend the view by which the physical partition size measurements are displayed. The possible display options are:

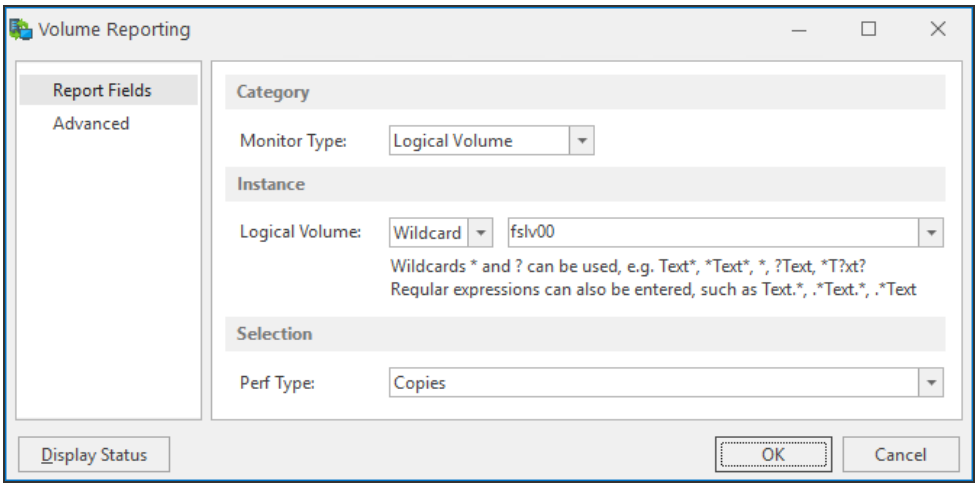
- **B**: Byte
- **KB**: Kilobyte
- **MB**: Megabyte
- **GB**: Gigabyte
- **TB**: Terabyte
- **PB**: Petabyte
- **EB**: Exabyte

5. Click **OK** to exit this display and return to the **Volume Group Reporting** dialog.

AIX Logical Volume Reporting

AIX Logical Volume Reporting provides reporting on the Logical Volumes of an AIX system.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Logical Volume**.
   This opens the **Volume Reporting** reporting dialog at the **Physical Volume** Monitor Type.



Category section

Monitor Type

Leave this parameter set to the default setting of **Logical Volume**.

Instance section

Logical Volume

Either select the name of the **Logical Volume** from the drop-down choice menu or use **Wildcards** or **Regular Expressions** (Regex) to define the name of the **Logical Volume** on which reporting is required.

Selection section

Performance Type

From the drop-down choice menu select one of the following options:

- **Current Logical Extent**: Reports on the number of Current Logical Extents within the selected logical volume
- **Segments**: Reports on the number of segments within the selected logical volume
- **Size**: Reports on the size of the selected logical value

Logical Volume Display Status

3. Click **Display Status** on the **Volume Reporting** dialog to display the current **Logical Volume Information** for this system.
4. Click **Show In...** to amend the view by which the physical partition size measurements are displayed. The possible display options are:

- **B**: Byte
- **KB**: Kilobyte
- **MB**: Megabyte
- **GB**: Gigabyte
- **TB**: Terabyte
- **PB**: Petabyte
- **EB**: Exabyte

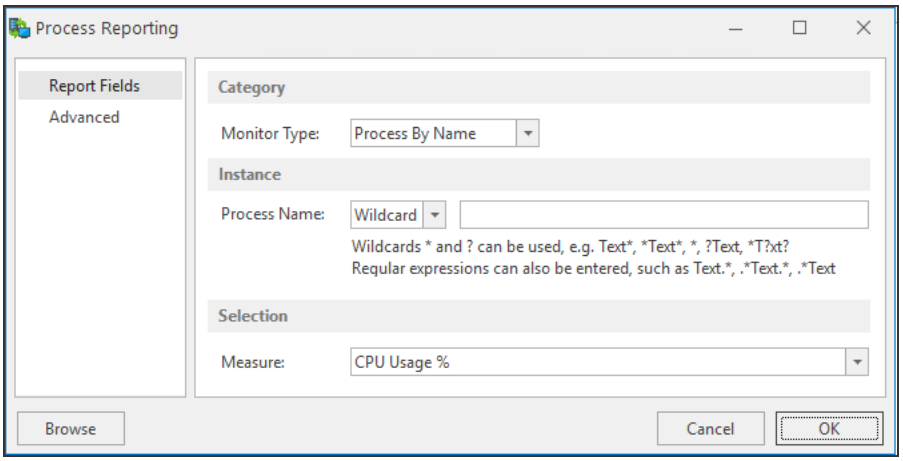
5. Click **OK** to exit this display and return to the **Volume Group Reporting** dialog.

AIX Process Reporting

Provides reporting on the processes running on an AIX system.

1. From the required **AIX System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **CPU**.

This opens the **CPU, Filesystem and Memory** reporting dialog at the **CPU** Performance Group.



Category section

Monitor Type

There are three possible options when selecting the Process Monitor Type:

- Process By Name
- Process By Owner
- Process By PID

Instance section

Process Name

Either type the name of the **AIX process** on which reporting is required or use **Wildcards** or **Regular Expressions** (Regex) to define the name of the process.

> **NOTE:** Wildcards and Regular Expressions cannot be used when the Monitor Type is Process by PID

Selection section

Measure

From the drop-down choice menu select one of the following options:

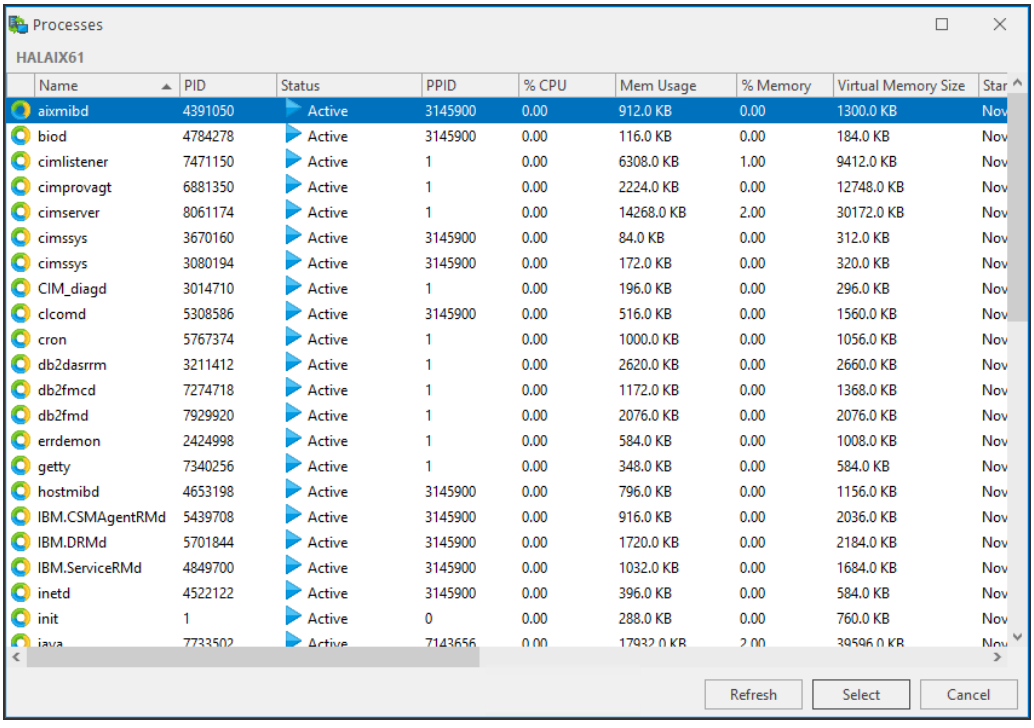
- **CPU Usage %**: Reports on the amount of CPU (expressed as a percentage value)
- **Cumulative CPU Time**: Reports on the cumulative CPU Time used by the selected process
- **Elapsed Time**: Reports on the time elapsed since the selected process was started

- **Number of Processes**: Reports on the number of processes running under the selected name
- **Process Physical Memory Used**: Reports on the amount of physical memory used by the selected process
- **Process Physical Memory Used %**: Reports on the amount of physical memory used by the selected process expressed as a percentage value
- **Virtual Memory Size**: Reports on the amount of virtual memory used by the named process

Process Browse

It is also possible to select any additional processes that may be running on this system for inclusion in AIX Reporting.

3. From the **Process Reporting** dialog, click **Browse** to open the list of Processes for this system.



4. Use the vertical scroll bar to move through the list of available processes.
5. Click on a process so that it is highlighted and click **Select** to automatically add the process so that it appears in the **Process Name** parameter of the **Process Reporting** dialog.

AIX Reporting Advanced Settings

Advanced Settings, available from the left navigation panel when setting reporting criteria, can be used to specify instances that can be ignored, to avoid triggering an unnecessary alert.

To specify instances that can be ignored:

1. Having set the required reporting criteria, select the **Advanced** tab.

> NOTE: If the **Ignore the following instances** box is unavailable, the option cannot be used for the selected criteria.

2. Click **Add** to open the **Add Instance Name** dialog.
3. Enter the name of the **Instance** that you wish to be ignored if encountered. Click **OK**.
4. Continue to add instances or click **OK** to save the changes and close the **Criteria** dialog.

Linux Reporting

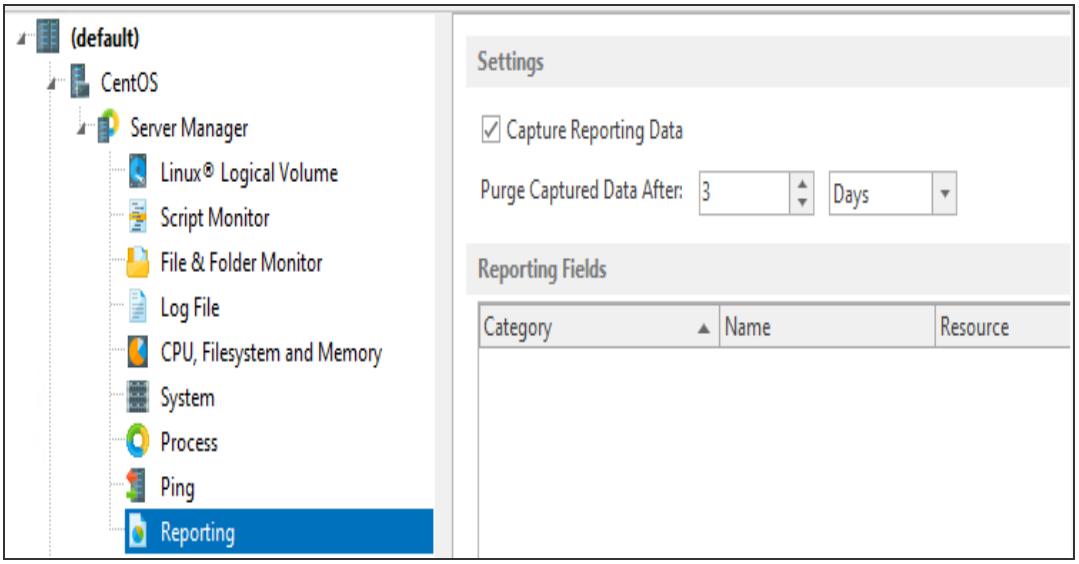
Specific field data from the following options are available for the purposes of Linux Reporting:

- CPU
- Filesystem
- Memory
- Volume Group
- Physical Volume
- Logical Volume
- Process

Getting Started

In order to begin gathering data on which to report, ensure that the **Capture Reporting Data** setting is enabled within the **Reporting Settings** panel.

1. From the left hand-navigation panel, select the **Systems** tab.
2. Expand the system view for the **Linux device**.
3. From the **Linux System** drop-down menu, select **Reporting**.



4. In the **Reporting** panel, **Settings** section click **Capture Reporting Data** to enable this setting.

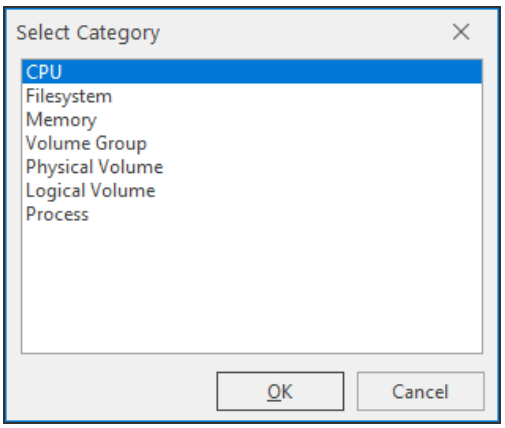
> **NOTE:** By default, any captured data is purged after three days. See Purging Performance Data for more information on setting this parameter.

Once these settings have been specified, specific field data can be added to the Linux Reporting monitor.

Specifying The Reporting Fields

To start adding reporting fields to the Linux Reporting Monitor:

1. Click **Add Field** at the bottom of the **Reporting** panel.
   The **Select Category** dialog is displayed.

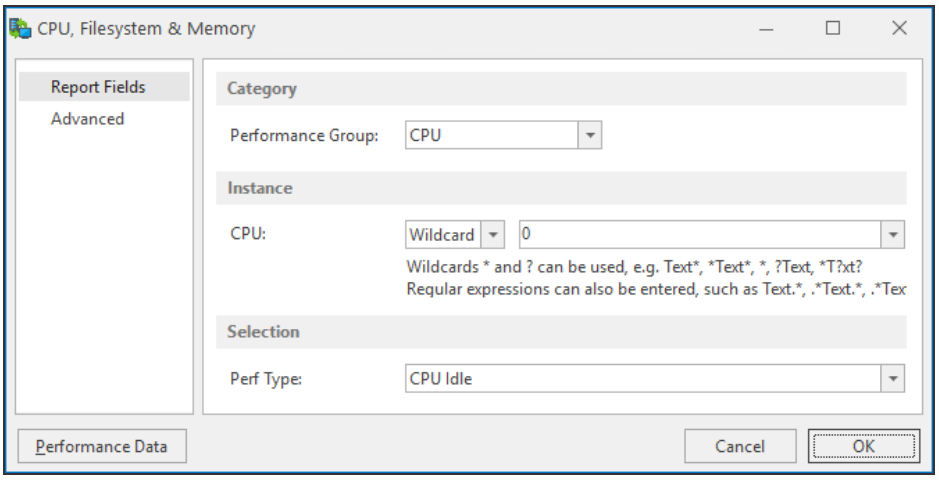


2. Click on an entry in this list followed by **OK** to be able to set specific reporting criteria for the selected category.

Linux CPU Reporting

Linux CPU Reporting provides reporting on the Idle or Load performance statistics of the CPU of the system on which the Linux Agent is installed.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **CPU**.
   This opens the **CPU, Filesystem and Memory** reporting dialog at the **CPU** Performance Group.



Category section

Performance Group

Leave this parameter set to the default setting of **CPU**.

Instance section

CPU Instance

For most CPU reporting purposes the **Wildcard** and **Regular Expressions (Regex)** options can be ignored for this parameter.

From the second drop-down choice menu, select the **CPU instance** on which reporting is required. Alternatively, select **Total** to report across the total of all CPU performance on this system.

Selection section

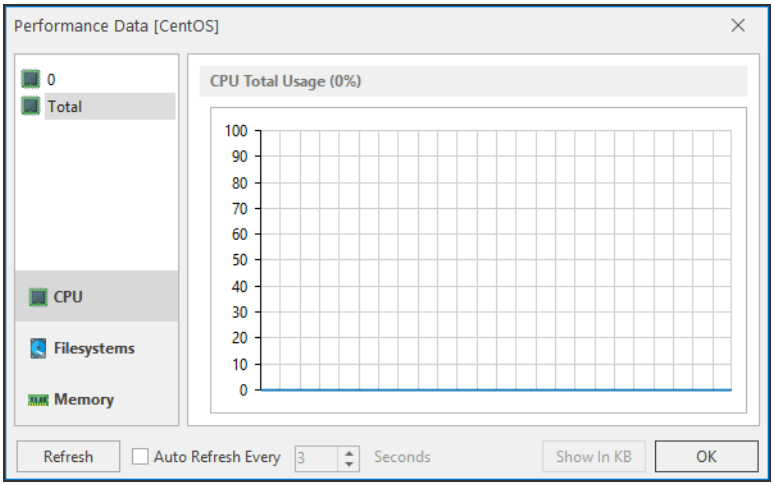
Performance Type

From the drop-down choice menu select one of the following options:

- **CPU Idle**: Reports the Idle levels for either the selected CPU instance or the Total CPU dependent on the selection within the Instance parameter. The higher the figure, the less work the CPU is doing.
- **CPU Load**: Reports the Load levels for either the selected CPU instance or the Total CPU dependent on the selection within the Instance parameter. The higher the figure, the more work the CPU is having to do

CPU Performance Data

Click **Performance Data** on this dialog to display the current CPU, Filesystem and Memory Performance Data for this system.



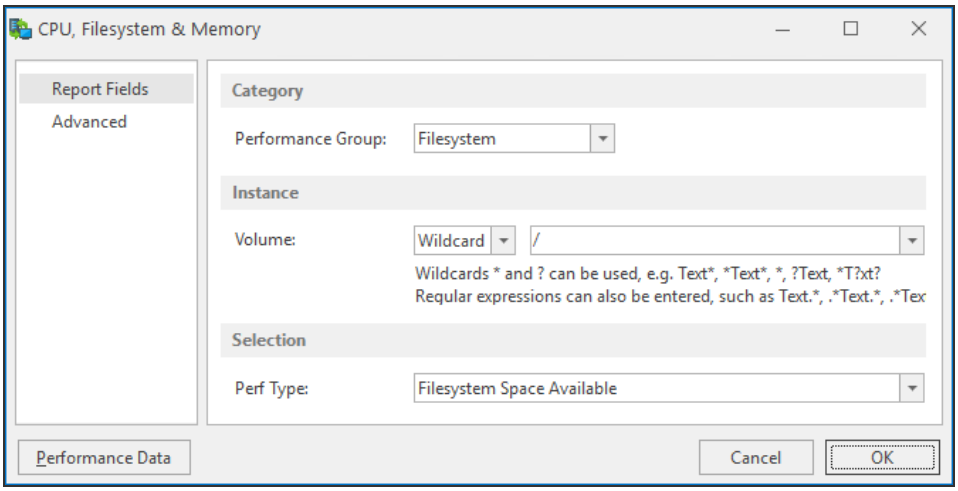
This dialog shows a view of the current performance data by individual CPU or as a Total.

3. Click **Refresh** to refresh the data display or click **Auto-Refresh Every** and specify a time interval in seconds to automatically update the information.
4. Click **OK** to exit this display and return to the **CPU, Filesystem & Memory** dialog.

Linux Filesystem Reporting

Linux Filesystem Reporting provides reporting on a variety of Filesystem characteristics of the system on which the Linux Agent is installed.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Filesystem**.
   This opens the **CPU, Filesystem and Memory** reporting dialog at the **Filesystem** Performance Group.



Category section

Performance Group

Leave this parameter set to the default setting of **Filesystem**.

Instance section

Volume Instance

For most Filesystem reporting purposes the **Wildcard** and **Regular Expressions (Regex)** options can be ignored for this parameter.

From the second drop-down choice menu, select the **Volume** instance on which reporting is required.

Performance Type

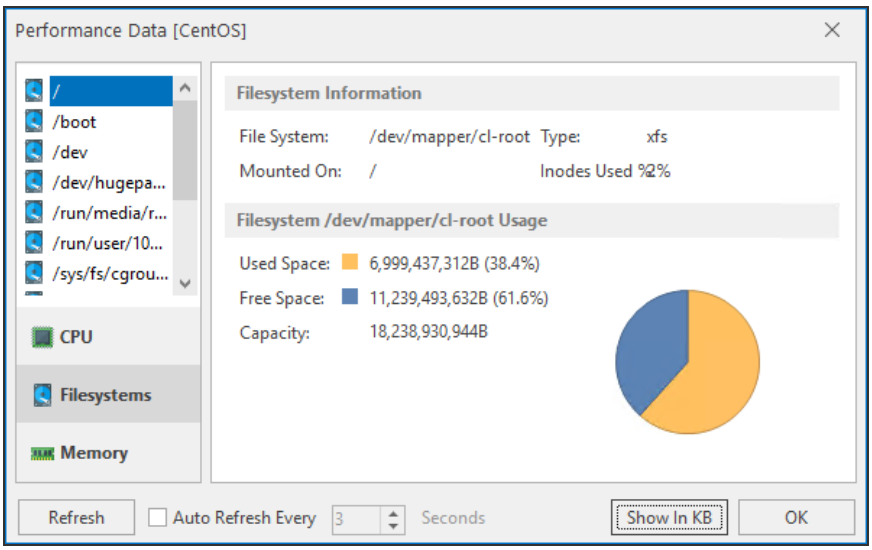
From the drop-down choice menu select one of the following options:

- **Filesystem Space Available**: Reports on the actual space available on the selected volume
- **Filesystem Space Available %**: Reports the space available on the selected volume as a percentage
- **Filesystem Space Total**: Reports on the total space available on the selected volume
- **Filesystem Space Used**: Reports on the actual amount of space used on the selected volume
- **Filesystem Space Used %**: Reports on the amount of space used on the selected volume as a percentage

- **Inodes Available**: Reports on the number of inodes available on the selected volume
- **Inodes Available %**: Reports on the inodes available on the selected volume
- **Inodes Total**: Reports on the total number of inodes on the selected volume
- **Inodes Used**: Reports on the number of inodes used on the selected volume
- **Inodes Used %**: Reports on the number of inodes used on the selected volume as a percentage

Filesystem Performance Data

Click **Performance Data** on this dialog to display the current CPU, Filesystem and Memory Performance Data for this system.



This dialog allows you to view the current Filesystem information by volume.

3. Click **Refresh** to refresh the data display or click **Auto-Refresh Every** and specify a time interval in seconds to automatically update the information.
4. Click **Show In...** to change the display measurements of the selected Filesystem. The available size options are:

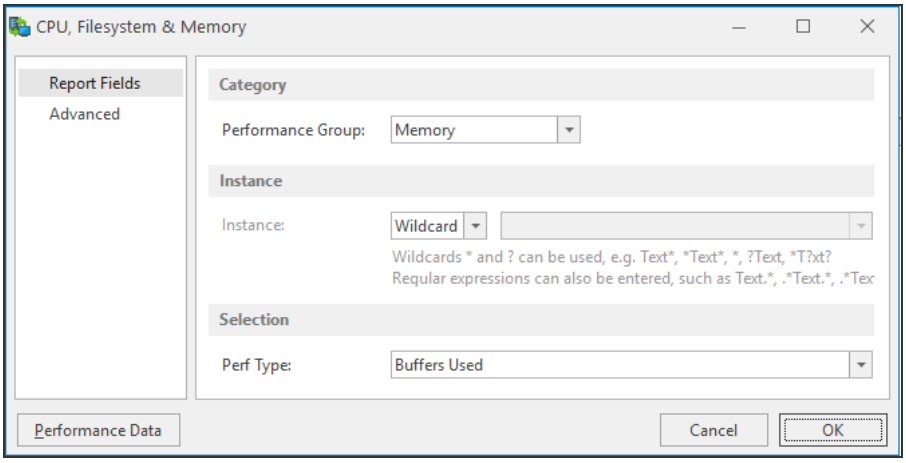
   B
   KB
   MB
   GB
5. Click **OK** to exit this display and return to the CPU, Filesystem & Memory dialog.

Linux Memory Reporting

Linux Memory Reporting provides reporting on a variety of memory characteristics of the system on which the Linux Agent is installed.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Memory.**

   This opens the **CPU, Filesystem and Memory** reporting dialog at the **Memory Performance** Group.



Category section

Performance Group

Leave this parameter set to the default setting of **Memory**.

Instance section

Instance

For the purpose of Memory Reporting, the Instance parameter is unavailable.

Selection section

Performance Type

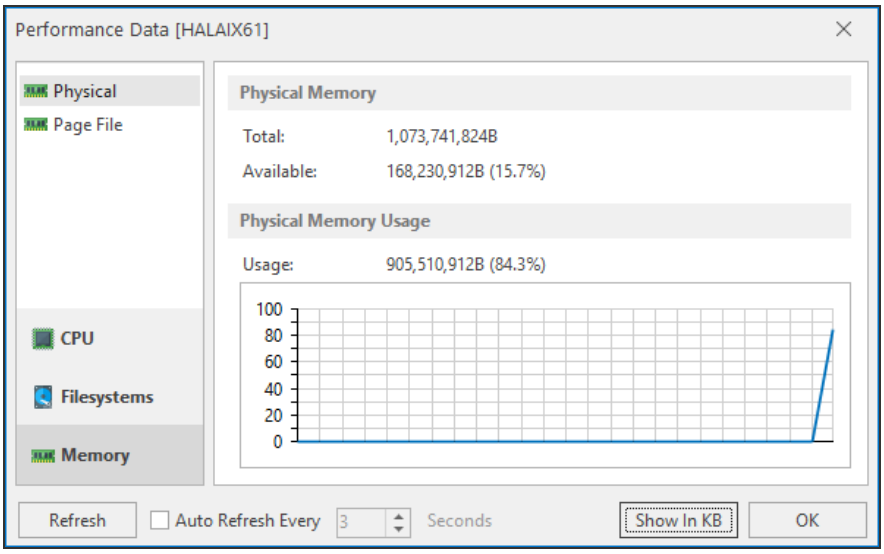
From the drop-down choice menu select one of the following options:

- **Buffers Used**: Reports on the number of buffers used on this system
- **Memory Load**: Reports on the loading of the available memory on this system

- **Page File Available**: Reports on the amount of Page File memory available on this system
- **Page File Available %**: Reports on the amount of Page File memory available on this system as a percentage value
- **Page File Total**: Reports on the total Page File memory available on this system
- **Page File Used**: Reports on the amount of Page File Memory used on this system
- **Page File Used %**: Reports on the amount of Page File Memory used on this system as a percentage value
- **Physical Memory Available**: Reports on the actual amount of Physical Memory available on this system
- **Physical Memory Available %**: Reports on the actual amount of Physical Memory available on this system as a percentage value
- **Physical Memory Total**: Reports on the total amount of Physical Memory available on this system
- **Physical Memory Used**: Reports on the amount of Physical Memory used on this system
- **Physical Memory Used %**: Reports on the amount of Physical Memory used on this system as a percentage value
- **Virtual Memory Total**: Reports on the total amount of Virtual Memory available on this system
- **Virtual Memory Available**: Reports on the actual amount of Virtual Memory available on this system
- **Virtual Memory Used**: Reports on the amount of Virtual Memory used on this system

Memory Performance Data

Click **Performance Data** on this dialog to display the current CPU, Filesystem and Memory Performance Data for this system.



This dialog allows you to view the current memory information by physical or page file attributes.

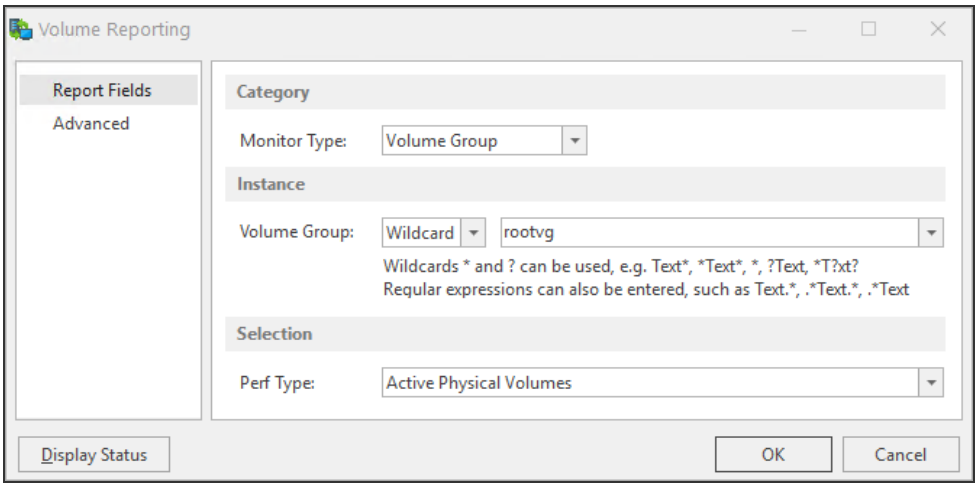
3. Click the **Refresh** button to refresh the data display or click **Auto-Refresh Every** and specify a time interval in seconds to automatically update the information.
4. Click the **Show In...** button to change the display measurements of the selected memory attribute. The available size options are:
   - B
   - KB
   - MB
   - GB
5. Click **OK** to exit this display and return to the **CPU, Filesystem & Memory** dialog.

Linux Volume Group Reporting

Linux Volume Group Reporting provides reporting on the Volume Groups of a Linux system.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Volume Group**.

This opens the **Volume Reporting** reporting dialog at the **Volume Group** Monitor Type.



Category section

Monitor Type

Leave this parameter set to the default setting of **Volume Group**.

Instance section

Volume Group

Either select the name of the **Volume Group** from the drop-down choice menu or use **Wildcards** or **Regular Expressions (Regex)** to define the name of the Volume Group on which reporting is required.

Selection section

Performance Type

From the drop-down choice menu select one of the following options:

- **Actual Physical Volumes**: Reports on the number of actual physical volumes within the selected volume group
- **Allocated Physical Extents**: Reports on the number of allocated physical extents within the selected volume group
- **Allocated Size**: Reports on the disk space allocated to accommodate the selected volume group
- **Current Logical Volumes**: Reports on the number of current logical volumes within the selected volume group

- **Current Physical Volumes**: Reports on the number of current physical volumes within the selected volume group
- **Free Physical Extents**: Reports on the number of free physical extents within the selected volume group
- **Free Size**: Reports on the free space left within the selected volume group
- **Maximum Logical Volumes**: Reports on the maximum number of logical volumes available within the selected volume group
- **Maximum Physical Volumes**: Reports on the maximum number of physical volumes available within the selected volume group
- **Meta Sequence Number**: Reports on the Meta Sequence Number of the selected volume group
- **Metadata Areas**: Reports on the number of Metadata Areas within the selected volume group
- **Open Logical Volumes**: Reports on the number of Open Logical Volumes within this selected volume group
- **Physical Extent Size**: Reports on the size of the Physical Extent within the selected volume group
- **Total Physical Extents**: Reports on the total number of Physical Extents within the selected volume groups
- **Volume Group Size**: Reports on the total size of the selected volume group

Volume Group Display Status

Click **Display Status** on the **Volume Reporting** dialog to display the current **Volume Group Information** for this system.

Click the **Show In...** button to amend the view by which the partition size measurements are displayed. The possible display options are:

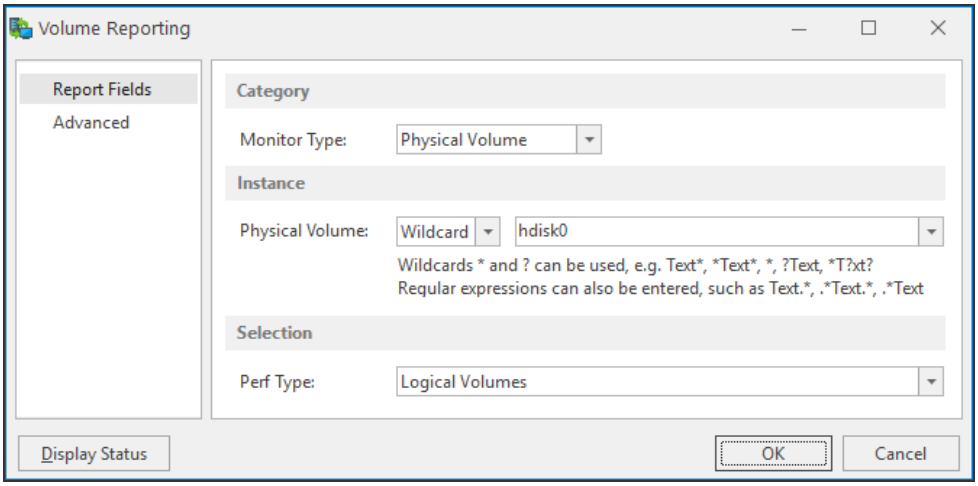
- **B**: Byte
- **KB**: Kilobyte
- **MB**: Megabyte
- **GB**: Gigabyte
- **TB**: Terabyte
- **PB**: Petabyte
- **EB**: Exabyte

3. Click **OK** to exit this display and return to the **Volume Group Reporting** dialog.

Linux Physical Volume Reporting

Linux Physical Volume Reporting provides reporting on the Physical Volumes of a Linux system.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Physical Volume**.
   This opens the **Volume Reporting** reporting dialog at the **Physical Volume** Monitor Type.



Category section

Monitor Type

Leave this parameter set to the default setting of **Physical Volume**.

Instance section

Physical Volume

Either select the name of the **Physical Volume** from the drop-down choice menu or use **Wildcards** or **Regular Expressions** (Regex) to define the name of the Physical Volume on which reporting is required.

Selection section

Performance Type

From the drop-down choice menu select one of the following options:

- **Allocated Physical Extents**: Reports on the number of Allocated Physical Extents within the selected physical volume
- **Free Physical Extents**: Reports on the number of free Physical Extents within the selected physical volume
- **Physical Extent Size**: Reports on the size of the Physical Extent within the selected physical volume
- **Physical Volume Size**: Reports on the size of the selected physical volume
- **Total Physical Extents**: Reports on the total number of Physical Extents on the selected physical volume

Physical Volume Display Status

Click **Display Status** on the **Volume Reporting** dialog to display the current **Physical Volume Information** for this system.

Click the **Show In...** button to amend the view by which the physical partition size measurements are displayed. The possible display options are:

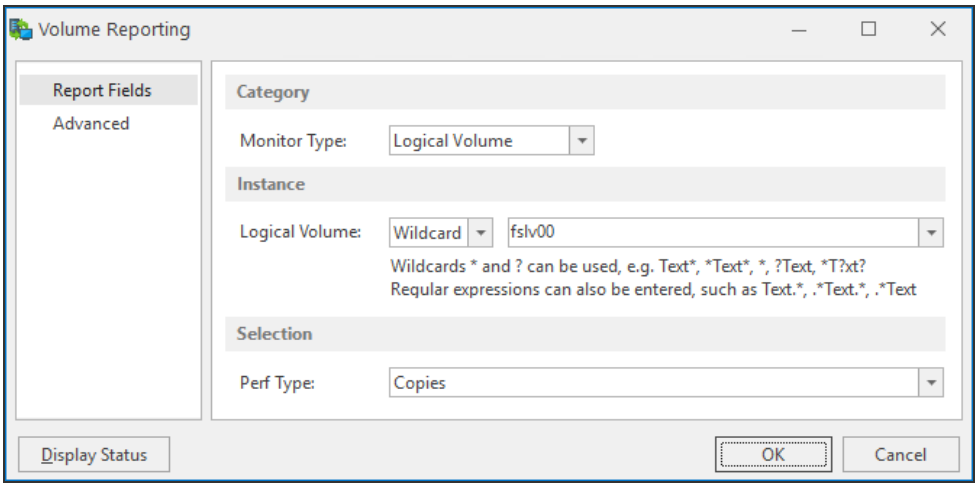
- **B**: Byte
- **KB**: Kilobyte
- **MB**: Megabyte
- **GB**: Gigabyte
- **TB**: Terabyte
- **PB**: Petabyte
- **EB**: Exabyte

3. Click **OK** to exit this display and return to the **Volume Group Reporting** dialog.

Linux Logical Volume Reporting

Linux Logical Volume Reporting provides reporting on the Logical Volumes of a Linux system.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **Logical Volume**.
   This opens the **Volume Reporting** reporting dialog at the **Physical Volume** Monitor Type.



Category section

Monitor Type

Leave this parameter set to the default setting of **Logical Volume**.

Instance section

Logical Volume

Either select the name of the **Logical Volume** from the drop-down choice menu or use **Wildcards** or **Regular Expressions** (Regex) to define the name of the **Logical Volume** on which reporting is required.

Selection section

Performance Type

From the drop-down choice menu select one of the following options:

- **Current Logical Extent**: Reports on the number of Current Logical Extents within the selected logical volume
- **Segments**: Reports on the number of segments within the selected logical volume
- **Size**: Reports on the size of the selected logical value

Logical Volume Display Status

Click **Display Status** on the **Volume Reporting** dialog to display the current **Logical Volume Information** for this system.

Click the **Show In...** button to amend the view by which the physical partition size measurements are displayed. The possible display options are:

- **B**: Byte
- **KB**: Kilobyte
- **MB**: Megabyte
- **GB**: Gigabyte
- **TB**: Terabyte
- **PB**: Petabyte
- **EB**: Exabyte

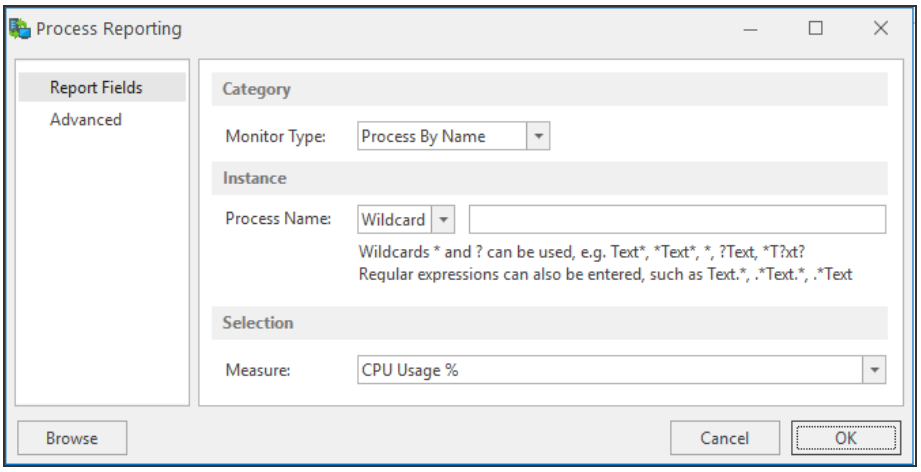
3. Click **OK** to exit this display and return to the **Volume Group Reporting** dialog.

Linux Process Reporting

Provides reporting on the processes running on a Linux system.

1. From the required **Linux System - Reporting Monitor** main panel, click **Add Field**.
2. From the **Select Category** dialog, select **CPU**.

This opens the **CPU, Filesystem and Memory** reporting dialog at the **CPU** Performance Group.



Category section

Monitor Type

There are three possible options when selecting the Process Monitor Type:

- Process By Name
- Process By Owner
- Process By PID

Instance section

Process Name

Either type the name of the **Linux process** on which reporting is required or use **Wildcards** or **Regular Expressions** (Regex) to define the name of the process.

> **NOTE:** Wildcards and Regular Expressions cannot be used when the Monitor Type is Process by PID

Selection section

Measure

From the drop-down choice menu select one of the following options:

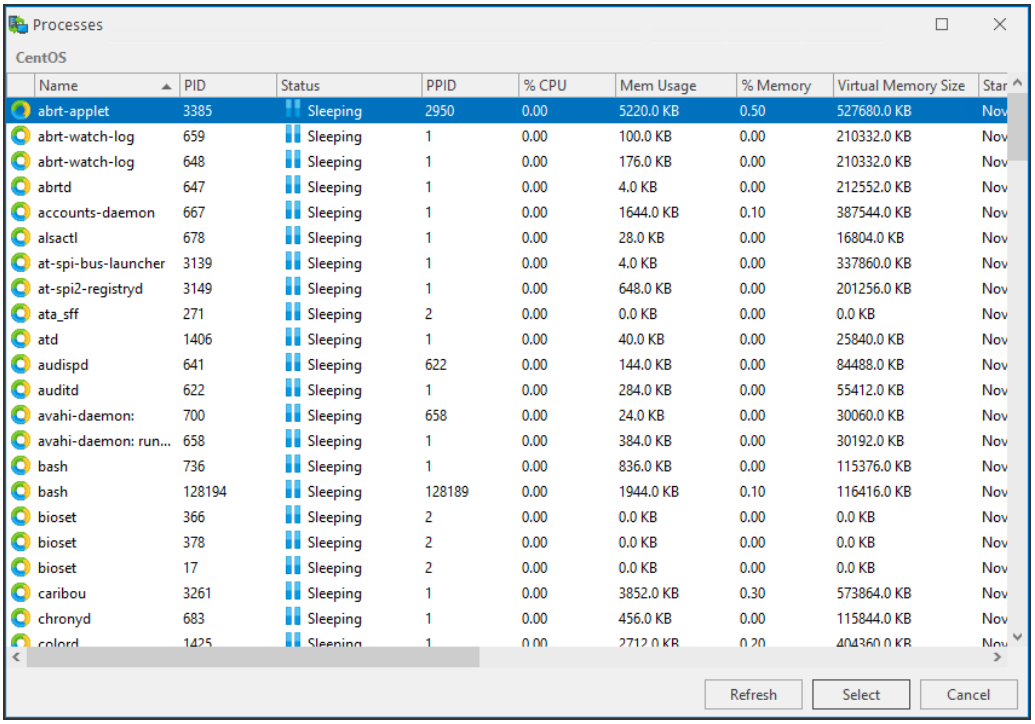
- **CPU Usage %**: Reports on the amount of CPU (expressed as a percentage value)
- **Cumulative CPU Time**: Reports on the cumulative CPU Time used by the selected process
- **Elapsed Time**: Reports on the time elapsed since the selected process was started

- **Number of Processes**: Reports on the number of processes running under the selected name
- **Process Physical Memory Used**: Reports on the amount of physical memory used by the selected process
- **Process Physical Memory Used %**: Reports on the amount of physical memory used by the selected process expressed as a percentage value
- **Virtual Memory Size**: Reports on the amount of virtual memory used by the named process

Process Browse

It is also possible to select any additional processes that may be running on this system for inclusion in Linux Reporting.

From the **Process Reporting** dialog, click **Browse** to open the list of Processes for this system.



Use the vertical scroll bar to move through the list of available processes.

3. Click on a process so that it is highlighted and click **Select** to automatically add the process so that it appears in the **Process Name** parameter of the **Process Reporting** dialog.

Linux Reporting Advanced Settings

Advanced Settings, available from the left navigation panel when setting reporting criteria, can be used to specify instances that can be ignored, to avoid triggering an unnecessary alert.

To specify instances that can be ignored:

1. Having set the required reporting criteria, select the **Advanced** tab.

> NOTE: If the **Ignore the following instances** box is unavailable, the option cannot be used for the selected criteria.

2. Click **Add** to open the **Add Instance Name** dialog.
3. Enter the name of the **Instance** that you wish to be ignored if encountered. Click **OK**.
4. Continue to add instances or click **OK** to save the changes and close the **Criteria** dialog.

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.

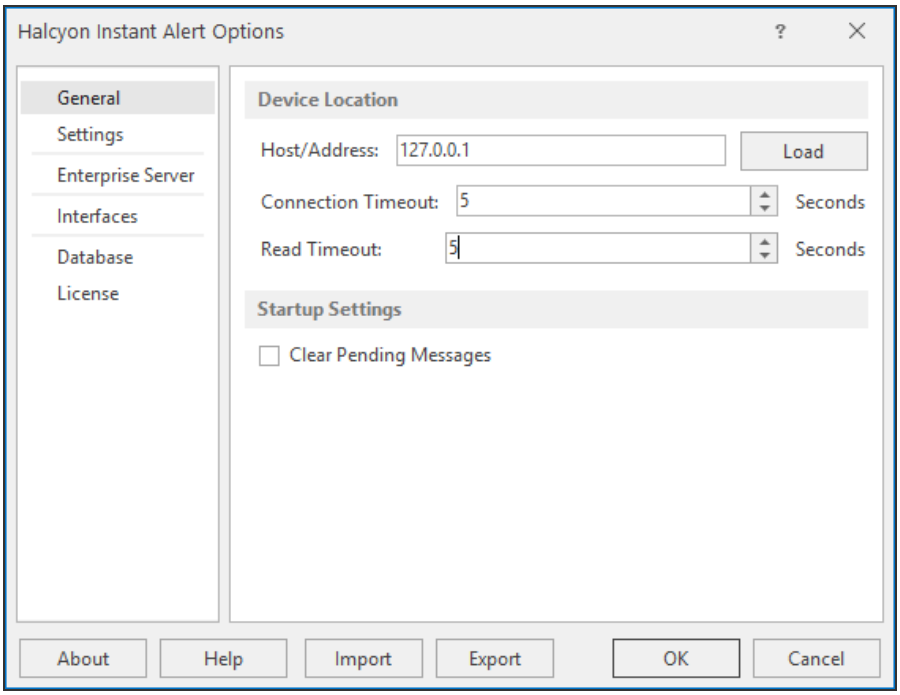
Learn more about Instant Alert Message Sender

Instant Alert Server Options

Instant Alert Server Options are used to configure various interfaces associated with Instant Alert and Network 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 Network Server Suite Configuration Guide.

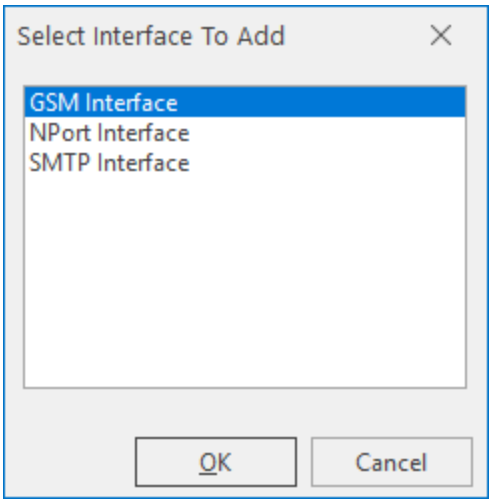
Adding Instant Alert Interfaces

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

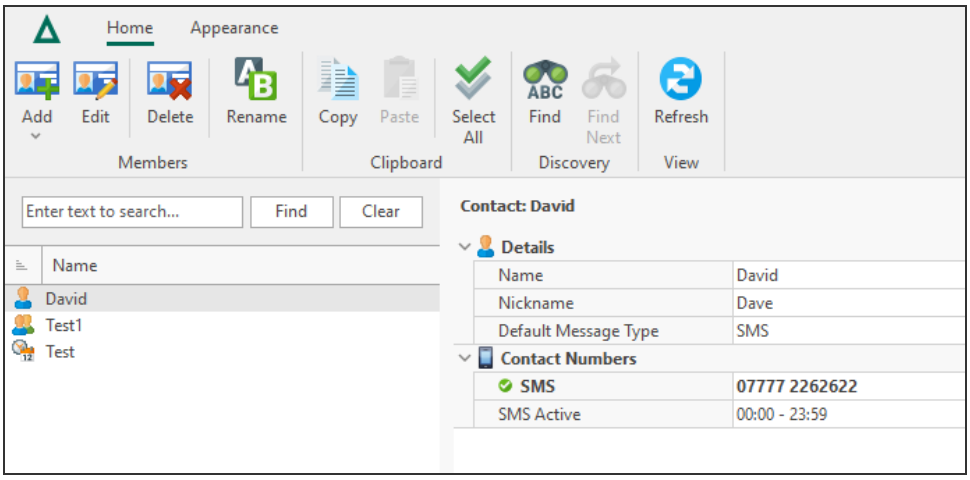
A call schedule is a list of employees with responsibilities for a given time period. A call schedule is a method of ensuring that the correct person is contacted at the right time, in the event of an alert being raised.

Roster

A roster is a list that shows the order in which a group of people will perform a duty or job. For example, "a duty roster".

The Address Book Main Display

Upon opening the Address Book, an alphabetical list of all the defined Contacts, Broadcast Groups, Call Schedules and Rosters that have been defined.



Click on any item in the list to display the details of the selection.

TIP: If there are multiple entries, use the search facility to locate the item of your choice.

Add

Click **Add** to create a new Contact, Broadcast Group, Schedule or Roster. The appropriate dialog opens depending on the selection made.

Edit

Click **Edit** to amend the details of the selection.

Delete

Click **Delete** to remove the selection from the Address Book.

Rename

Click **Rename** to open a dialog enabling you to change the name of the selection.

Copy

Click **Copy** to create a duplicate of the selection. You can then use Paste to complete the transaction.

Paste

Click **Paste** to complete the procedure following the use of the Copy action. A new item is created, identifiable by the insertion of the word Copy after the item name. Use the Rename option to create a unique name for the copied item. Note that Paste is unavailable for selection unless a Copy action has been initiated.

Select All

Click **Select All** to select all items in the Address Book list for selection prior to using one of the other options on this display.

Find

Click **Find** to open a dialog into which alphanumeric text can be entered. Click OK to discover any items in the Address Book that contain the entered characters.

Find Next

Click **Find Next** to discover the next instance of the previously entered alphanumeric text in the Address Book.

Refresh

Click **Refresh** to update the display with any new Address Book information that has been created since this instance of the Address Book was opened.

Address Book Appearance

Use the options in the Appearance tab to change the look of the Instant Alert Address Book.

From the Instant Alert Address Book menu ribbon, click **Appearance**.

Dark Mode

Use the toggle switch to change the display mode from light (default setting) to dark.

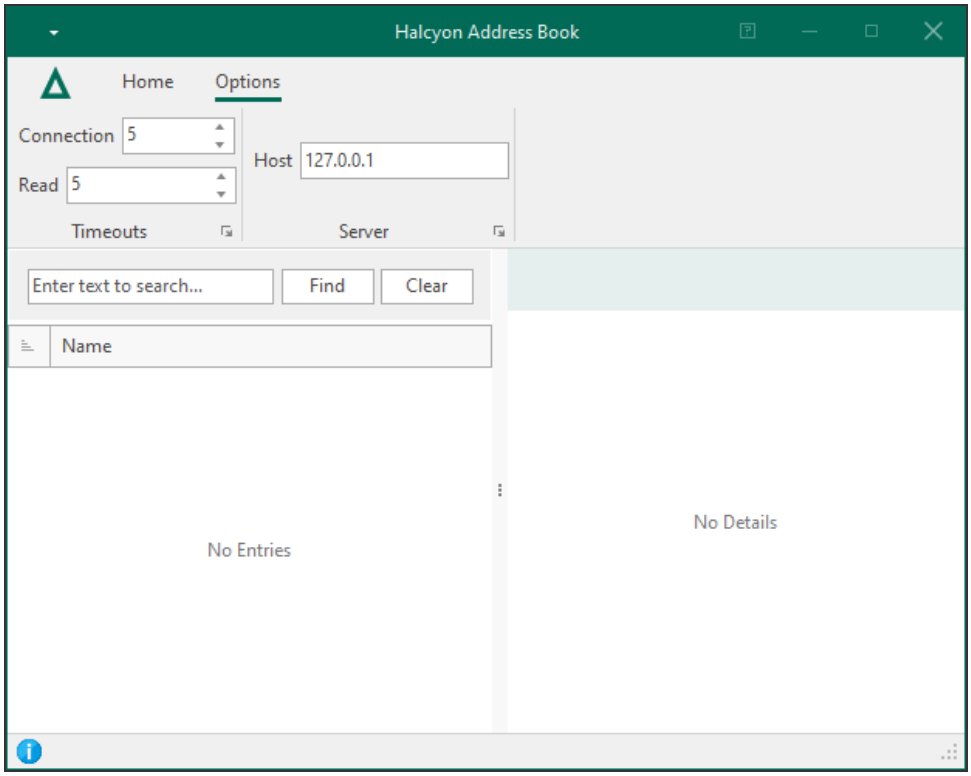
> IMPORTANT: Dark Mode is saved per user and not by the application.
>
> Setting Dark Mode in any one of the UI ribbons applies it across all of the Network Server Suite applications, even those not currently loaded, which will then use the theme once opened.

Click the toggle switch again to return to the default light mode setting across all Network Server Suite applications.

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.

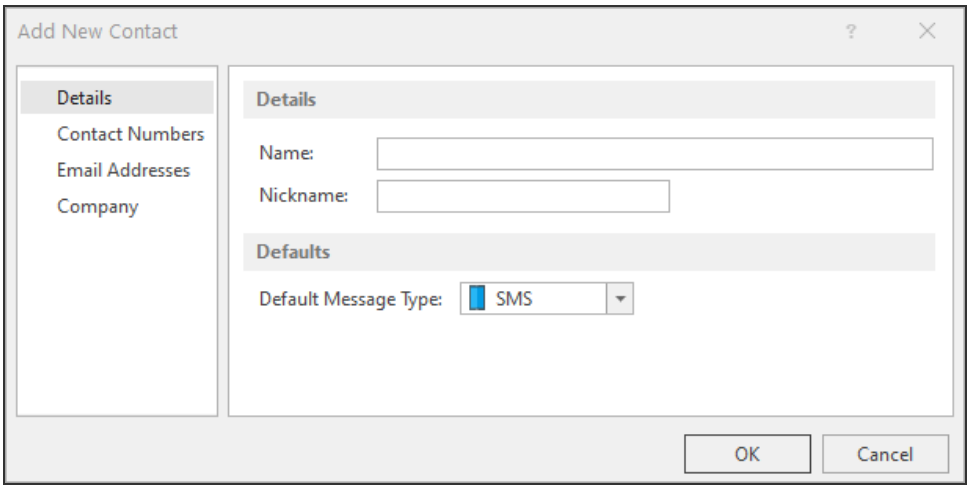
Adding a Contact to the Instant Alert Address Book

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.

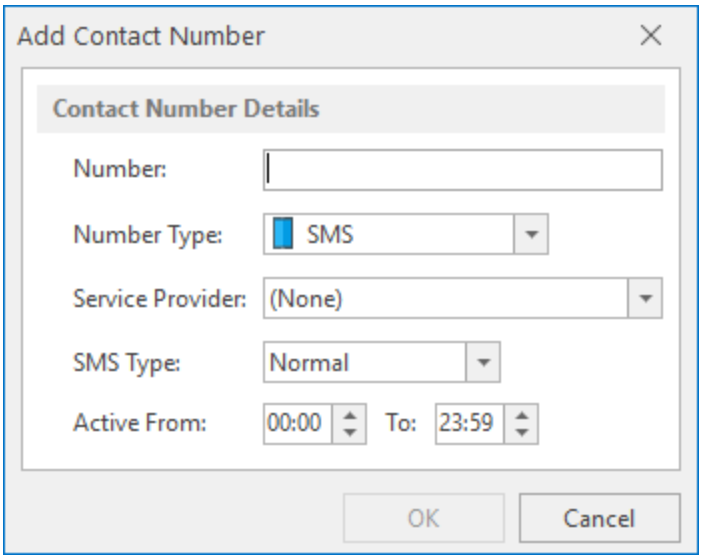
Adding a Number to a Contact

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.

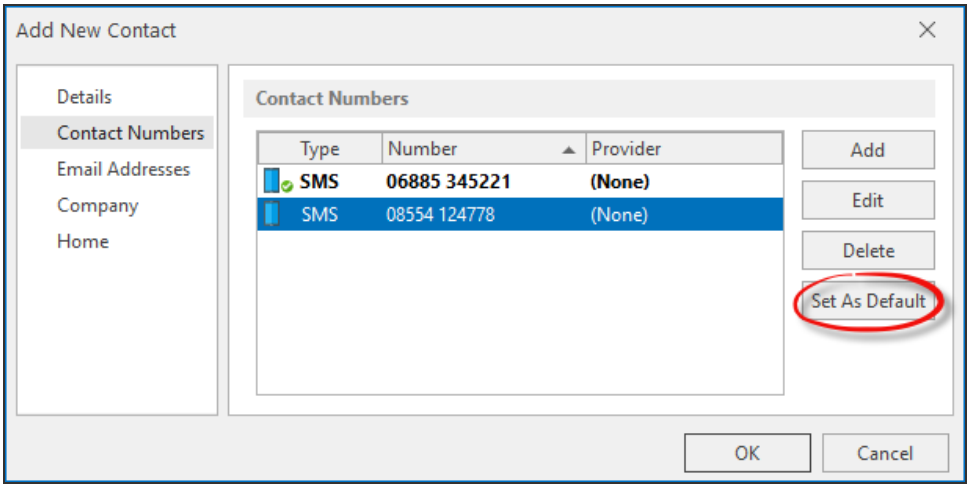
Working with Contact Numbers

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.

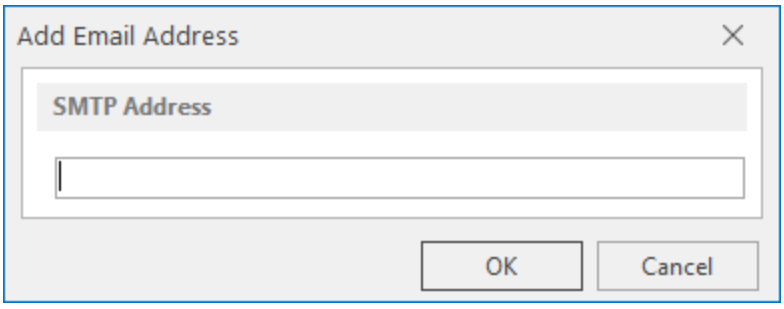
> **WARNING:** Deleting a number also removes it from any Broadcast Groups or Call Schedules to which it belongs.

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**.

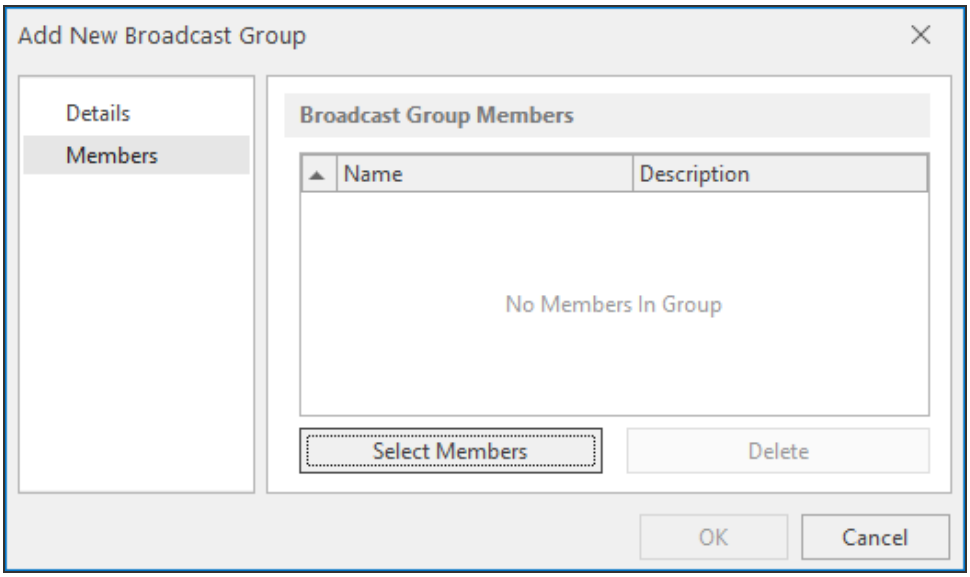
Working with Email Addresses

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

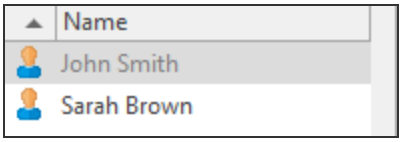
Should a contact no longer use this email address, it is possible to remove it.

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.

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**.

Call Schedules

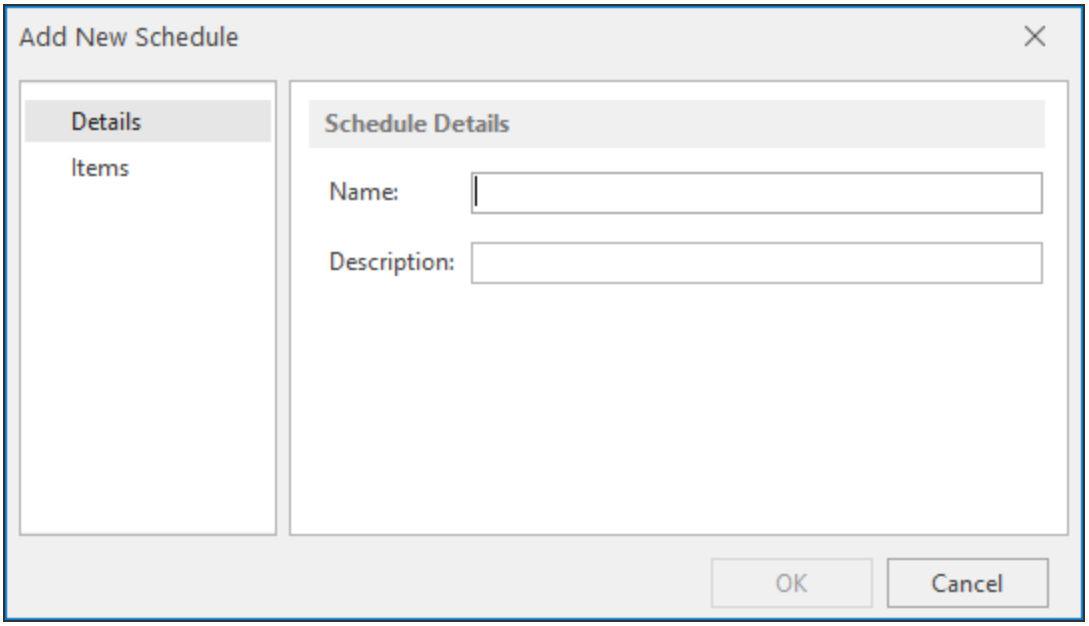
A call schedule is a method of ensuring that the correct person is contacted at the right time, in the event of an alert being raised.

> **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.

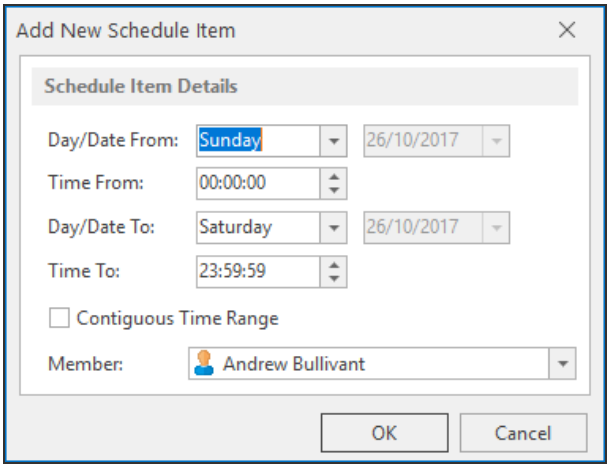
See Adding a Schedule Item for more information.

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.

Working with Call Schedule Items

The following section describes the options for working with call schedule items.

Editing a Call Schedule item

Should a different working pattern be required, it is possible to edit an existing call schedule to meet the new requirements.

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Call Schedule** for which the number information has changed.
3. From the **Home** | **Members** panel, select **Edit**. The **Edit Call Schedule** dialog is displayed.
4. From the left navigation panel select **Items**.
5. From the **Schedule Items** panel select the item to be edited and click **Edit**.

6. The details of the call schedule item can now be edited using the same fields as when adding a call schedule item.
7. Click **OK** to confirm the changes.

Deleting a Call Schedule Item

Should a call schedule item no longer be required, it can be removed from the call schedule.

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Call Schedule** for which the number is no longer required.
3. From the **Home** | **Members**panel select **Edit**. The **Edit Call Schedule** dialog is displayed.
4. From the left navigation panel select **Items**.
5. From the **Schedule Items** panel select the schedule item to be removed and click **Delete**.
6. When prompted, click **OK** to confirm the deletion.

Working with Call Schedules

Once Instant Alert Call Schedules have been defined, they can be edited, deleted, copied and renamed. A search facility is also provided should an extensive list of contacts exist.

Call Schedules are displayed alongside contacts and broadcast groups in the left-hand panel of the Address Book and, by default, are listed in alphabetical order.

Editing Call Schedules

The current details of any call schedule can be amended at any time. For assistance with editing a call schedule item please see: Editing a call schedule item.

To edit the details of a call schedule:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Call Schedule** for which the information has changed.
3. From the **Home** | **Members** panel, select **Edit**. The **Edit Call Schedule** dialog is displayed.
4. Use the same parameters as when adding a call schedule to update the call schedule information.
5. Once complete, click **OK** to confirm and save the changes.

Deleting Call Schedules

If a call schedule is no longer required, it can be removed from the Address Book. For assistance with removing a call schedule item please see: Deleting a call schedule item.

To delete a call schedule:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Call Schedule** that is to be removed from the Address Book.
3. From the **Home** | **Members** panel, select **Delete**.
4. When prompted, click **Yes** to confirm or **No** to cancel the deletion.

Copying Call Schedules

Copying call schedules is a useful and quick way of adding schedules without having to create a new entry each time. When a call schedule 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 schedule. Once updated, the schedule can be renamed to the actual call schedule name.

To copy a call schedule:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Call Schedule** 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 call schedule is now displayed in the list as '**Call Schedule Name - Copy**'. Use the Edit Call Schedule functionality to amend the required details. Use the Rename functionality to give the copied call schedule a unique identity.

> TIP: To copy all of the contact, call schedule and broadcast group details in one action, use **Select All** from the **Clipboard** panel.

Renaming Call Schedules

The primary use of renaming call schedules is to give a unique identity to call schedules which have previously been copied.

The Edit functionality cannot be used to change the name of a call schedule.

To rename a call schedule:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Call Schedule** that is to be renamed.
3. From the **Home** | **Members**panel, select **Rename**.
4. When prompted, enter the new name for the call schedule and click **OK**.

Broadcast Groups

A broadcast group is a team of people who have an interest in a specific function or routine.

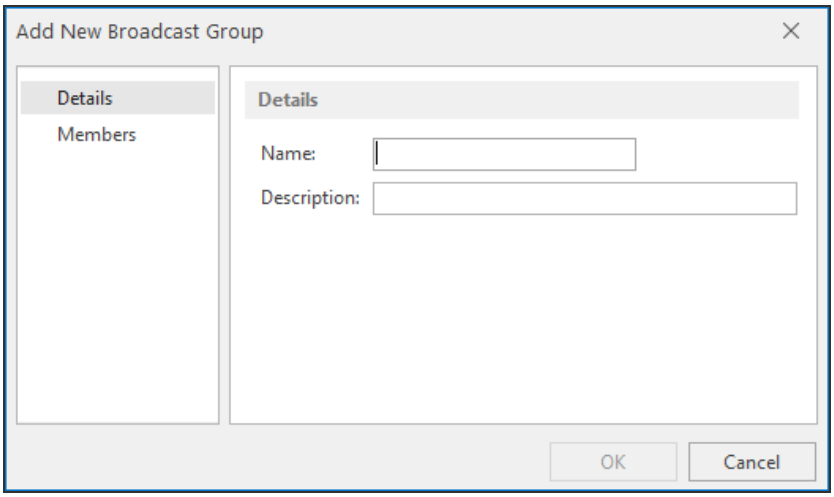
For large organizations it may be that many people are involved in very specific functions or routines across a department. For example, different support groups for different operating systems. In smaller organizations it is likely that one or two people have the responsibility of running all functions.

> **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.

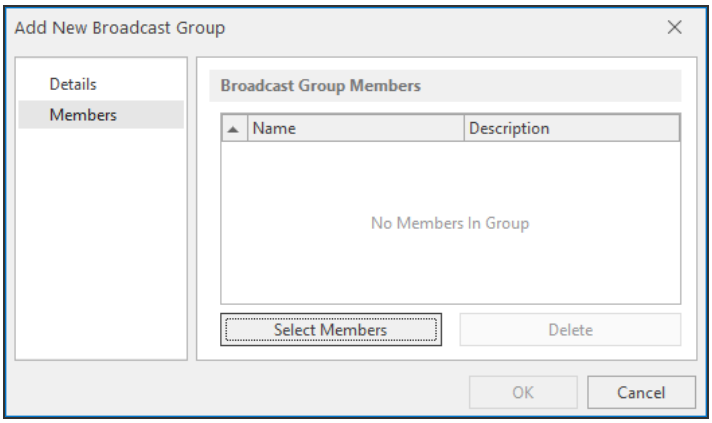
See Working with Broadcast Group Members for more information on how to add and remove members from this broadcast group.

Adding and Removing Members in a Broadcast Group

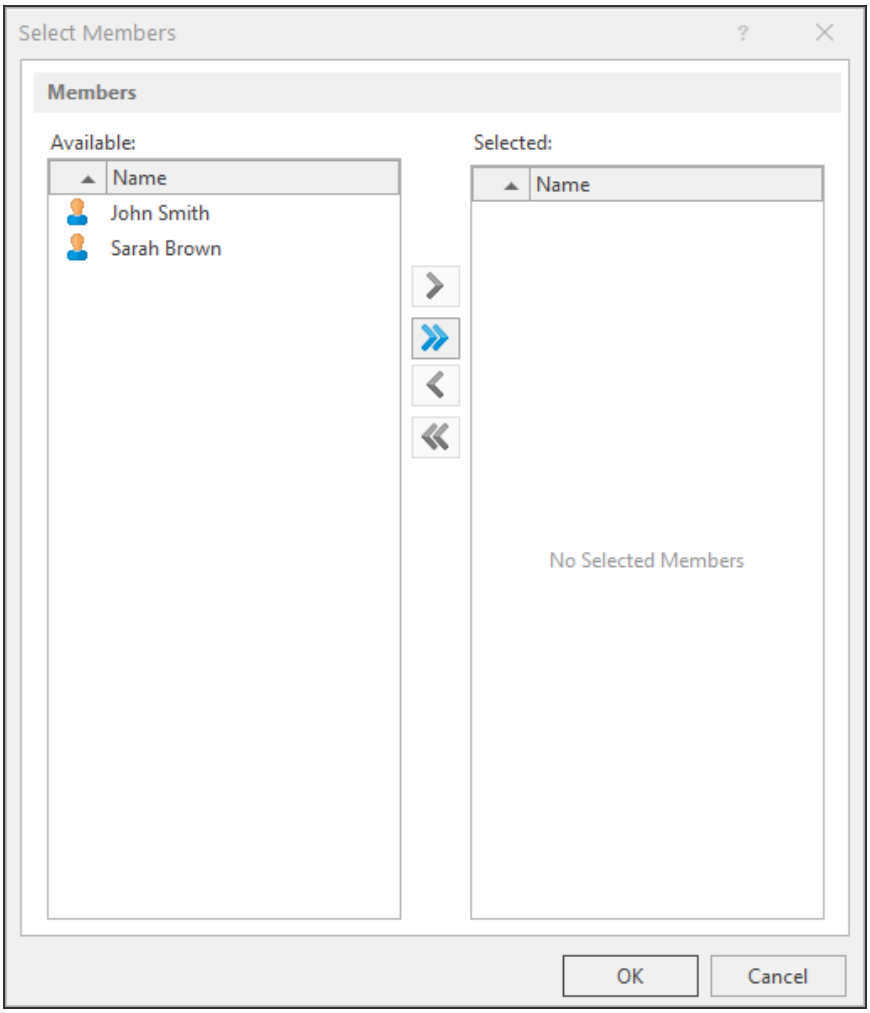
The following section describes how to add and remove single and multiple members from a broadcast group.

> **NOTE:** For the purposes of broadcast groups, a member is a contact, call schedule or broadcast group.

Members are added and removed using **Select Members** when Adding or Editing a broadcast group.



Click **Select Members** to open the Select Members dialog from where members can be added and removed from the broadcast group.



Adding single members to a broadcast group

1. From the list of members, click on the one that you want to add to this broadcast group. It is now highlighted.
2. Click [›] to transfer the member from the **Available** panel to the **Selected** panel.

Adding multiple members to a broadcast group

Multiple members can be added to a broadcast group in the following ways:

Select all members

To select all the available members for a broadcast group click [»].

You do not need to click on any of the members first when using this option.

All members are transferred from the **Available** panel to the **Selected** panel.

Select a continuous block of members

To select a continuous block of members, click on the first member to be included in the list, hold down the Shift key and click on the last member to be included in the list.

All the members between the two mouse-clicks are now selected.

Click › to transfer the block of members from the **Available** panel to the **Selected** panel.

Select multiple members

To select multiple member that are not in a continuous block, keep a finger depressed on the Ctrl key while you single-click on each member.

Once finished selecting members, click › to transfer all selected members from the **Available** to the **Selected** panel.

Click **OK** to create the broadcast group.

Removing members from a broadcast group

Removing members from a broadcast group is a reversal of the above process.

You select the members in the **Selected** panel and use the ‹ and « reverse arrows to transfer them back to the **Available** panel.

Working with Broadcast Groups

Once Instant Alert Broadcast Groups have been defined, they can be edited, deleted, copied and renamed. A search facility is also provided should an extensive list of contacts exist.

Broadcast groups are displayed alongside contacts and call schedules in the left-hand panel of the Address Book and, by default, are listed in alphabetical order.

Editing Broadcast Groups

Only the **Description** field can be amended when editing broadcast groups. For assistance with adding and removing members in a broadcast group please see: Working with Broadcast Group Members.

> **NOTE:** It is not possible to amend the contact name using the Edit function. Use the Rename function instead.

To edit the description of a broadcast group:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Broadcast Group** for which the information has changed.
3. From the **Home** | **Members** panel, select **Edit**. The **Edit Broadcast Group** dialog is displayed.
4. Enter a new **Description** for the Broadcast Group.
5. Click **OK** to confirm and save the changes.

Deleting Broadcast Group

If a broadcast group is no longer required, it can be removed from the Address Book. For assistance with removing members from a broadcast group please see: Removing members from a broadcast group.

To delete a broadcast group:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Broadcast Group** that is to be removed from the Address Book.
3. From the **Home** | **Members** panel, select **Delete**.
4. When prompted, click **Yes** to confirm or **No** to cancel the deletion.

Copying Broadcast Groups

Copying broadcast groups is a useful and quick way of adding broadcast groups without having to create a new entry each time. When a broadcast group 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 group. Once updated, the broadcast group can be renamed to the actual broadcast group name.

To copy a broadcast group:

1. Open the **Instant AlertAddress Book**.
2. Find and select the **Broadcast Group** 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 broadcast group is now displayed in the list as '**Broadcast Group Name - Copy**'. Use the Edit Broadcast Group functionality to amend the Description. Use the Rename functionality to give the copied broadcast group a unique identity.

> TIP: To copy all of the contact, call schedule and broadcast group details in one action, use **Select All** from the **Clipboard** panel.

Renaming Broadcast Groups

The primary use of renaming broadcast groups is to give a unique identity to broadcast groups which have previously been copied.

The Edit functionality cannot be used to change the name of a call schedule.

To rename a broadcast group:

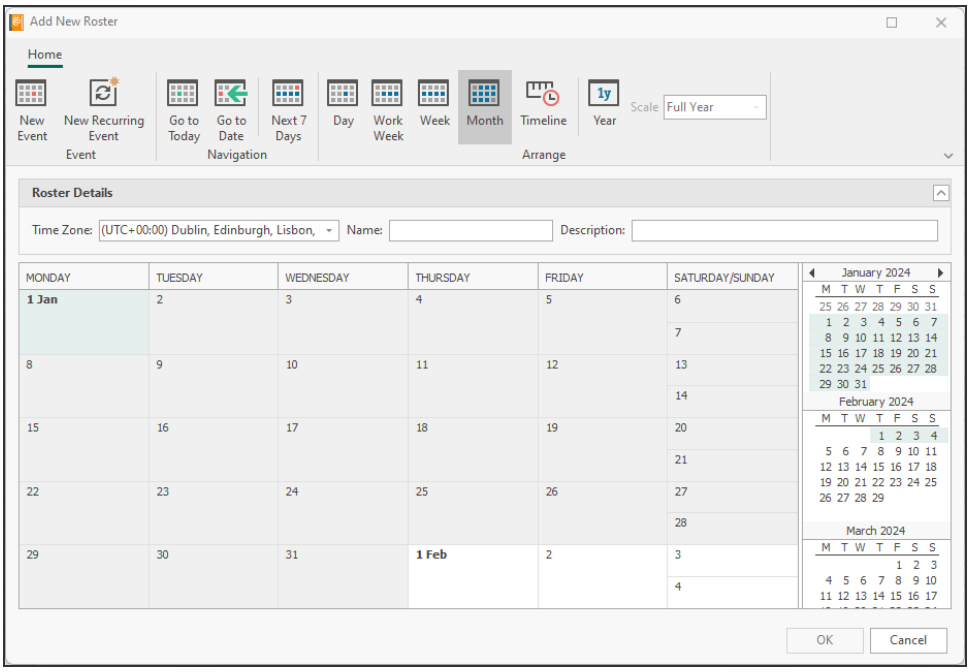
1. Open the **Instant AlertAddress Book**.
2. Find and select the **Broadcast Group** that is to be renamed.
3. From the **Home** | **Members**panel, select **Rename**.
4. When prompted, enter the new name for the broadcast group and click **OK**.

Rosters

A roster is a list that shows the order in which a group of people will perform a duty or job. For example, "a duty roster".

Adding a New Roster

From the Instant Alert Address Book select **Add** and then **Roster** from the drop-down menu. The Add New Roster dialog is displayed.



Options on the Add New Roster display

Options on this display allow you to add, view and group events.

Roster Details

These settings contain the parameters that define the Roster within the Address Book.

Time Zone

Use the drop-down menu to select the World time-zone in which this Roster operates.

Name

Enter a unique name for the Roster.

Description

Enter a description that identifies and explains the purpose of the Roster.

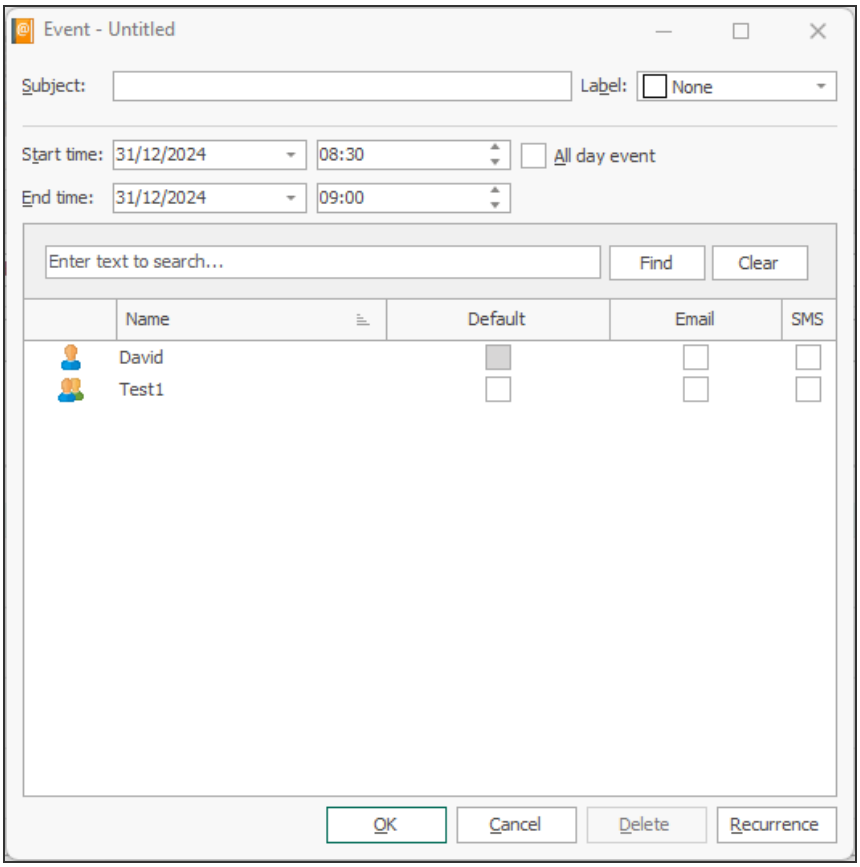
Adding New Events to a Roster

There are two types of event that can be added to a roster.

- A single, one-off event
- A recurring event that repeats every day, week, month or year over a specified time period.

Adding a New Event

Click **New Event** to add a single event to the roster. The Event - Untitled dialog is displayed.



Subject

Enter the unique alphanumeric name of the event to be added to the roster.

Label

If required, use the drop-down menu in the Label field to identify what type of event this is, based on specific time elements, such as Out of Hours, Morning, Weekend and so on.

Start time

Enter the date on which the event is to start. Use the drop-down arrow to display a calendar which can then be used to select the required date.

> TIP: The date that is initially displayed is determined by the position of the highlighted square in the calendar list to the right of the main panel.

Enter the time of day at which this event is due to start. Use the Up and Down arrows in this field to change the hour at which the event starts. Also see All Day Event.

End Time

Enter the date on which the event is to finish. Use the drop-down arrow to display a calendar which can then be used to select the required date.

> TIP: The date that is initially displayed is determined by the position of the highlighted square in the calendar list to the right of the main panel.

Enter the time of day at which this event is due to end. Use the Up and Down arrows in this field to change the hour at which the event ends. Also see All Day Event.

All Day Event

Click **All Day Event** to specify that the event lasts all day and therefore no actual start and end times need to be entered.

Selection

From the main panel on this display, select the Contacts, Call Schedules and Broadcast Groups and the method of contact which this event uses in the Roster.

- **Default**: The default contact method for this selection is used.
- **Email**: Email is used as the contact method
- **SMS**: Short Message Service is used as the contact method.

> **NOTE:** More than one method may be selected for each Contact, Call Schedule or Broadcast Group.

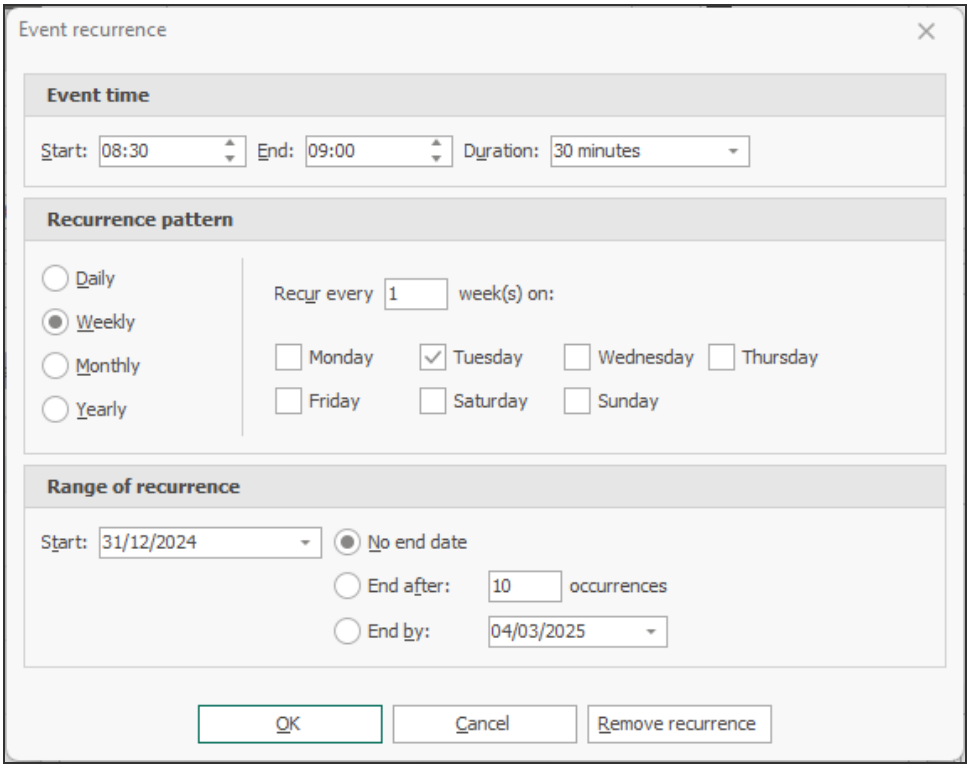
Recurrence

Click **Recurrence** to open the Event Recurrence dialog. See Adding a New Recurring Event.

Click **OK** to create the new event for the Roster.

Adding a New Recurring Event

Click **New Recurring Event** to add a recurring event to the roster. The Event recurrence dialog is displayed.



Event time

Use the options in the Event time section to specify the time dynamics of the recurring event

- **Start**: Enter the time at which the event is to start. Then enter one of the following:
- **End**: Enter the time at which the event is due to end. The entry in the Duration field changes accordingly.
- **Duration**: Enter the duration of the event. The entry in the End field changes accordingly.

Recurrence pattern

The recurrence over which the event can be defined in one of four ways. Subsequent criteria change in this section depending on the selection made:

- **Daily**: Select this option to specify that the event occurs on a daily basis. The following options are available:
  - **Every n day**: Enter the daily interval at which this event occurs. The default is every day.
  - **Every weekday**: Select this option to specify that the event occurs on every weekday (not weekends).
- **Weekly**: Select this option to specify that the event occurs on a weekly basis. The following options are available:
  - **Recur every n week on**: Enter the number of weeks between which this event occurs. The default setting is every week.
  - **Days**: Specify the days of the week on which the event occurs. Multiple selections are allowed.
- **Monthly**: Select this option to specify that the event occurs on a monthly basis. The following options are available:
  - **Day**: Specify on which day of which month this event occurs. The default setting is the first day of every month.
  - **The n day of every n month**: Use this option to generate a more detailed occurrence of the event by specifying:
    - The first, second, third, fourth or last...
    - Day, Weekday, Weekend Day, Specific Day...
    - Of every single or every number of months.
- **Yearly**: Select this option to specify that the event occurs on a yearly basis. The following options are available:

- **Every Month and Date**. The default setting is the first of January.
- **The n day of a month**: Use this option to generate a more detailed occurrence of the event by specifying:
    - The first, second, third, fourth or last...
    - Day, Weekday, Weekend Day, Specific Day...
    - Of a specified month.

Range of recurrence

Fields in this section specify the number of times that the event reoccurs before ending. The following options are available:

- **Start**: Specify on which date of the year this event starts
- **No end date**: The event continues infinitely
- **End after**: Specify the number of occurrences of the event that must run before it ends. The default setting is 10 occurrences.
- **End by**: Specify the actual date on which the event stop recurring.

Click **OK** to add the recurring event to the Roster.

Working with Rosters

The information in this section provides detailed instructions for working with Rosters.

Roster Details

From the left-navigation panel in the main Address Book display, click on the Roster for which you want to view the details.

The main panel of the Address Book displays the full details of the Roster including:

- **Name**: The name of the Roster
- **Description**: The unique description given to the Roster
- **Time Zone**: The time zone in which the Roster operates
- **Events** (which in turn display):
    - **Name**: The name of the event
    - **Label**: The label given to identify the event
    - **Duration**: The time period over which the event runs
    - **Start Date/Tme**: The Date and Time which the event starts
    - **End Date/TIme**: The Date and Time at which the event finishes
    - **Members**: The names of the members in the vent and their contact methods
- **Exceptions**: The details of any exceptions that may have been made to a recurring ecvent

Navigation

Use the options in the Navigation section to select a date to view.

Today

Select **Today** to go to today's date (if you are currently viewing a date other than today). This date is shown as the highlighted day in the current Roster view.

Go To Date

Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Next 7 Days

Select **Next 7 Days** to display the next 7 days, starting with the selected date in the Calendar, in the main panel of the Rosters display.

Roster Views

Roster views allow you to drill down into specific time periods and view, add, edit and delete rosters .

Roster views are available when Adding and Editing events.

Roster views can be selected from the menu ribbon by clicking on the required selection.

Roster views when selecting a blank time slot

When Selecting a blank time slot in a Roster view, the following options are available. The options are dependent on the view selected.

Day

Select **Day** to display the event contents of a specific day. The day displayed is controlled by the date highlighted in the Calendar selection. You can change the date by clicking on a new date in the Calendar. In addition to viewing the events that exist for this day, further options are also available:

Right-click on an empty time slot in the main Day panel to display a pop-up menu with the following options:

- **New Event**: Select **New Event** to create a new event at the time point on the day at which the right-click was initiated. See Adding a New Event.
- **New All Day Event**: Select **New All Day Event** to create a new event that lasts all day for the day on which the right-click was initiated. See All Day Event.
- **New Recurring Event**: Select **New Recurring Event** to create a new recurring event at the time point on the day at which the right-click was initiated. See Adding a New Recurring Event.
- **Today**: Select **Today** to go to today's date (if you are currently viewing a date other than today)
- **Go To Date**: Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Work Week

Select **Work Week** to display the event contents of a specific working week. The week displayed is controlled by the date highlighted in the Calendar selection and starts on the Monday of the week chosen. You can change the date by clicking on a new date in the Calendar. Note that the view changes back to Day. In addition to viewing the events that exist for the work week, further options are also available:

Right-click on an empty time slot in the main Work Week panel to display a pop-up menu with the following options:

- **New Event**: Select **New Event** to create a new event at the time point on the day in the week at which the right-click was initiated. See Adding a New Event.
- **New All Day Event**: Select **New All Day Event** to create a new event that lasts all day for the day in the week on which the right-click was initiated. See All Day Event.
- **New Recurring Event**: Select **New Recurring Event** to create a new recurring event at the time point on the day in the week at which the right-click was initiated. See Adding a New Recurring Event.
- **Today**: Select **Today** to go to today's date (if you are currently viewing a date other than today). This date is shown as the first day in the Work Week display.
- **Go To Date**: Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Week

Select **Week** to display the event contents of a specific full week (including weekends). The week displayed is controlled by the date highlighted in the Calendar selection and starts on the Monday of the week chosen. You can change the date by clicking on a new date in the Calendar. Note that the view changes back to Day. In addition to viewing the events that exist for the week, further options are also available:

Right-click on an empty time slot in the main Week panel to display a pop-up menu with the following options:

- **New Event**: Select **New Event** to create a new event at the time point on the day in the week at which the right-click was initiated. See Adding a New Event.
- **New All Day Event**: Select **New All Day Event** to create a new event that lasts all day for the day in the week on which the right-click was initiated. See All Day Event.
- **New Recurring Event**: Select **New Recurring Event** to create a new recurring event at the time point on the day in the week at which the right-click was initiated. See Adding a New Recurring Event.
- **Go To This Day**: Select **Go To This Day** to open the selected date in Day view.

- **Today**: Select **Today** to go to today's date (if you are currently viewing a date other than today). This date is shown as the first day in the Week display.
- **Go To Date**: Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Month

Select **Month** to display the event contents of a specific full month. The month displayed is controlled by the date highlighted in the Calendar selection. You can change the date by clicking on a new date in the Calendar. Note that the view changes back to Day. In addition to viewing the events that exist for the month, further options are also available:

Right-click on an empty time slot in the main Month panel to display a pop-up menu with the following options:

- **New Event**: Select **New Event** to create a new event on the day in the week at which the right-click was initiated. See Adding a New Event.
- **New All Day Event**: Select **New All Day Event** to create a new event that lasts all day for the day in the week on which the right-click was initiated. See All Day Event.
- **New Recurring Event**: Select **New Recurring Event** to create a new recurring event on the day in the week at which the right-click was initiated. See Adding a New Recurring Event.
- **Go To This Day**: Select **Go To This Day** to open the selected date in Day view.
- **Today**: Select **Today** to go to today's date (if you are currently viewing a date other than today). This date is shown as the first day in the Week display.
- **Go To Date**: Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Year

Select **Year** to display the event contents of a specific year. The year displayed is controlled by the date highlighted in the Calendar selection. You can change the date by clicking on a new date in the Calendar. Note that the view changes back to Day.

You can also select the **Scale** by which you want the Year to be displayed:

- **Full Year**: The full year is displayed in the main panel
- **Half Year**: The half year containing the selected date is displayed in the main panel
- **Quarter**: The quarter year containing the selected date is displayed in the main panel

In addition to viewing the events that exist for the year, further options are also available:

Right-click on an empty time slot in the main Year panel to display a pop-up menu with the following options:

- **New Event**: Select **New Event** to create a new event on the day in the year at which the right-click was initiated. See Adding a New Event.
- **New All Day Event**: Select **New All Day Event** to create a new event that lasts all day for the day in the year on which the right-click was initiated. See All Day Event.
- **New Recurring Event**: Select **New Recurring Event** to create a new recurring event on the day in the week at which the right-click was initiated. See Adding a New Recurring Event.
- **Go To This Day**: Select **Go To This Day** to open the selected date in Day view.
- **Today**: Select **Today** to go to today's date (if you are currently viewing a date other than today). This date is shown as the highlighted day in the Year display.
- **Go To Date**: Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Timeline

Select **Timeline** to display the current schedule of events from the selected date highlighted in the calendar. You can change the date by clicking on a new date in the Calendar. In addition to viewing the events, further options are also available:

Right-click on an empty date slot in the main Timeline panel to display a pop-up menu with the following options:

- **New Event**: Select **New Event** to create a new event on the day in the agenda at which the right-click was initiated. See Adding a New Event.
- **New All Day Event**: Select **New All Day Event** to create a new event that lasts all day for the day in the year on which the right-click was initiated. See All Day Event.
- **New Recurring Event**: Select **New Recurring Event** to create a new recurring event on the day in the week at which the right-click was initiated. See Adding a New Recurring Event.
- **Go To This Day**: Select **Go To This Day** to open the selected date in Day view.
- **Today**: Select **Today** to go to today's date (if you are currently viewing a date other than today). This date is shown as the highlighted day in the Year display.
- **Go To Date**: Select **Go To Date** to open a dialog allowing you to select both the date to which to go to and the view in which you want it displayed.

Roster views when selecting an existing event

The above options are available when right-clicking on an empty slot in the chosen calendar view. Right-clicking on an existing event in the view provides access to the following menu options:

Open

Select **Open** to display the event ready for Editing.

Label

Select **Label** to open a sub-menu from where a new label for the event can be chosen. See Label.

Delete

Select **Delete** to remove the event from the Roster.

> WARNING: There is no prompt if you select the Delete action. The event removal takes place immediately.

Calendar

Calendar views are available on the right-hand side of both the Add and Edit Roster dialog.

Use the Calendars display to select the day on which the Roster views are based and on which events are created.

Today's date is highlighted by default whenever the Add Roster option is selected. When Editing an event, the date on which the event is scheduled is displayed in the Calendar view.

Click on a new date in the Calendar to open the main panel at the chosen date. Note that this works for all views except Year.

You can move through the Calendar (either backwards or forwards in time) by using the directional arrows at the top of the Calendar panel.

Work with Roster Options

Editing a Roster

It is possible to edit an existing Roster in one of two ways:

- From the left-hand panel of the Address Book, select the Roster you want to edit from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. From the menu ribbon click the **Edit** icon.
- From the left-hand panel of the Address Book, select the Roster you want to edit from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. Right click and select **Edit** from the pop-up menu.

Renaming a Roster

It is possible to rename an existing Roster in one of two ways:

- From the left-hand panel of the Address Book, select the Roster you want to rename from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. From the menu ribbon click the **Rename** icon.
- From the left-hand panel of the Address Book, select the Roster you want to rename from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. Right click and select **Rename** from the pop-up menu.

Copying a Roster

It is possible to copy an existing Roster in one of two ways:

- From the left-hand panel of the Address Book, select the Roster you want to copy from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. From the menu ribbon click the **Copy** icon.
- From the left-hand panel of the Address Book, select the Roster you want to copy from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. Right click and select **Copy** from the pop-up menu.

You can now use Paste to create a copy of the Roster which can then be renamed.

- From the menu ribbon click the **Paste** icon.
- Right click in the left-hand panel of the Address Book and select **Paste** from the pop-up menu.

Deleting a Roster

It is possible to delete an existing Roster in one of two ways:

- From the left-hand panel of the Address Book, select the Roster you want to delete from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. From the menu ribbon click the **Delete** icon.

- From the left-hand panel of the Address Book, select the Roster you want to delete from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. Right click and select **Delete** from the pop-up menu.

When prompted, click **Yes** to confirm the deletion or No to cancel.

Working with Roster Events

Editing an Event

To edit an event:

1. From the left-hand panel of the Address Book, select the Roster you want to edit from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. From the menu ribbon click the **Edit** icon.
2. Go to the date on which the event that you want to edit exists.
3. Right-click on the event and select **Open** from the pop-up menu. The Event dialog opens ready for editing.
4. Once Editing is complete, click **OK** to confirm.

Renaming an Event

To rename an event:

1. Follow steps 1 to 3 in Editing an Event.
2. Change the entry in the **Subject** field.
3. Click **OK** to confirm

Deleting an Event

To delete an event:

1. Follow steps 1 to 2 in Editing an Event.
2. Right-click on the event and select **Delete** from the pop-up menu.

> WARNING: There is no prompt if you select the Delete action. The event removal takes place immediately.

Alternatively:

1. From the left-hand panel of the Address Book, select the Roster you want to edit from the list of Contacts, Call Schedules, Broadcast Groups and Rosters. From the menu ribbon click the **Edit** icon.
2. Go to the date on which the event that you want to edit exists.
3. Right-click on the event and select **Open** from the pop-up menu. The Event dialog opens ready for editing.
4. From the Event dialog, click **Delete**.

Creating a Recurring Event from an existing Event

1. Follow steps 1 to 3 in Editing an Event.
2. On the Event dialog, click Recurrence to open the Event Recurrence dialog.
3. Follow the instructions in Adding a New Recurring Event.

Finding Contacts, Call Schedules, Broadcast Groups and Rosters

If the Address Book database contains many contacts, call schedules, broadcast groups and Rosters, the **Find** functionality can be used to search for entries with a unique or shared name.

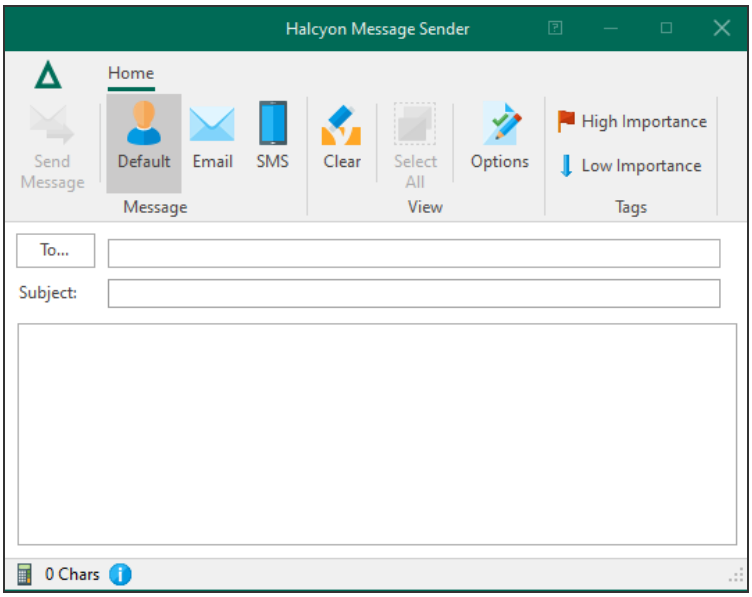
To find a contact, call schedule, broadcast group or roster in the Address Book database

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, broadcast groups and rosters 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.

Message Sender Appearance

Use the options in the Appearance tab to change the look of Instant Alert Message Sender.

From the Instant Alert Message Sender menu ribbon, click **Appearance**.

Dark Mode

Use the toggle switch to change the display mode from light (default setting) to dark.

IMPORTANT: Dark Mode is saved per user and not by the application.

Setting Dark Mode in any one of the UI ribbons applies it across all of the Network Server Suite applications, even those not currently loaded, which will then use the theme once opened.

Click the toggle switch again to return to the default light mode setting across all Network Server Suite applications.