

Quick Reference Card for NerveCenter 5.1.06

Viewing NerveCenter Objects

NerveCenter contains lists of all defined objects. You can open the following lists from the Admin menu or from the toolbar:



The Property Group List window displays all property groups and their properties.



The Node List window displays all nodes and indicates if they are managed or suppressed. This window also displays the severity associated with any node that has an active alarm instance.



The Poll List window displays all polls and indicates if they are on. This list also displays each poll's property and the MIB base object that the poll monitors.



The Mask List window displays each trap mask, its generic trap, any associated enterprise, and its trigger name.



The Alarm Definition List window displays each alarm, its property and scope, and whether it's on.



The Correlation Expression List window displays each correlation expression.



The Alarm Severities List window lists severity levels and types.



The Perl Subroutine List window displays all Perl subroutines used by alarm actions.



The Reports window displays all available reports, report descriptions and authors.



The Action Router Rule List window displays all Action Router conditions and actions.



The Server Status window contains the current settings for any NerveCenter to which you are connected.

TO VIEW NOTES ABOUT AN OBJECT

- ◆ From a NerveCenter list window, select an object and click **Notes**.

Monitoring Alarms

You use the following windows to monitor alarms:



The Alarm Summary window displays alarm instances for the connected server.



The Aggregate Alarm Summary window displays alarm instances collectively for all servers to which you are connected.

TO CHANGE THE ACTIVE CONNECTED SERVER

- ◆ If connected to more than one server, select the server you want from the drop-down listbox on the NerveCenter toolbar.

TO SORT ALARM INSTANCES

- ◆ Click the button at the top of the column you want to use for sorting. Click again to reverse the sort order.

TO VIEW AN ALARM INSTANCE'S HISTORY

- ◆ Double-click the alarm instance. Select each item in the list to trace activity to the current state. Select a button, if enabled, to view an associated poll, node, trap mask, or alarm.

TO VIEW ALL INSTANCES OF AN ACTIVE ALARM

- ◆ From the Alarm Definition List window, select the alarm and click the **Alarms** button.
-

Resetting Alarm Instances

You can reset alarm instances from the following windows:

Alarm Definition List	Right-click one or more alarms and choose Reset to Ground .
Alarm Summary	Right-click the alarms and reset to ground or another state.
Alarm Instances	Right-click the alarms and reset to ground or another state.
Node Definition	In either Alarms tab, select Reset All to reset all alarms for a node.

Filtering Alarms

NerveCenter enables you to filter alarms by severity, property group, and IP subnet. You can apply a filter to a NerveCenter Server before or after connecting to the server.

TO ASSOCIATE AN EXISTING FILTER WITH A SERVER

1. From the **Client** menu, choose **Configuration** and select the **Alarm Filter Selection** tab.
2. From the Server list, select the name of the server whose alarms you want to filter.
3. Select one or more filters in the Available Filters list, and click >>.
4. Select **OK**.

TO DEFINE OR MODIFY A FILTER

1. From the **Client** menu, choose **Configuration** and select the **Alarm Filter Modification** tab.
2. Select **New** to define a filter and **Edit** to change an existing filter.
3. Enter your filter parameters in the Alarm Filter Definition window.
4. When finished, click **OK**.

Exporting Behavior Models

TO EXPORT AN ALARM AND ITS ASSOCIATED OBJECTS

- ◆ From the Alarm Definition List window, right-click the alarm and choose **Export Model**, then provide a name for the model file.

Viewing Log Files

If your alarms are assigned logging actions, you can view the following logged data:

File log	ASCII files are stored in the following locations: <ul style="list-style-type: none"> ◆ Windows: <i>installation</i>\Log directory on the server. ◆ UNIX: <i>installation</i>/userfiles/logs directory on the server.
Event or system log	<ul style="list-style-type: none"> ◆ Windows: From the Start menu, choose Administrative Tools > Event Viewer. ◆ Linux: View the system log in <i>/var/log/messages</i> using the following command: tail -f /var/log/messages ◆ Solaris: View the system log in <i>/var/adm/messages</i> using the following command: tail -f /var/adm/messages
Database	Available only on Windows in the <i>installation</i> \Db directory on the server. This data can be used in reports.

Auditing Behavior Models

Check for triggers that aren't defined in a trap mask or poll, mask/poll triggers not used in an alarm, or alarm states transitioned by undefined triggers.

TO RUN AN AUDIT

1. From the **Admin** menu, choose **Audit**.
2. Select one or more checkboxes corresponding to the conditions you want to audit.
3. Select **Run Audit**.