



NSP Network Services Platform

Release 19.11

Fault Management Application Help

3HE-15156-AAAE-TQZZA

Issue 1

November 2019

Legal notice

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2019 Nokia.

Contents

1	Fault Management	5
1.1	Overview	5
1.2	Top Unhealthy NEs view	5
1.3	Alarm List views	6
1.4	Top Problems view	11
1.5	Inspector view	12
1.6	Fault Management settings	13
1.7	Fault Management general operations	16
2	Fault Management Procedures	17
2.1	Fault Management procedures	17
	Displaying alarms	19
2.2	How do I configure current alarm list settings?	19
2.3	How do I configure historical alarm list settings?	19
2.4	How do I configure which columns are displayed in an alarm list?	20
2.5	How do I configure column sorting in an alarm list?	21
2.6	How do I create an advanced filter?	21
2.7	How do I create a watched filters list or alarm sublist?	22
	Investigating alarms	23
2.8	How do I find the object affected by an alarm?	23
2.9	How do I list other objects impacted by an alarm?	23
2.10	How do I display alarms from the point of view of an object?	23
2.11	How do I display the root cause of an alarm?	23
2.12	How do I export high-severity alarms to a file?	24
2.13	How do I configure an e-mail policy?	24
	Managing alarms	26
2.14	How do I configure system alarm settings?	26
2.15	How do I acknowledge an alarm?	26
2.16	How do I delete or clear an alarm?	27
2.17	How do I edit alarm custom text?	27
2.18	How do I automate alarm management using a policy?	28
2.19	How do I configure multiple alarm policies at the same time?	29
2.20	How do I suppress all alarms raised on a port or NE?	31
2.21	How do I open an SSH or Telnet session with an NE?	31
2.22	How do I automate escalating or de-escalating alarms?	32

1 Fault Management

1.1 Overview

The Fault Management application provides alarm monitoring, correlation, and troubleshooting for the most unhealthy NEs in the network. Filter alarm lists, identify root causes, and determine alarm impacts.


Fault Management components are also available in other applications in the NSP suite, such as Network Supervision and Service Supervision. Quickly investigate network problems and assess service impact with Fault Management and on-application alarm lists. Target specific alarms by filtering on set criteria.

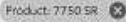



1.2 Top Unhealthy NEs view


Overview

The Top Unhealthy NEs view displays the NEs in your network with the highest number of alarms in a matrix format. NEs are represented as tiles, with alarm count information and links to alarm lists for the selected NE.

Manage the order and content of your Top Unhealthy NEs view using the following tasks:

- **Control what's visible in the matrix.** Click on the Filter button  and select one of these options:
 - Product - Select a product type from the list and you'll only see that NE product type in the matrix.
 - Topology Group - Select a topology group from the list and you'll only see NEs in that topology group in the matrix.
 - Chassis Type - Select a hardware chassis type from the list and you'll only see NEs of that chassis type in the matrix.
 - Unlocked Only - Select this option to see only unlocked NEs in the matrix.

The filters appear as chip filters  at the top of the matrix. Click the Close button on a chip filter to remove it from the matrix.
- **Sort the matrix NE tiles.** Click the sort menu in the top right-hand corner of the matrix and select one of these options:
 - Total Active - NE tiles are sorted by the number of alarms against them.
 - Total Unacknowledged Active - NE tiles are sorted by the number of unacknowledged alarms against them.
 - Impact Counts - NE tiles are sorted by the number of network objects impacted by alarms on each NE.
- **View current alarms on an NE.** Hover over the More icon  on the NE tile and click the Current Alarms button .
- **View current and historical alarms on an NE.** Hover over the More icon and click the Merged Alarms button .

- **View historical alarms on an NE.** Hover over the More icon ******* on the NE tile and click the Historical Alarms button .
- **View additional details.** Click on the Show More icon on the NE tile and select More Details to expand the tile.
- **Open an NE session.** Click on the Show More icon ******* on the NE tile and select Open NE Session. You can only open a session with an NE that is managed using the NFM-P.
- **Export a list of unhealthy NEs to a local CSV file.** Click More **⋮** > Export.

1.3 Alarm List views

Overview

The alarm list views present all alarms against NEs in your network. The lists can be filtered and sorted in a variety of ways to reduce the number of visible alarm messages to a manageable number. Open an alarm list from a specific NE to view alarms only for that NE. Open the general Alarm List view to see alarms for your entire network. There are three categories of alarm lists:

- The **current alarm list** displays all active alarms in the network, or for specific NEs.
- The **merged alarm list** displays all active and previously-active alarms in the network (or for specific NEs) over a specified time period.
- The **historical alarm list** displays all previously-active alarms in the network (or for specific NEs) over a specified time period.






Role-based access control in Fault Management


A user's visibility of network equipment is based on role settings, which are configured by an administrator. A user cannot view alarms raised on network equipment that is not a part of their role. See the User Manager Application Help and your network administrator for more information.





Role-based access is not supported on the historical and merged alarms lists, which may show alarms outside of a user's assigned role.

To manage an alarm list

Perform the following operations to manage the order and content of your alarm list:





- **Filter the Current Alarm List by severity.** Click on an alarm severity level icon in the Severity filter selector  to display only alarms of that particular severity level. Click on the Clear Filter button  to clear filters.
- **Filter the Current Alarm List to show root cause alarms only.** Click on the Filter button  and select Show Root Causes Only. A chip filter appears at the top of the list. Click on the close button  to clear column chip filters.
- **Configure an advanced filter for the Current Alarm List.** Click on the Filter button  and select Advanced Filter.

In the Advanced Filter form, specify a name and configure one or more filter criteria. Enable the Public option to make the filter available to other users, and accessible for alarm e-mail policies. Save the filter and click on the Apply button to apply it immediately. A chip filter appears at the top of the list. Click on the Close button  to remove the filter.

- **Filter the Historical or Merged Alarm List.** Click on the Source and Time Period chip filters to display alarm messages from a specific source system, and over a specific time period.
- **Filter the alarm list under a specific column.** Type a text string in the text field at the top of a column and press Enter, or use the date picker or drop-down menu (where available) and press Enter. Click on the Clear Filter button  to clear column filters.
- **Sort the alarm list under a specific column.** Click on a column header to sort the list under that column. Click the column header a second time to toggle the sort order (ascending/descending), as indicated by the Up/Down arrow.
- **Refresh the alarm list manually.** Click the Refresh button. 
- **Configure columns.** Right-click on a column header and choose Columns. A list of column names appears.
Click on the names of the columns that you want to display. Click above the column headers on the list to close the column selector and refresh the view.
- **Configure column sorting.** Right-click on a column header and choose Configure Sort. In the Configure Sort form, click Add Level  and choose the first column on which to sort, in ascending or descending order. You can continue to choose columns by which to sort the list. In the Configure Sort form, you can also copy, delete, and re-order selected entries.
- **Export alarms to a local CSV file.** Click More  > Export Visible Rows | All | Selected.

To manage alarm messages

Perform the following operations on selected alarm messages in the alarm list:

- **Acknowledge or unacknowledge an alarm.** On the right-hand side of an alarm item in the list, click More  > Acknowledge Alarm(s) | Unacknowledge Alarms.
You can acknowledge or unacknowledge multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Acknowledge Alarm(s) | Unacknowledge Alarms in the top right-hand corner of the application window.
If you select multiple NFM-P alarms, you can configure the Assigned Severity, and Acknowledgement Note. If you select multiple NFM-T alarms, you can configure the Acknowledgement Note. If you select both NFM-P and NFM-T alarms, you can configure the Acknowledgement Note.
- **Delete or clear an alarm.** Click More  on the right side of a row and choose Delete Alarm(s) | Clear Alarm(s).
You can delete or clear multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Delete Alarm(s) | Clear Alarms in the top right-hand corner of the application window.
- **Assign alarm severity.** On the right-hand side of an alarm item in the list, click More  > Assign Severity.
You can assign the same severity to multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More > Assign Severity in the top right-hand corner of the application window.
- **Assign alarm admin state.** On the right-hand side of an alarm item in the list, click More  > Assign Admin State.




You can assign the same admin state to multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More ******* > Assign Admin State in the top right-hand corner of the application window.

- **Edit alarm custom text.** On the right-hand side of an alarm item in the list, click More ******* > Edit Custom Text.

You can add the same custom text to multiple alarms by pressing the Ctrl key and selecting the alarms, and clicking More ******* > Edit Custom Text in the top right-hand corner of the application window.


To investigate alarms

Perform the following operations to further investigate selected alarm messages in the alarm list:

- **Show alarm details.** A selected alarm list item shows expanded information in the Details panel on the right-hand side of the GUI.
- **Show alarm impacts.** Click Show Impacts  on the right-hand side of an alarm item in the list to open the Impacts diagram for the selected alarm.
Note: This function is not available for alarm messages that are not involved in correlation.
- **Show the root cause of an alarm.** Click Show Root Causes  on the right-hand side of an alarm item in the list to open the Root Cause diagram for the selected alarm.
Note: This function is not available for alarm messages that are not involved in correlation.
- **Show the objects impacted by an alarm.** Click Show Object Impacts  on the right-hand side of an alarm item in the list to view the objects that are impacted by the alarm.
- **Show alarms from the point of view of an affected object.** On the right-hand side of an alarm item in the list, click More **⋮** > Show Object Point Of View to open the Object Point of View diagram for the selected alarm.
Note: This function is not available for alarm messages that are not involved in correlation.
- **Open an NE session with the affected NE** On the right-hand side of an alarm item in the list, click More ******* > Open NE Session to open an SSH or Telnet session with the affected NE. You can only open a session with an NE managed using the NFM-P.


Watched Filters list

The Watched Filters list shows a summary of up to ten saved filters. You can add or remove saved filters from the list, and click on a filter in the list to display that filter in the Alarm List panel. Perform the following operations to manage filters displayed in the list:

- **Display the Watched Filters list.** Click the Watched Filters  button in the details panel to open the Watched Filters list.
- **Add a saved filter to the list.** Click Add and select one or more filters from the displayed list, then click Add.
- **Remove a saved filter from the list.** Hover over a filter in the list, and click on the Delete button.
- **Edit a saved filter.** Select a filter in the list, and click on the Edit button. The Advanced Filter window appears, with the selected filter displayed.


- **Move a saved filter in the list.** Click and drag a filter row, and move it to a new location in the list.
- **Apply a saved filter to the alarm list.** Click on a filter in the list. The selected filter is applied to the alarm list.
- **Stop applying a saved filter to the alarm list.** Click on the Clear Selection button. The alarm list is returned to an unfiltered state.
- **Choose which columns appear in the list.** Click More > Columns and select the columns to display in the Watched Filters list.


Alarm statistics

The Alarm Statistics chart displays network alarm counts by alarm severity. Click the Alarm Statistics button  to see the chart.

Click More  > Export Data to CSV to export the chart to a CSV file.



Alarm distribution

The Alarm Distribution diagram shows all root cause trees for the most impacting alarms for the network, with root cause alarms with no impacts hidden. Click the Alarm Distribution button  to see the diagram. The inner circle is each root cause alarm. The outer circles are objects impacted by the alarm, with the width of the blocks representing the impact magnitude. Click on an alarm to see its information in the panel on the right.


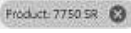


 **Note:** If the managed network yields only alarms with no impact, the Alarm Distribution diagram is blank.

In cases where the number of impacted objects is very high, the Alarm Distribution diagram data content is scaled down to maintain diagram readability. A message appears at the bottom of the diagram, indicating that it has been scaled due to high impact counts.


On the Info panel:


- Click Show Impacts  to open the Impacts diagram.
- Click Alarm List  to open the alarm list for the selected alarm, filtered by the alarm object full name.

Manage the order and content of your alarm distribution diagram using the following tasks:

- **Control what's visible in the alarm distribution diagram.** Click on the Filter button  and select one of the options (date range, name, site ID, product, topology group, or saved filter). Depending on what you select, additional filters options appear. The filters appear as chip filters  at the top of the diagram. Click the Close button on a chip filter to remove it from the diagram.
- **Hide specific alarm types.** Click More  and select the appropriate menu option, then click Refresh to hide acknowledged alarms or maintenance (admin state) alarms.
- **Hide alarms of specific severity.** Click More  and de-select the appropriate severity options, then click Refresh.



Alarm hierarchy

The Alarm Hierarchy diagram shows the most impactful problems in the network, allowing you to locate the biggest problems first, from the root cause alarm to the symptomatic alarms. Click the Alarm Hierarchy button  to see the diagram. Click on a ring or dot to zoom in, and click again to zoom out. Click on an alarm to see its information in the panel on the right.


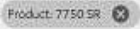


 **Note:** Root cause alarms with no impact are hidden. If the managed network yields only alarms with no impact, the Alarm Hierarchy diagram is blank.

In cases where the number of impacted objects is very high, the Alarm Hierarchy diagram data content is scaled down to maintain diagram readability. A message appears at the bottom of the diagram, indicating that the diagram has been scaled due to high impact counts.

On the Info panel:

- Click Show Impacts  to open the Impacts diagram.
- Click Alarm List  to open the alarm list for the selected alarm, filtered by the alarm object full name.

Manage the order and content of your Alarm Hierarchy diagram using the following tasks:

- **Control what's visible in the Alarm Hierarchy diagram.** Click on the Filter button  and select one of the options (date range, name, system ID, product, topology group, or saved filter). Depending on what you select, additional filters options appear. Add as many of these filters as you need. They appear as chip filters  at the top of the diagram. Click the Close button on a chip filter to remove it from the diagram.
- **Hide specific alarm types.** Click More  and select the appropriate menu option to hide acknowledged alarms or maintenance (admin state) alarms.
- **Hide alarms of specific severity.** Click More  and de-select the appropriate severity options.



Squelch settings

The squelch settings view shows you the squelch status of all ports or NEs monitored by the Fault Management application. You can squelch a specific port or NE to discard all new alarms on the squelched object, and some logical objects associated with a squelched port. Squelched alarms are dropped when received by the NSP, and do not appear as historical events.

 **Note:** Squelching objects is not supported in NFM-T standalone deployments.

 **Note:** You can squelch up to 500 NEs and 1000 ports.

Manage squelched objects using the following tasks:

- **View squelch status of ports.** In the Alarm List or Current Alarms view, click on the Squelch Settings  button. Click on the Close button to return to the previous view.
- **View squelch status of NEs.** In the Squelch Settings view, click on the NE Squelch Settings  button.
- **Filter objects in the list.** Use the filters at the top of each column to filter the list of displayed objects. The list can display up to 100,000 objects.

- **Squelch alarms on an object.** Select an object in the list and click on the Squelch Selected Port or Squelch Selected NE button. To squelch multiple objects, select up to 80 objects in the list and click on Squelch Selected Ports or Squelch Selected NEs in the banner that appears.
- **Unsquelch alarms on an object.** Select an object in the list and click on the Unsquell Selected Port or Unsquell Selected NE button. To unsquell multiple objects, select up to 80 objects in the list and click on Unsquell Selected Ports or Unsquell Selected NEs in the banner that appears.

Alarm squelching behavior

The Fault Management application discards alarms on squelched objects based on the Affected Object and Site ID parameters of the alarm. Squelching an NE discards alarms with a Site ID that matches the squelched NE. Squelching a port discards alarms with an Affected Object parameter that matches the squelched port. Squelching a port also discards alarms for some logical objects associated with the port.




NFM-P alarms

Alarms that are squelched in the Fault Management application are not squelched in the NFM-P, and continue to appear in the NFM-P client. Squelched alarms received from the NFM-P are not displayed in the Current alarm list, but are displayed in the Merged and Historical alarm lists.

1.4 Top Problems view

The Top Problems view displays the alarm types with the most occurrences in the network in the form of a bar chart. Each bar represents a specific alarm type, and its size represents the number of occurrences. The top 50 alarm types with the most occurrences are listed by default, from the highest to lowest number of occurrences. The top problems are polled according to the time interval your administrator set in the system preferences or that you set in your user preferences, from the Settings menu on the NSP Launchpad.

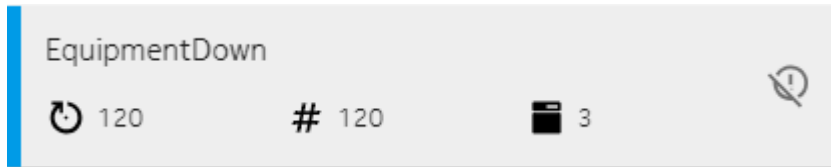
When you hover over a bar in the chart, the corresponding alarm type in the list is highlighted.


- **Sort alarms.** Click the sort menu in the top right-hand corner of the chart and select a sort option (by total number of occurrences, total alarm count, or number of NEs on which the alarm is raised).
- **Display preferences.** click More  and select a display preference for the chart. You can display the alarms by name, probable cause, or specific problem.
- **Filter alarms by severity.** Click on the Filter button  (appears only when the alarms are displayed by alarm name) and select a severity level from the drop-down menu. Only alarms of the selected severity are displayed in the chart. Click the Close button on the chip filter to remove it from the chart.
- **Export list of top problems to a CSV file.** Click More  > Export. Your display and sorting selections are preserved in the CSV file.

Alarm Type list

The Alarm Type list displays name and alarm count information for the top 50 alarm types displayed in the chart. The first icon in an alarm type list item shows the number of occurrences of the alarm







type, the second icon shows the total alarm count, and the third icon shows the number of NEs affected by the alarm type. When you hover over an alarm type in the list, the corresponding bar in the chart is highlighted.



Hide Alarm Types. Hide an alarm type from the list and the chart by clicking the Hide button  that appears when you hover on the right-hand side of an alarm type item. If any alarms are hidden, the Hidden Alarm Type button is enabled on the main toolbar. Click this button to remove the alarm type from the list of hidden alarms (the alarm type is re-displayed).

Top Problems Matrix

The Top Problems Matrix view displays up to 50 NEs on which the selected alarm type occurs. Click on a bar in the Top Problems view to open it in the Matrix view. Each affected NE is represented as a tile. The first icon in a tile shows the number of occurrences of the alarm type and the second shows the total alarm count.

- **View current alarms on an NE.** Hover over the More icon on a tile  and click the Current Alarms button .
- **View historical alarms on an NE.** Hover over the More icon on a tile and click the Historical Alarms button .
- **View current and historical alarms on an NE.** Hover over the More icon on a tile and click the Merged Alarms button .
- **Export a list of unhealthy NEs to a local CSV file.** Click More  > Export.
- **Open an NE session.** Hover over the More  icon on the NE tile and click Open NE Session. You can only open a session with an NE that is managed using the NFM-P.

1.5 Inspector view

In the Inspector, search for specific NEs to be displayed in a matrix.

Adding NEs - Click on Add New NE and use the search menu to select your search criterion. You can enter text in the search field to limit the results or scroll through the list. Up to 256 results are listed. Click on an NE to add it to the beginning of the matrix, or drag an NE to the desired location in the matrix. You can add up to 50 NEs.

Details Click on an NE to view more information about the NE in the Details panel.


Merged Alarms Hover over the right side of the NE and click Merged Alarms to view the merged list of current and historical alarms.

Removing NEs Hover over the right side of the NE and click Remove to remove the NE from the Inspector. Click Remove All to remove all of the NEs from the Inspector.

Open an NE Session Hover over the right side of the NE and click Open NE Session to open an SSH or Telnet session with the NE.

1.6 Fault Management settings

This section describes configuration options for the Fault Management application's appearance and behavior. To access the settings page, click on the More button and choose Settings.

 **Note:** Fault management settings can only be configured by an administrator.

Current Alarms settings

The Current Alarms settings page manages settings related to the alarm database and alarms in the alarm list. These settings apply to NSP, NFM-T, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*. Using this page, you can:

- **Enable alarm aging** Enable the Aging Settings option and configure the number of days after which an alarm is deleted in the Delete After (days) parameter. You can also configure aging for a specific alarm using an alarm policy.
- **Configure when an overflow warning is triggered** Configure the Warning Threshold (%) parameter
- **Purge alarms in the event of an overflow** Select Wrap from the Overflow Action drop-down menu, then configure the percentage of the database to purge in the Purge Amount parameter, and which alarms to purge first in the Purge Policy parameter.
- **Halt alarm collection in the event of an overflow** Select Halt from the Overflow Action drop-down menu.

Historical alarms settings

The Historical Alarms settings page manages settings related to the historical alarm database. These settings apply to NSP, NFM-T, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*. Using this page, you can:

- **Configure archive settings** Enable the Archive Settings pattern and select either the Log on Change or Log on Deletion options.
- **Specify overflow actions** Specify the maximum alarm count, then specify warning and critical thresholds as a percentage of the maximum, and the number of alarms to purge when each threshold is reached.

System Settings

The System settings page manages settings related to NSP, NFM-T, and MDM alarms. Using this page, you can:

- **Enable manual changes to alarms** Enable the Manual Settings parameter, then enable options to allow users to promote, demote, or clear alarms.
- **Configure when users can delete alarms** Enable the Alarm Deletion Settings and Manual

Alarm Deletion Settings parameters, then choose an option that specifies when a user can delete a system alarm (for example, only after it has been acknowledged, or anytime without restriction).

- **Enable notifications for deleting correlated alarms** Enable the Alarm Deletion Settings and Correlated Alarm Settings for Manually Deleted Alarms parameters, then choose an option that specifies whether an alert is displayed when correlated alarms would be deleted by manually deleting a system alarm.
- **Configure automatic deletion of alarms** Enable the Alarm Deletion Settings and Automatic Alarm Deletion Settings parameters, then choose an option that specifies when to automatically delete alarms.
- **Configure automatic acknowledgement of correlated alarms.** Enable the Alarm Acknowledgement Policy and Correlated Alarm Settings for Manually Acknowledged Alarms parameters to automatically acknowledge any correlated alarms when a system alarm is manually acknowledged, and specify whether a GUI notification occurs when the correlated alarms are acknowledged.
- **Configure automatic acknowledgement of cleared alarms.** Enable the Alarm Acknowledgement Policy and Acknowledge alarms when cleared parameters to automatically acknowledge any alarms when they are cleared.

Alarm Policies

The Alarm Policies page manages policies related to NSP, NFM-T, and MDM alarms. When the Fault Management application receives an alarm for the first time, the application creates an alarm policy for the received alarm. You can use an alarm policy to perform automatic operations on an alarm when it is received. Changes to alarm policies are not retroactive, and only apply to alarms received in the future; to modify existing alarms, use the Alarm List view.

You can filter and sort the list using the columns, and select multiple policies at a time to perform mass configurations. Using this page, you can:

- **Squelch alarms.** Select an alarm policy and enable the Squelch option in the Alarm Policy details panel, or select multiple alarm policies then click on the More **•••** button and select Set Squelch.
- **Assign severity.** Select an alarm policy and choose a severity from the Initial Severity Assignment drop-down menu in the Alarm Policy details panel, or select multiple alarm policies then click on the More button and select Initial Severity Assignment.
- **Acknowledge alarms.** Select an alarm policy and enable the Auto Acknowledge option in the Alarm Policy details panel, or select multiple alarm policies then click on the More button and select Set Auto Acknowledge.
- **Disable historical alarm archiving.** Select an alarm policy and disable the History Enabled option in the Alarm Policy details panel, or select multiple alarm policies then click on the More button and select Set History Disabled.
- **Apply custom text.** Select an alarm policy and enter custom text into the Custom Text field on the Alarm Policy details panel, or select multiple alarm policies then click on the More button, select Edit Custom Text, and enter custom text into the dialog box that appears.

- **Restore default values.** Select an alarm policy and click on the Return to Default button in the Alarm Policy details panel, or select multiple alarm policies then click on the More button and select Return to Default.
- **Enable alarm debouncing.** Select an alarm policy and enable the Enable Alarm Debouncing option in the Alarm Debouncing panel, then configure the Hold Period parameter. Alarm debouncing is only available for implicitly cleared alarms.
- **Configure automatic escalation and de-escalation.** Select an alarm policy and click on the Add Policy button to create an escalation or de-escalation policy. See [2.22 “How do I automate escalating or de-escalating alarms?”](#) (p. 32).
- **Configure alarm aging.** Select an alarm policy and configure the options in the Aging Settings panel. Enable Use Global Aging Policy to use the default aging settings configured in the Fault Management application, or disable it and enable Enable Auto Deletion Rule and specify how many days to wait before deleting alarms. Disable both options to disable alarm aging for the selected alarm.

E-mail Policies

The Fault Management e-mail policy feature allows administrative users to configure e-mail notification policies for specific alarm messages in NFM-P, NFM-T, MDM, and NSP. An e-mail policy is configured with a filter. When an alarm message matches the filter criteria, the policy sends alarm notifications to a specified list of up to 20 user e-mail addresses. In order to manage bursts of alarms, e-mail notifications are pooled for up to one minute before sending. If there are more than ten alarms within one minute for a specific policy, a single e-mail notification is sent with a list of ten alarms. Each e-mail policy specifies the maximum number of e-mail notifications (up to 10) that can be sent over a one-hour period. The recipients are notified when the maximum has been reached.

 **Note:** LI and mirror service alarms are not sent in e-mail notifications.

E-mails are not sent for alarm attribute change events, only for alarm creation. For example, if an alarm is created with a severity of major, and the severity is subsequently changed to critical, alarm e-mail policy filters for critical alarms will not include this alarm.

In order for Fault Management to send e-mail notifications, you must configure connection information for an e-mail server through the NSP Launchpad.

Using the E-Mail Policies settings page, you can:

- **Create an e-mail policy** Click on the Create New Policy button and configure the parameters. See [2.13 “How do I configure an e-mail policy?”](#) (p. 24).
- **Configure an e-mail policy** Select an e-mail policy and configure the parameters in the details panel.
- **Disable an e-mail policy** Select an e-mail policy and disable the Enable parameter in the details panel.
- **Delete an e-mail policy** Select an e-mail policy and click the Delete button at the end of the row.

1.7 Fault Management general operations

This section describes specific application functions for which users may need additional information in order to maintain proper system operations. Where appropriate, recommendations are provided to assist in the resolution of functional issues.

Alarm reload behavior

When alarm messages from MDM and NFM-T sources are modified or deleted in the Fault Management application, the change is recorded in the NSP database, but not at the alarm source. If alarms are bulk-reloaded from an MDM or NFM-T source to the Fault Management application, previously modified or deleted alarms from that source are handled in the following manner:

- For alarms with modified fields, any data already in the NSP database is not overwritten by the reloaded alarm.
- Alarms in the NSP database that are tagged as Transient (i.e., not standing alarms) are not deleted by the reload, even if they are no longer present on the source system.

NE session behavior

When you log out of the NSP, any NE sessions you have opened are disconnected. When you log in to the NSP, any NE sessions that remain open elsewhere are also disconnected.

2 Fault Management Procedures

2.1 Fault Management procedures

Purpose

This chapter describes how to perform operations related to displaying, investigating, and managing alarms using the Fault Management application.

Contents

2.1 Fault Management procedures	17
Displaying alarms	19
2.2 How do I configure current alarm list settings?	19
2.3 How do I configure historical alarm list settings?	19
2.4 How do I configure which columns are displayed in an alarm list?	20
2.5 How do I configure column sorting in an alarm list?	21
2.6 How do I create an advanced filter?	21
2.7 How do I create a watched filters list or alarm sublist?	22
Investigating alarms	23
2.8 How do I find the object affected by an alarm?	23
2.9 How do I list other objects impacted by an alarm?	23
2.10 How do I display alarms from the point of view of an object?	23
2.11 How do I display the root cause of an alarm?	23
2.12 How do I export high-severity alarms to a file?	24
2.13 How do I configure an e-mail policy?	24
Managing alarms	26
2.14 How do I configure system alarm settings?	26
2.15 How do I acknowledge an alarm?	26
2.16 How do I delete or clear an alarm?	27
2.17 How do I edit alarm custom text?	27
2.18 How do I automate alarm management using a policy?	28
2.19 How do I configure multiple alarm policies at the same time?	29


2.20 How do I suppress all alarms raised on a port or NE?	31
2.21 How do I open an SSH or Telnet session with an NE?	31
2.22 How do I automate escalating or de-escalating alarms?	32

Displaying alarms

2.2 How do I configure current alarm list settings?

Configure aging and overflow settings for the current alarm list. These settings apply to NFM-T, NSP, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*.


You must have administrator privileges to configure alarm settings.

- 1 _____
Click the More button  and select Settings. The Alarm Settings form opens.
 - 2 _____
Click Current Alarms on the left-hand panel.
 - 3 _____
Enable the Aging Settings option and specify the number of days after which alarms are deleted.
 - 4 _____
Under Overflow Settings, specify the percentage of the maximum alarm count at which an alarm overflow warning is issued. (The maximum alarm count is hard coded at 150000 alarms if NFM-T and NFM-P are deployed in shared mode, or 300000 alarms if NFM-T is deployed alone.)
 - 5 _____
Specify an overflow action. If you choose Halt, all new alarms are dropped. If you choose Wrap, alarms are purged from the database, based on the following settings:
 - Purge Amount - the percentage of the current alarm count to be deleted.
 - Purge Policy - either the lowest severity alarms are deleted first or the oldest alarms are deleted first.
 - 6 _____
Save your changes.
- END OF STEPS _____

2.3 How do I configure historical alarm list settings?

Configure logging and overflow settings for the historical alarm list. These settings apply to NSP, NFM-T and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

- 1 _____
Click the More button  and select Settings. The Alarm Settings form opens.
- 2 _____
Click Historical Alarms on the left-hand panel.
- 3 _____
Enable the Archive Settings option and enable either or both of the Log on Change and Log on Deletion options.
- 4 _____
Under Overflow Settings, specify the maximum alarm count at which an alarm overflow warning is issued.
- 5 _____
Specify a warning threshold as a percentage of the maximum alarm count, and specify the percentage of the alarm count to be purged at the time of the warning message.
- 6 _____
Specify a critical threshold as a percentage of the maximum alarm count, and specify the percentage of the alarm count to be purged at the time of the critical message.
- 7 _____
Save your changes.


END OF STEPS _____

2.4 How do I configure which columns are displayed in an alarm list?

- 1 _____
Right-click on a column header and choose Columns. A list of column names appears
- 2 _____
Click on the names of the columns that you want to display.
- 3 _____
Click above the column headers on the list to close the column selector.

END OF STEPS _____


2.5 How do I configure column sorting in an alarm list?

- 1 _____
Right-click on a column header and choose Configure Sort.
- 2 _____
Click Add Level  and choose the first column on which to sort, in ascending or descending order. You can continue to choose columns by which to sort the list.
- 3 _____
Select an entry and click Copy Level to duplicate the entry. Click the arrows to move the order of the entries.
- 4 _____
Select an entry and click Delete Level to remove it.
- 5 _____
Click on Apply to save and apply the sorting configuration.

END OF STEPS _____

2.6 How do I create an advanced filter?

You can create and save an advanced search filter. Advanced search filters are more detailed than simple search filters.

- 1 _____
Click on the Filter  button to open the advanced filter configuration form.
- 2 _____
Enter a filter name and description, and specify whether you want the filter to be public or private. Multiple filter properties in an advanced search filter are combined using Boolean operators.
- 3 _____
Choose a Boolean operation from the drop-down list:
 - AND - When you combine properties using the AND operator, the search returns objects that meet both or all of the specified criteria
 - OR - When you combine properties using the OR operator, the search returns objects that meet at least one of the specified criteria
 - NOT - When a filter property is preceded by the NOT operator, items that meet the criteria in that filter property are excluded from the results

4

Choose an alarm attribute from the drop-down list, choose a search function, such as equals, between, or is not null, for example, and then choose or enter a value. You can click on the + or - button to add or remove clauses. Click on the +{} button to add sub-clauses.

5

Click Search or Save. Advanced search filters that you save appear in the Saved Filter list.

END OF STEPS

2.7 How do I create a watched filters list or alarm sublist?

You can use the Watched Filters list to display a summary of up to ten saved filters and apply those filters to the Alarm List with a click. Perform the following to add saved filters to the Watched Filters list.

1

Click the Watched Filters  button in the details panel to open the Watched Filters list.

2

Click Add in the Watched Filters panel and select one or more saved filters from the displayed list.

3

Click Add in the list of filters to add the selected filters to the Watched Filters list.

4

Click on a filter in the Watched Filters list to apply the selected filter to the Alarm List.

5


Click and drag a filter row in the Watched Filters list to move the filter in the list.


END OF STEPS

Investigating alarms

2.8 How do I find the object affected by an alarm?

1 _____


Click More  on the right side of a row and choose Show Affected Object to open the affected object of the alarm in the object management application.


 **Note:** When you choose Show Affected Object for an optical alarm on an NFM-T-managed NE, the NFM-T web client opens in a new browser tab. If the alarm is MDM-managed, the MDC application launches. If the alarm is on an NE that is not NFM-T or MDM-managed, the NFM-P launches.

END OF STEPS _____

2.9 How do I list other objects impacted by an alarm?

1 _____


Click Show Object Impacts  on the right side of a row to open the Object Impacts list for the selected alarm.


 **Note:** This function is not available for alarm messages that are not involved in correlation.

END OF STEPS _____

2.10 How do I display alarms from the point of view of an object?

1 _____


Click More  on the right side of a row and choose Show Object Point Of View to open the Object Point of View diagram for the selected alarm.


 **Note:** This function is not available for alarm messages that are not involved in correlation.

END OF STEPS _____

2.11 How do I display the root cause of an alarm?

1 _____


Click Show Root Causes  on the right side of a row to open the Root Causes diagram for the selected alarm.

 **Note:** This function is not available for alarm messages that are not involved in correlation.


END OF STEPS

2.12 How do I export high-severity alarms to a file?

1

Open the Alarm List view or the current alarms list for an NE, and click on an alarm severity level icon in the Severity filter selector  to display only alarms of that severity level.

2

Click on the More  button and select an export option to save the displayed alarms to a CSV file.

END OF STEPS

2.13 How do I configure an e-mail policy?

The Fault Management e-mail policy feature allows administrative users to configure e-mail notification policies for specific alarm messages in NFM-P, NFM-T, MDM, and NSP. See [1.6.5 “E-mail Policies” \(p. 15\)](#) for information about e-mail policies.

You must have administrator privileges to configure alarm e-mail policies.

1

Click the More button  and select Settings. The Alarm Settings form opens.

2

Click E-mail Policies on the left-hand panel.

3

Click on the Create New Policy button .

4

Check or un-check the Enabled option to enable/disable the policy.

5

Type a name for the policy.

6

Select an alarm filter.

The Alarm Filter menu is populated with public advanced filters configured and saved in the Current Alarms list; see [1.3.2 “To manage an alarm list” \(p. 6\)](#).

7

Click on the Add Recipient button and type the e-mail address of an intended recipient for the alarm notification. You can specify up to 20 recipients.

8

Adjust the Max E-mails Per Hour slider to set the maximum number of alarm notifications that can be sent per hour.

9

Click Save to save the e-mail policy.

END OF STEPS

Managing alarms

2.14 How do I configure system alarm settings?

Use this procedure to configure alarm handling options for alarm messages originating from the NSP system for the Fault Management application. These settings apply to NSP, NFM-T, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

1 _____

Click the More button  and select Settings. The Alarm Settings form opens.

2 _____

Click System Settings on the left-hand panel to configure system-wide alarm settings.

3 _____

Enable the Alarm Severity Settings option and then configure manual options, as required.

4 _____

Enable the Alarm Deletion Settings option, as required, and then enable and configure any of the following options:

- Manual Alarm Deletion Settings
- Correlated Alarm Settings for Manually Deleted Alarms
- Automatic Alarm Deletion Settings

5 _____

Enable the alarm acknowledgement policy, as required.


6 _____

Save your changes.

END OF STEPS _____

2.15 How do I acknowledge an alarm?

1 _____

Click More  on the right side of a row and choose Acknowledge Alarm(s) or Unacknowledge Alarm(s).

2

You can acknowledge or unacknowledge multiple alarms by using the Ctrl key and selecting the rows. When you select multiple alarms, the following limitations apply:

- When you select multiple NFM-P alarms, you can configure the Assigned Severity, and Acknowledgement Note.
- When you select multiple NSP, NFM-T, or MDM alarms, you can configure the Acknowledgement Note.
- When you select a mix of NFM-P and NSP, NFM-T, or MDM alarms, you can configure the Acknowledgement Note.


3


Configure the Assigned Severity and Acknowledgement Note and click Save. For NSP, NFM-T, or MDM alarms, configure the Acknowledgement Note and click Save.

END OF STEPS

2.16 How do I delete or clear an alarm?

1

Click More  on the right side of a row and choose Delete Alarm(s) to remove or Clear Alarm(s) to clear the alarm or alarms. You can delete or clear multiple alarms by using the Ctrl key and selecting the alarms.

 **Note:** If the Delete Alarm(s) or Clear Alarm(s) actions are not available, an administrator may need to enable manual alarm deletion or clearing.


2

Click OK on the dialog box to confirm the action, or Cancel to close the dialog box without deleting or clearing the alarms.

END OF STEPS

2.17 How do I edit alarm custom text?

1

Click More  on the right side of a row and choose Edit Custom Text. You can edit custom alarm text for multiple alarms by using the Ctrl key and selecting the alarms.


2

Enter text in the Custom Text field and click OK. You can enter a URL, for example: <http://www.example.com>.

END OF STEPS

2.18 How do I automate alarm management using a policy?

When the Fault Management application receives an alarm for the first time, the application creates an alarm policy for that alarm. You can use an alarm policy to perform operations automatically on future instances of the alarm. See [1.6.4 “Alarm Policies” \(p. 14\)](#) for more information.

1 _____
Click on the More  button in the title banner of the current tab and select Settings.

2 _____
Click on the Alarm Policies tab. A list of alarm policies appears.

3 _____
Select an alarm policy. You can use the column headers to filter or sort the list of alarm policies.

4 _____
Configure the alarm policy parameters in the Alarm Policy details panel. The following table describes the alarm policy parameters.


Parameter	Effect
General Actions	
Squelch	Hides future instances of this alarm. Squelched alarms are not displayed in the Alarm List.
Initial Severity Assignment	Assigns the chosen severity to the alarm when it is received, overriding the severity assigned by the source.
Auto Acknowledge	Acknowledges the alarm when it is received.
History Enabled	Disables or enables historical alarm archiving for the alarm.
Custom Text	Applies the specified custom text to the alarm when it arrives, overwriting any custom text assigned by the source.
Aging Settings	
Use Global Aging Policy	Uses the aging settings configured in the Current Alarms tab of the Fault Management settings page. Enabled by default.

Parameter	Effect
Enable Auto Deletion Rule	Uses individual aging settings for the alarm. When enabled, you can configure the Delete after (days) parameter to specify how long to wait before deleting the alarm. This option is available if Use Global Aging Policy has been disabled.
Alarm Debouncing	
Enable alarm debouncing	Enables debouncing for the alarm. When alarm debouncing is enabled, alarm clear events are held until the specified hold period expires instead of being processed immediately. If an alarm raise event occurs before the hold period expires, the existing debounced alarm is updated with the new occurrence and the event is processed immediately. This prevents unnecessary historical alarm logging and lowers the frequency of alarm NBI notifications for highly active (flapping) alarms.
Escalation Policies	
Escalation threshold	Enables escalation policies for the alarm. Click on the Add Policy button to create an escalation policy.
De-escalation threshold	Enables de-escalation policies for the selected alarm policy. Click on the Add Policy button to create a de-escalation policy.

- 5 _____
Click on the Save button to save your changes.

END OF STEPS _____

2.19 How do I configure multiple alarm policies at the same time?

- 1 _____
Click on the More  button in the title banner of the current tab and select Settings.
- 2 _____
Click on the Alarm Policies tab. A list of alarm policies appears.

3

Choose one or more alarm policies. You can use the column headings to filter and sort the list.

4

Click on the More button in the Alarm Policies panel and choose an action to perform on the chosen alarm policies. The following table describes the available actions.

Action	Effect
Set Squelch	Squelch the selected alarms. Squelched alarms are not displayed in the Fault Management application.
Unset Squelch	Unsquench the selected alarms.
Set History Enabled	Enable historical alarm archiving for the selected alarms.
Unset History Enabled	Disable historical alarm archiving for the selected alarms.
Set Auto Acknowledge	Automatically acknowledge the selected alarms when they are received.
Unset Auto Acknowledge	Do not automatically acknowledge the selected alarms.
Assign Initial Severity...	Assign the chosen severity level to the selected alarms when they are received. Choose "as received" to use the severity level assigned by the alarm source.
Edit Custom Text...	Apply the specified custom text to the selected alarms when they are received.
Set Escalation Policy...	Create an escalation policy for the selected alarms.
Set De-escalation Policy...	Create a de-escalation policy for the selected alarms.
Set to Use Global Aging Settings	Set the selected alarm policies to use the alarm aging settings configured in the Current Alarms tab.
Enable Alarm Policy Aging	Set the selected alarm policies to use the specified alarm aging timeout.
Disable Alarm Policy Aging	Disable the specified aging timeout for the selected alarm policies.
Enable Alarm Debouncing	Enable alarm debouncing for the selected alarm policies and configure an alarm


Action	Effect
Disable Alarm Debouncing	Disable alarm debouncing for the selected alarm policies.
Return to Default	Return all alarm policy parameters for the selected alarms to their defaults.
Export Selected	Export the selected alarm policies to a file.

END OF STEPS

2.20 How do I suppress all alarms raised on a port or NE?

You can use the Fault Management Application to squelch all new alarms raised against an NE or a port, including some logical objects associated with the port. Squelched alarms are dropped when received, and do not appear as historical events.

1


In the Alarm List view, click on the Squelch Settings  button. The Port Squelch Settings view appears, with a list of up to 100,000 ports displayed. You can filter and sort the list using the column headers.

2

To squelch a port, select a port from the list and click on the Squelch Selected Port button at the end of the row. To squelch multiple ports, select up to 80 ports and click Squelch Selected Ports in the banner that appears.

3

To squelch an NE, perform the following:

1. Click on the NE Squelch Settings  button. The NE Squelch Settings view appears, with a list of up to 100,000 NEs displayed. You can filter and sort the list using the column headers.
2. Select an NE from the list and click on the Squelch Selected NE button at the end of the row. To squelch multiple NEs, select up to 80 NEs and click Squelch Selected NEs in the banner that appears.

END OF STEPS

2.21 How do I open an SSH or Telnet session with an NE?

You can use the Fault Management application to open an SSH or Telnet session with an NE in a browser window. You can open a session from an alarm entry or NE tile in any view. You can only open a session with NEs that are managed using the NFM-P.

-
- 1

Perform one of the following:

 - a. To open a session from the Top Unhealthy NEs or Top Problems tabs, click on the Show More button on an NE tile and select Open NE Session.
 - b. To open a session from any alarm list, click on the More button on an alarm entry and select Open NE Session.
 - c. To open a session from the Inspector, hover over the right side of an NE tile and click on the Open NE Session icon.

An NE session form opens in a new tab.
 - 2

Select the type of session in the drop-down menu, and click on the Connect button. For SSH sessions, a Login window appears.
 - 3

Enter the username and password for the NE in the Login window for a SSH session, or in the terminal window for a Telnet session.
 - 4

Click on the Disconnect button when your session is finished to log out and close the session.

i **Note:** You can click Connect to open the session again, or enter an IP address in the IP field and click Connect to open another session with a different NE.


END OF STEPS

2.22 How do I automate escalating or de-escalating alarms?

You can use an alarm policy to automatically escalate or de-escalate an alarm based on configurable triggers. These settings apply to NSP, NFM-T, and MDM alarms. NFM-P alarm settings are configured in the NFM-P GUI; see the *NFM-P Administrator Guide*.

You must have administrator privileges to configure alarm settings.

- 1

Click on the More  button in the title banner of the current tab and select Settings.
- 2

Click on the Alarm Policies tab. A list of alarm policies appears.
- 3

Choose one or more alarm policies. You can use the column headings to filter and sort the list.

4 _____
 Expand the Escalation Policy panel and click on the Add Policy button under the Escalation Policy or De-Escalation Policy list.

5 _____
 Configure the Severity parameter to specify a different severity to be applied to the alarm when the frequency threshold is reached.

6 _____
 Select an Escalation Threshold Type. The following table describes the escalation threshold types. De-escalation policies only support the Frequency threshold type.

Threshold type	Description
Frequency	How many times the alarm has occurred in the last 24 hours.
Number of Occurrences	How many occurrences of the alarm have been reported.
Days without Ack/Clear	How many days have elapsed without the alarm being acknowledged or cleared.

7 _____
 Configure the Escalation Threshold Value parameter for the selected escalation threshold type.

8 _____
 Click Save. The new policy is applied to the alarm.

END OF STEPS _____

