Carrier VoIP

IEMS Fault Management

NN10334-911

Document status: Standard
Document version: 04.02
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

IEMS Fault Management

New in this release

Feature changes

These are the feature changes in this release.

- IPSec Certificate Manager Support

  This feature integrates the Certificate Manager application with IEMS to provide the following capabilities from the IEMS GUI:

  — Add the Certificate Manager as an application to the IEMS topology

  — View Certificate Manager alarms on IEMS

  — Launch the Certificate Manager GUI client from IEMS using single sign-on

- IEMS Fault Feed Failover Time Reduction

  This feature aims to minimize the downtime for critical services during failover. The feature aims to decrease the IEMS NB agent startup time and IEMS server startup time. It introduces the following changes:

  — reduced IEMS fault feed failover time for critical resources by keeping a redundant server in warm standby mode

  — reduced IEMS OSS visibility outage time. Since the IEMS application also provides OSS log feeds, reducing fault feed failover time reduces the duration of OSS invisibility during outages.

  — a new STANDBY status is reported by the **`servquery -status`** command when a redundant server is in warm standby mode. For details, refer to Viewing the IEMS server status in *IEMS Administration and Security*, NN10336-611.

- ERS8600 alarm mapping correction in IEMS

  This feature corrects ERS8600 alarm mappings defined in IEMS system. From (I)SN08, some ERS8600 traps have an incorrect mapping relationship with the IEMS fault code. This causes unknown and

misunderstanding alarms or events in IEMS system. In (I)SN09U, the content of some alarms and events will change.

- MCS System Manager Auto-Failover Support

  This feature introduces System Manager support for auto-failover. This changes the way the data is forwarded or sent to the OSS (IEMS in this case). The changes for IEMS are as follows:

  — SNMP Traps (faults from the System Manager) will have the logical IP Address as their source address and not the physical unit IP address.

  — SNMP Requests will go to the logical IP address of the System Manager to retrieve any fault or performance data.

- IEMS Call Server 2000 SIP integration

  This feature integrates the new SSLines platform SIP applications. It integrates the management of the fault and performance interfaces of the SSLines platform applications. This feature also includes rebranding changes to the existing Session Server managed object.

Introduction

Fault Management is an essential part of network management. IEMS enables you to manage events and alarms raised by managed objects and inventory details of managed objects. IEMS provides Java Web Start Client and Web Client graphic user interfaces the capability to connect and interact with the IEMS server. The IEMS Fault Management documentation is divided into following sections:

- Fault Management using Java Web Start Client

  — "Working with events" (page 7)

  — "Configuring northbound fault feeds" (page 45)

  — "Working with alarms" (page 65)

- Fault Management using Web Client

  — "Working with events in Web Client" (page 95)

  — "Working with alarms in Web Client" (page 111)

Working with events

The IEMS event browser provides a consolidated historical and real-time view of the events that have occurred in a CS 2000 central office. Event browser is a tool to view the events from the EMSs, NEs, platforms, and applications in a common GUI. The event browser enables the monitoring and debugging of network activities and issues.

A user can access the IEMS event browser by selecting the Network Events node under the Fault Management node of the IEMS Topologies tree.

Viewing event details

Application

Use this procedure to view event details.

The Event Details window provides detailed information about the properties of the event that is selected from the displayed event viewer.

Action

Step	Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.

2 Select the **Network Events** node under the Fault Management node in the IEMS tree.

3 Select a required event (row) of the table in the Network Events panel (or Event Viewer).

4 Double-click any part of the selected event row to view the event property details in the Event Details dialog. Alternatively, the Event Details dialog can be displayed using the **View-->Details** menu command.

An Event Details window opens.

The event details properties and their descriptions are listed in the following table.

Property	Description
LogName	Displays the log name of the event. The log name is either present in the event sent by component or inserted by IEMS.
LogNumber	Displays the log number of the event.
Index	Displays a unique numeric ID generated for each event.
Message	Displays any important additional information of the event.

Property	Description
Category	Displays the category, useful for the categorization of alarms. The alarm category can be one of the following: • communications • qualityOfService • processionError • equipment • environmental • other • others
Source	Displays the object name to which the event is associated.
Date/Time	Displays the time stamp of the event.
SequenceNumber	Displays the sequence number of the event.
EquipmentIdentifier	Displays the managed object display name or IP address that raised the event.
NeType	Displays the type of NE that raised the event.
EventLabel	Displays the label of the event.
OfficeIdentifier	Displays the office identifier of the component that raised the alarm.
LogKey	Displays the log number of the event.
ComponentID	Displays the name of the component that raised the event.
BodyText	Displays the time stamp of the event, component ID, specific cause of the event, and description of the event. The text displayed here varies depending on the device.
Severity	Displays the severity of the event.

Opening many Event Details dialogs and closing the most recently opened Event Details dialog hides all the other Event Details dialogs. You can view other Event Details dialogs by moving the IEMS client main screen or invoking a new Event Details dialog. This issue is experienced with the IEMS client on a Sun Solaris platform.

5 To close the Event Details dialog, select the **Close** button.

6 You have completed this procedure.

—End—

IEMS log details

Each event displayed in the Network Events panel has the index, message, category, source, date or time, log number, log name, and other properties. Traps from SNMP devices and notifications are converted to events by IEMS. IEMS assigns a log number to events depending on the source and nature of event.

The following table lists events that are raised on IEMS. For full details of these logs, see the *Carrier Voice over IP Fault Management Logs Reference Manual*, NN10275-909.

Logs generated from events
BKM300, BKM600
IEMS398, IEMS399, IEMS601, IEMS602, IEMS603, IEMS604, IEMS605, IEMS606, IEMS607, IEMS608, IEMS609, IEMS610, IEMS611, IEMS612, IEMS613, IEMS615, IEMS616
EMSS306, EMSS307, EMSS308, EMSS309, EMSS310, EMSS311, EMSS312, EMSS313, EMSS314, EMSS304, EMSS315, EMSS316, EMSS317, EMSS318, EMSS319, EMSS325, EMSS326, EMSS327, EMSS300, EMSS301, EMSS302, EMSS303, EMSS305, EMSS600, EMSS601, EMSS602, EMSS603, EMSS604, EMSS605, EMSS320, EMSS321, EMSS322, EMSS323, EMSS324
EMJS340, EMJS341, EMJS350, EMJS351, EMJS360, EMJS371, EMJS540, EMJS560, EMJS570, EMJS640, EMJS641, EMJS642, EMJS651, EMJS652, EMJS661, EMJS662, EMJS671, EMJS672, EMJS840, EMJS841
PKM300, PKM301, PKM302, PKM303, PKM304, PKM305, PKM306
QCA201, QCA202, QCA203, QCA300, QCA301, QCA302, QCA305, QCA310, QCA315, QCA322, QCA399

The following table lists logs that are introduced in the (I)SN09U release. For full details of these logs, see the *Carrier Voice over IP Fault Management Logs Reference Manual*, NN10275-909.

New logs for (I)SN09U	Description
IEMS616	Generated when an SNMP protocol authentication failure occurs. It is an INFO event.
PKM300	Generated when an attempt to create and validate an X509 certificate has failed or when X509 certificate creation and validation succeeds after previously having failed

New logs for (I)SN09U	Description
PKM301	Generated when an attempt to deliver an X509 certificate to an application has failed or when delivery of an X509 certificate succeeds after previously having failed. The severity is major.
PKM302	Generated when an X509 certificate used by a device to authenticate itself during call control operations has expired. The device cannot send or receive call control messages. Log report PKM302 is also generated when an X509 certificate for a call control device that was expired has been replaced with a new valid certificate. The severity is critical.
PKM303	Generated when the expiration date of an X509 certificate has reached the forewarning date for the last alarm before expiration. A previous forewarning date has already passed. The alarm raised at that time has been escalated. Log report PKM303 is also generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate reached the last alarm before expiration date. The severity is major.
PKM304	Generated when the expiration date of an X509 certificate has reached the date for the initial expiration warning. The severity is minor. Log report PKM304 is also generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate has raised the initial log. The severity is minor.
PKM305	Generated when an X509 certificate used by a device to authenticate itself for OAM&P functions has expired. The device cannot send or receive OAM&P commands. Log report PKM305 is also generated when an X509 certificate for an OAM&P device that was expired has been replaced with a new valid certificate. The severity is major.

Managing CS 2000 Core and Call Agent Core events in IEMS

IEMS CS 2000 Core management

IEMS offers two options in its Java Web Start GUI client to view logs from a Carrier VoIP CS 2000 office (CS 2000 Core and associated devices):

- an event browser that allows a craftperson to view both a real-time and a historical view of the events (alarm raises, clears, and info events)
- an active alarm browser which provides a real-time view of the active alarms in the network. It is used to depict alarm states for the devices that support the ability to perform alarm raise and alarm clear correlation (state-full alarm events)

The IEMS provides the ability to monitor the associated SDM/CBM SCC2 or NT STD logroute event stream. All events from the CS 2000 Core Manager/SDM are visible in the event browser. To view the CS 2000 Core Manager events, select the Element Managers folder in the IEMS topology tree and right click on the associated CS 2000 Core Manager. Select the **Display Recent Events** menu item from the drop down menu. For further details of how to view events, see "Working with events" in *IEMS Fault Management*, NN10334-911.

The CS 2000 Core and Call Agent Core do not support alarm raise and clear correlation rules in the IEMS. As a result, all events from the CS 2000 Core and Call Agent Core are only visible in the IEMS event browser. They are not displayed in the active alarm browser. The IEMS provides the ability to proxy these events over the IEMS northbound event interfaces (SCC2, NT STD, SNMP and custlog) and maintains historical message formats.

Using CEM to manage CS 2000 Core events

The Core Element Manager (CEM) client and server components are integrated with the IEMS from (I)SN08 onwards. When the CEM is used to manage the CS 2000 Core or Call Agent Core events, it provides the following:

- an alarm correlation engine allowing the correlation of alarm raise and clear events
- the CEM graphical interface, which provides a mechanism to graphically view the alarm states of the sub-components in the CS 2000 core
- the ability to view the CS 2000 Core events in both the IEMS event and active alarm browsers

When the CEM is used to manage the CS 2000 Core events, the IEMS forwards these events over its northbound event interfaces (SCC2, NT STD, SNMP and custlog). Historical message formats are not maintained. The output format of these messages from the CS 2000 core is optimized to reflect the relation between the core alarm raise and clear events.

You can configure either the CS 2000 Core Manager or the CEM manager in the IEMS client to manage the CS 2000 Core or Call Agent Core devices. Due to capacity concerns, only one mode of fault management (CS2000 Core Manager or CEM) should be used in the IEMS at a time.

Searching for missed notifications

This sub-section provides procedures on how to search for missed notifications from EMS/NEs managed by IEMS, as well as how to create an events custom view for missed notifications.

Notifications are messages from device agents or messages forwarded by EMSs in the network. Missed notifications are notifications not generated by the IEMS. The IEMS monitors the sequence numbers in the incoming fault streams from the managed objects. When it detects a gap in the sequence numbers in the incoming stream, it tries to recover the missed events from the managed device (if the device supports a recovery mechanism). If it is unable to recover the event or if the managed device does not support missed event recovery, it generates a missed notification information log.

For example, a device agent is sending notifications to the IEMS. If the nth event sent by the agent has the notification sequence number "2", and the subsequent event sent by the agent has the notification sequence number "4", the IEMS has missed the notification sequence number "3". In this case, the IEMS generates an event with Info severity.

Searching for all missed notifications from EMS/NEs

Application

Use this procedure to search for all missed notifications from EMS/NEs managed by IEMS

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Ensure the Category column appears in the Network Events panel in the IEMS Client. If the Category column is not visible, follow these steps to make the Category column appear: a. Right-click the **Network Events** node to display the popup menu. b. Select the **Custom Views-->Modify Custom View** menu command to launch the Specify Event Filter Criteria dialog for the Network Events panel.

c. Click the **Select Props To View** button to display the Select Table Columns dialog.

d. Check the **category** check box.

e. Click the **OK** button to close the Select Table Columns window.

f. Click the **Apply Filter** button to save the changes and then close the window using the **Close** button.

4 Select the **Edit-->Search** menu command to display the Search dialog.

5 Select the **Match all of the following** option, since two search criteria have to be satisfied.

6 Select the **Severity** value from the first list box in Search Criteria panel.

7 Select the **equals** value from the second list box in Search Criteria panel.

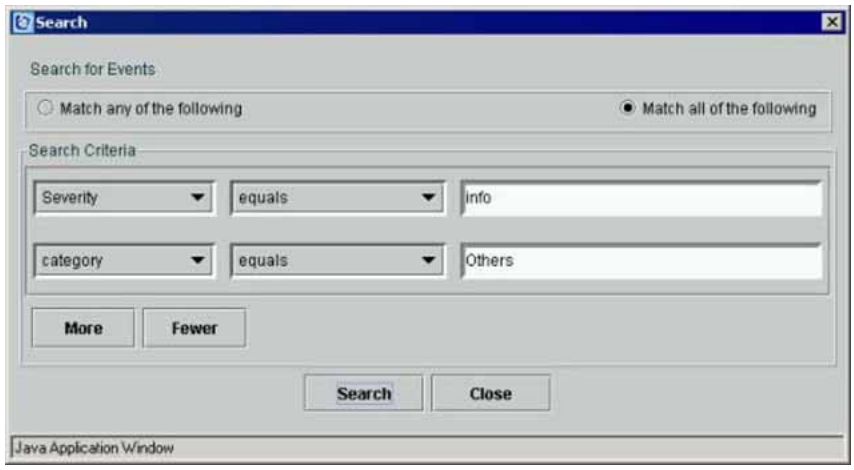
8 Enter the text **`Info`** in the text field present as the third field in Search Criteria panel.

9 Click the **More** button to add another criteria. You can find another row of three fields added in Search Criteria panel.

10 Select the **category** value from the first list box in the second row of panel.

11 Select the **equals** value from the second list box in the second row of Search Criteria panel.

12 Enter the text **`Others`** in the text field (which is the third field in the second row of the Search Criteria panel). Check whether you have specified the criteria in the Search window similar to the following figure.



13 Click the **Search** button to search for the events from unknown devices.

The missed notifications are listed in the Network Events panel.

14 You have completed this procedure.

To monitor the missed notifications, create an events custom view. For details on creating a custom view, refer to "Managing custom views for events" (page 33).

—End—

Creating an Events Custom View for missed notifications

Application

Use this procedure to create the events custom view for missed notifications.

Action

Step	Action
	At the IEMS workstation
1	Follow step 1 to step 3 of the "Searching for all missed notifications from EMS/NEs" (page 15) procedure.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Right-click and select the **Custom Views-->Add Custom View** menu command. *The Specify Event Filter Criteria window is displayed.*

4 Enter the text **`Missed Notifications`** in Filter Value Name field.

5 Select **Props** to view button selection.

6 Click the **Additional table columns** button.

The User defined table columns dialog is launched.

7 Check the Log Name and Log Number text boxes under **Display Name**.

8 Click the **OK** button.

The User defined table columns dialog is closed and returns back to the Select Table Columns window.

9 Click the **OK** button.

The Select Table Columns window is closed and returns to the Specify Filter Criteria window.

10 Click the **Additional Criteria** button.

The criteria dialog is launched.

11 Type the text **logNumber** in the field under the Property Name column since the criteria is based on log number.

12 Type the value **603** in the field under the Match Criteria column since the criteria is based on this log number.

13 Click the **More** button.

A row is added below the existing row.

14 In the second row, type the value **`logName`** in the field under the Property Name column since the criteria is also based on log name.

15 Type the value **`IEMS`** in the field under the Match Criteria column since the criteria is based on this log name.

16 Click the **OK** button.

The Criteria dialog is closed and the Specify Filter Criteria window is displayed.

17 Click the **Apply Filter** button to create the custom view for missed notifications.

18 Click the **Close** button to close the dialog.

19 You have completed this procedure.

—End—

You can modify the search criteria for a custom view after it is created. To do this, right-click on the custom view node (under Fault Management-->Network Events node of IEMS tree) and selecting the **Modify Custom View** option from the Custom Views menu.

You can also remove the custom view by right-clicking the custom view and selecting the **Remove Custom View** option from the Custom Views menu.

Navigating the events database using Java Web Start Client

Application

Use this procedure to navigate the events database and sort the data as required using Java Web Start Client.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree. *The Navigation toolbar is displayed in the top part of the **Network Events** panel.* By default, the pages of the Network Events panel or event viewer panel show the latest events at the top since the list is sorted by the Date column. The ways in which the events database can be navigated are as follows: • **Viewing the range:** The range of rows that are displayed in the table. It is placed above the Network Events panel. You can select the default page length from the Page Length list box. • **Using the Navigator buttons:** The four navigator buttons, first, previous, next, and last, are located at the top of the internal frame. • **Sorting the data:** The data can be sorted based on the column type and the details can be viewed in ascending or descending order. For details, refer to "Understanding sorting of data" in *IEMS Overview*, NN10329-111. • **Reordering the columns:** The columns can be reordered by dragging a column header and moving it to the required place in the table.
3	You have completed this procedure.

—End—

Using other operations in events

This sub-section deals with operations involving events, including saving and printing generated events, and viewing alarms related to the events. The save option is used to save the current range of event data displayed on the page. The print option prints the current range of event data displayed in the page. Alarms that are generated from corresponding events can also be viewed.

Saving events in a file

Application

Use this procedure to save all the events displayed in the Network Events panel.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Select the **Actions-->Save** to File menu command. Selecting the **Save** button in the toolbar or selecting the ***Actions-->Save To File*** menu command saves the current range of data displayed in the Event Viewer in the style of the current custom view. The file is saved in ASCII text format with values in each column separated with a colon (:). ***Example*** *The following text is saved, which is the equivalent of a row in the Network Events panel:* *Critical : 192.168.113.109 : Jul 08,2005 06:06:05 PM : 0 : IEMS398 : FLT* *The event details are saved in a log file under the /opt/nortel/iems/current/logs/eventlogs directory. The format of filename is as follows:* *iems_events.<uid>.<mmm_dd_yyyy_hh:mm:ss>.log* *To conserve disk space on the server, the log file is compressed to an archive (.gz) file. The format of the archive filename is as follows:* *iems_events.<uid>.<mmm_dd_yyyy_hh:mm:ss>.log.gz*

When the event details are saved to the log file and archived, a confirmation dialog box opens with the following message: /var/logs/iems/eventlogs/iems_events.iem-sadm.<mmm_dd_yyyy_hh:mm:ss>.log.gz has been saved.

4 You have completed this procedure.

—End—

Viewing related alarms

Application

Use this procedure to view the related alarms for an event.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Select a required event (row) of the table in the Events Viewer.
4	Select the **View-->Alarms** menu command to display the related alarms of the selected event in the Alarms panel.
5	You have completed this procedure.

—End—

Viewing related topology

Application

Use this procedure to view the related topology for an event.

Action

Step	Action
	At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.

2 Select the **Network Events** node under the Fault Management node in the IEMS tree.

3 Select a required event (row) of the table in the Events Viewer.

4 Select the **View-->Show Map** menu command to display the related topology of the selected event.

5 You have completed this procedure.

—End—

Printing events

Application

Use this procedure to print the events in the Network Events panel.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Select the **Actions-->Print** menu command to print the event data in the current custom view that is displayed on the current page. This print command is sent to the default printer configured for the IEMS server. The IEMS server has to be configured to use the print option. Refer to the "Configuring a printer for the IEMS" in *IEMS Administration and Security*, NN10336-611 for more details.
4	You have completed this procedure.

—End—

Configuring the Message Overload Controller parameters

The IEMS Overload Controller sub-system protects the IEMS server application when it is being sent excessive incoming event rates. Under these conditions it will detect the terminals with the highest incoming message rates and will flag them as message babblers. A message babbler will be temporarily placed in a unmanaged state in an attempt to protect the overall system. As the IEMS plays a prominent role in managing the Carrier VoIP network, it must be protected from devices that exceed acceptable message rates. This sub-section provides the procedure which describes how to configure the parameters for IEMS Overload Controller.

Understanding the fault interface state of managed objects

The IEMS serves as a fault or log integration point for the devices in a Carrier VoIP network. It allows a craftsperson to view both the active alarm states as well as the historical events in the IEMS Client alarm and event GUI browsers. When the cumulative event rate from the managed devices exceeds the supported rate, the IEMS Overload Controller does the following actions.

- Drops the events from the devices not provisioned in the IEMS.

  Example
  SNMP traps and Custlog messages.

- Identifies the managed devices with the highest incoming event rates and changes their fault interface state to "Throttle_Unmanaged state" (page 26) or "System_Unmanaged state" (page 26). The devices stay in this state until the total incoming event rate is reduced below the steady state rate supported by the IEMS.
- After a timeout period, it will evaluate and determine if the incoming message rate has been reduced to a manageable rate. If it has, it will change the state of devices in a "Throttle_Unmanaged state" (page 26) back to the managed state and again begin monitoring the fault interface for these devices.

When the event rate from the managed object can be handled by IEMS, the managed object fault interface state is "Normal".

Throttle_Unmanaged state

When the IEMS system enters overload controls, it will place the devices with the highest incoming event rates in a "Throttle_Unmanaged state". When a managed object fault interface is "Throttle_Unmanaged" state, IEMS does the following:

- Changes the managed object state to "Throttle_Unmanaged". In this state the IEMS drops the incoming events received from these devices.
- Generates alarms to indicate that the devices have entered the "Throttle_Unmanaged" state.
- After the Throttle State Count, if the incoming event rate is within acceptable limits, the devices fault interface state is changed back to "Normal". A clear event is sent for the previously raised "Throttle_Unmanaged" state alarm.

System_Unmanaged state

If the managed object is in the "Throttle_Unmanaged" state for a specified number of times (Throttle State Count), the fault interface state for this device is changed to "System_Unmanaged" state. When a device is placed in this state, it will require a craftsperson to manually change the state back to normal. When a managed object fault interface is "System_Unmanaged" state, IEMS does the following:

- Changes the managed object state to "System_Unmanaged".
- Generates alarms to indicate the "System_Unmanaged" state.

Configuring the parameters

Application

Use this procedure to configure the Message Overload Controller parameters.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.
3	Select the **MessageOverloadControl Setting** node under the Miscellaneous tree. *The Message Overload Controller Configuration GUI opens.*.

4 Check the **Message Overload Controller** check box to enable the IEMS message overload controller. (By default, the Message Overload Controller field is enabled.)

5 Modify the message buffer size in the Message Buffer Size field.

Message Buffer Size
The maximum number of events in the buffer that IEMS can handle.

6 Modify the message monitor count in the Message Monitor Count field.

Message Monitor Count
The number of events to be received by the IEMS before checking the buffer size of the IEMS.

7 Modify the throttle state period in the Throttle State Period field.

Throttle State Period
Time in milliseconds that a managed object fault interface is in the "Throttle_Unmanaged" state. After the Throttle State Period, the IEMS automatically changes the managed object to the "Managed" state.

8 Modify the throttle state count in the Throttle State Count field.

Throttle State Count
It represents the maximum number of times a managed object is changed to the "Throttle_Unmanaged" state. Afterwards the IEMS automatically changes the managed object fault interface state to the "Unmanaged" state.

9 Click the **Apply** button to save the changes.

ATTENTION
You must click the **Apply** button after adding the host configuration details to the list. Otherwise, added host configuration details are not saved.

10 You have completed this procedure.

—End—

Searching for events

Application

Use this procedure to search for events.

The search events function enables the user to search for related events from the event database. The search operation is performed on the entire database and is not restricted to the displayed event viewer alone. The search feature allows for specific or general condition searches.

Action

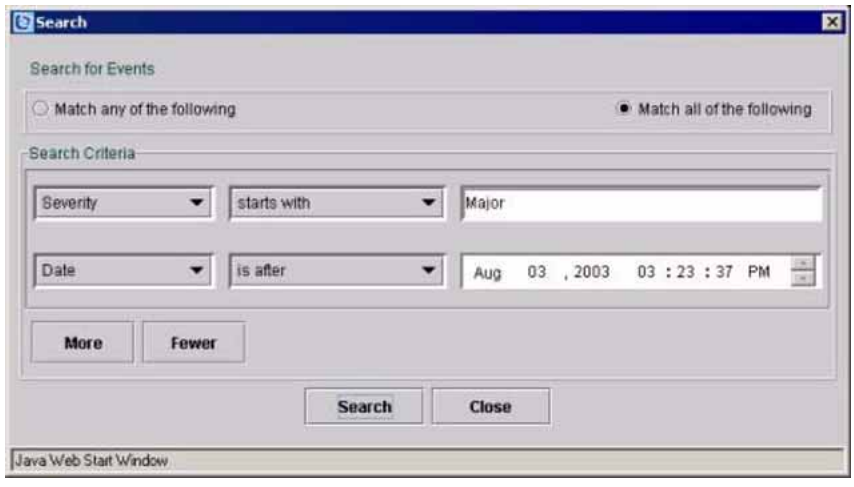
Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Launch the search dialog using the **Edit-->Search** menu command or using the find button in the toolbar.
4	Select the **Match any of the following** or **Match all of the following** radio button to specify whether all or any of the search criteria must be satisfied.
5	Specify the one or more search criteria. More search criteria can be added using the **More** button, and last search criteria in the window can be removed using the **Fewer** button. The first option in the search window is a list box listing the existing column headers in the Events table of the Events panel. The second option has two different sets of criteria to search with: • Normal set of criteria, which consists of

- starts with
- doesn't start with
- ends with
- doesn't end with
- contains
- doesn't contain
- equals
- not equals

- Date / Time criteria, which consists of
  - is before
  - is after
  - equals
  - not equals

The third option is a data field or the Date/Time component for entering the specific search data. The Date/Time component by default shows the current date and time but requires the month, date, year, hour, minute, second, and am/pm indicators which can be selected using the up and down arrows.

The following figure shows the Search dialog and some of the available options to search for a specific event.



6 You have completed this procedure.

—End—

Searching for events raised by an unknown device

Application

Use this procedure to search for events from raised by unknown devices.

The events from an object (that is present in the IEMS database) are received by the IEMS Client and displayed in the Events panel with the severity, source, date, and other properties. The events received from devices that are not part of IEMS database are known as "unknown devices". The events from these devices are received and displayed in the Events panel. The events from unknown devices have the source field value "Unknown Device". This procedure describes how to search for events from an unknown device.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Select the **Edit-->Search** menu command to launch the Search dialog.
4	Select "Log Number" from the first drop-down list in the Search Criteria panel.
5	Select "equals" from the second drop-down list in the Search Criteria panel.
6	Enter the text "601" in the text field.
7	Click the **Search** button to search for events from unknown devices. To monitor the events from unknown devices, create an events custom view. For details on creating a custom view, refer to "Managing custom views for events" (page 33) section.
8	You have completed this procedure.

—End—

Managing custom views for events

Application

A custom view is an option to view a subset of data that satisfies a given criteria from a large collection. The update of data is dynamic.

Use this procedure to do the following:

- View an event based on specific criteria.
- Customize the Properties to view column.
- Change the column order, sort the data, and save these states.
- Modify or rename the custom view. You can use the same custom view name at different levels.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Select the required action from the following table.

Tool button in toolbar	Menu bar option	Shortcut	Description
	Custom Views--> Add Custom View	Ctrl+N	This option adds a new custom view with the given criteria. When this command is chosen by the user, a custom view property sheet is displayed on the screen. For details on using search criteria, refer to "Setting the search criteria for a

Tool button in toolbar	Menu bar option	Shortcut	Description
			custom view of events" (page 35). The fields in the Tree Node Properties tab can also be used for configuring a custom view. After the form is completed and submitted, the new custom view is created and can be seen in the tree on the left.
	Custom Views--> Remove Custom View	Ctrl+D	Removes a custom view. The parent custom view (Network Events) cannot be removed. If a custom view has one or many custom child views, both the parent and child views are removed. The main parent custom view (Network Events) cannot be removed. Selecting the Remove Custom View option asks for a confirmation to remove the custom view.
	Custom Views--> Modify Custom View	Ctrl+M	Modifies any custom view.
	Custom Views--> Save Custom View	Ctrl+S	Saves the current state of the custom view, such as column order, sort order, and others.
	Custom Views--> Rename Custom View	Alt+F2	This option renames the current custom view. To cancel the rename, press the Esc key before completing.

4 You have completed this procedure.

—End—

Setting the search criteria for a custom view of events

Application

Use this procedure to set the search criteria for a custom view of events. The search criteria is specified in the Specify Event Filter Criteria window and the Tree Node Properties window.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Select the **Custom Views-->Add Custom View** menu command. *The Specify Event Filter Criteria window is displayed.*
4	Fill in the fields as required. The following table lists the fields and explains how to complete the form.

Description of properties in the Specify Event Filter Criteria window

Property	Description
Filter View Name	Specifies the name of the custom view being created.
Parent Name	Determines the node in the IEMS tree under which this custom view is to be added. The default value is "Network Events". This field can be modified by selecting the node under which the new custom view is added.
Severity	Determines the severity of the event to be included in the view. Multiple severities can be assigned by typing the severities separated with commas.
Message	Specifies all or part of a message associated with the events to be displayed. **Example** Unable to communicate with managed device

Property	Description
Category	Specifies the category of the events, and includes: • communications • qualityOfService • processingError • equipment • environmental • other • others
Domain	Not currently used by IEMS.
Network	Not currently used by IEMS.
Node	Specifies any additional information about the source of the event.
Failed Object	Specifies the information about the specific entity that is primarily responsible for the occurrence of this event.
Source	Specifies the information about the source of the event.
From Date/Time	Specifies the beginning of the date or time range to be displayed in the custom view.
To Date/Time	Specifies the end of the date or time range to be displayed in the custom view.
Event Age	Specifies the criteria to be used to filter events based on the age of the event. The age can be in minutes, hours, days, today, yesterday, or all these criteria together.

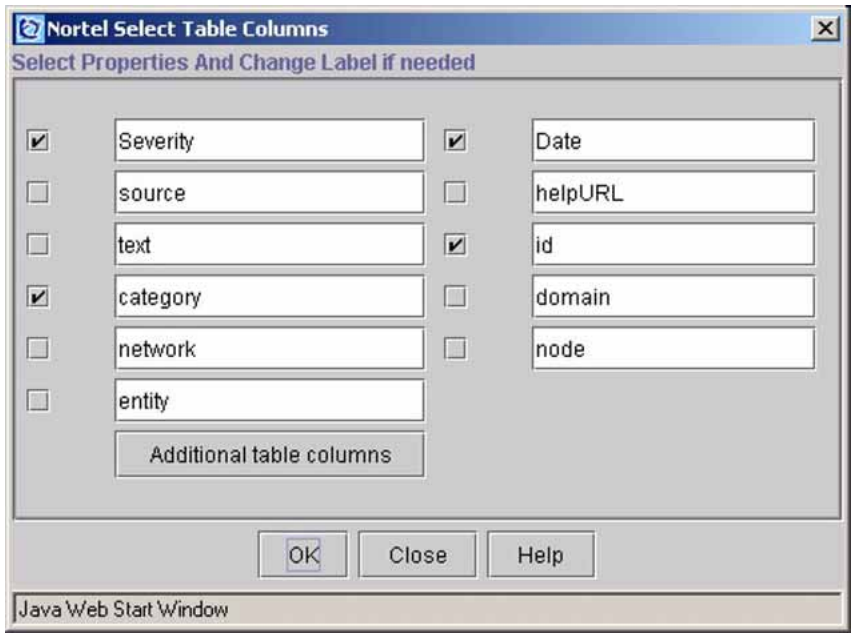
ATTENTION

If all the above parameters (except for filter view name) are left blank, the default value "all" is assigned. Date/Time properties by default show the current date and time, but the month, date, year, hour, minute, second, and am/pm indicators are required. This is chosen using the up and down arrow keys.

The age of an event denotes the time lapsed since the last modification of the event in the IEMS Server.

5 Specify other properties by selecting the **Select Props to View** button.

The following dialog is displayed



6 Select the check box against the column names that you want to display in the Network Events table.

7 Click the Additional table columns button to invoke the User defined table columns dialog.

8 Select the check box against the column names or click the **More** button to specify any other column not displayed in the window. The other column names which can be specified in the User defined table columns dialog must be as Property Name column of the following table.

Property names for the user defined table columns dialog

Display name (can be modified)	Property name
Log key	logKey
Event type	eventType
Equipment identifier	equipmentIdentifier
Device sequence number	sequenceNumber

9 Click the **Additional criteria** button in the custom view properties form to specify additional criteria for viewing the filtered data.

The Criteria dialog is displayed.

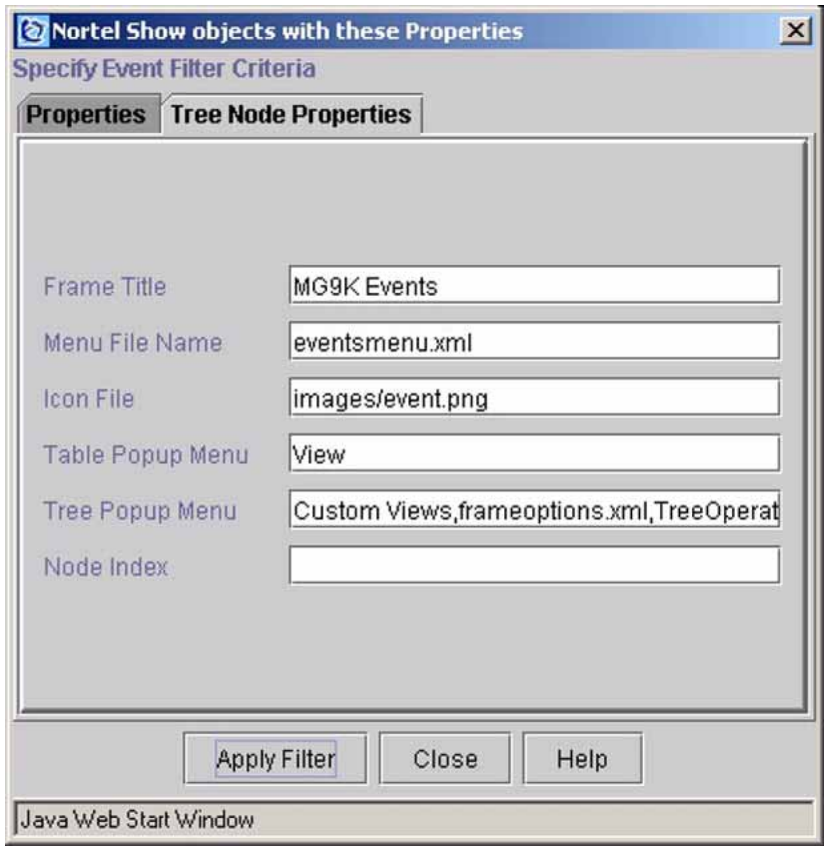
10 Fill the property fields according to the following table.

Property names for the Additional Criteria dialog

Property	Property name
Severity	severity
Owner	owner
Entity	entity
Message	message
Source	source
Date or time	modTime
Category	category
Group name	groupName
Previous severity	previousSeverity
Create time	createTime
Probable cause	probableCause
Event label	eventLabel
Log name	logName
Probable cause	probableCause
Specific problem	specificProblem

11 Select the **Tree Node Properties** tab in the Specify Event Filter Criteria window. (The tree node properties determines the way the subset of data is presented.)

The following dialog is displayed.



The description of each field in the Tree Node Properties tab is given in the following table.

12 Fill the property fields according to the following table.

Properties in the Tree Node Properties tab of the Specify Event Filter Criteria window

Property	Description
Frame Title	Specifies the name to be displayed on the title bar of the custom view's internal frame.
Menu File Name	Specifies the panel-specific menu file name for the **Network Events** panel. Do not modify this field.
Icon File	Indicates which icon to use for the custom view. This icon is visible in the tree as well as in the title bar of the internal frame. The image must be in PNG format. The icon file must be present under the /opt/nortel/iems/current/ directory (or any sub directory).
Table Popup Menu	Specifies the file name of the menu used to display a contextual menu for the objects displayed in the table of the **Network Events** table. Do not modify this field.

Property	Description
Tree Popup Menu	Specifies the file name of the menu used to display a contextual menu for the **Network Events** node in the IEMS tree. Do not modify this field.
Node Index	Specifies the position of the custom view in relation to previously added views. If this field is left blank, the view is appended to the end of the current list of custom views. The values must be less than the number of custom views under the selected parent node in the parent node. **Example** For example, if you want to add the new custom view after the first custom view in the list, enter 1 in the Node Index field.

13 You have completed this procedure.

—End—

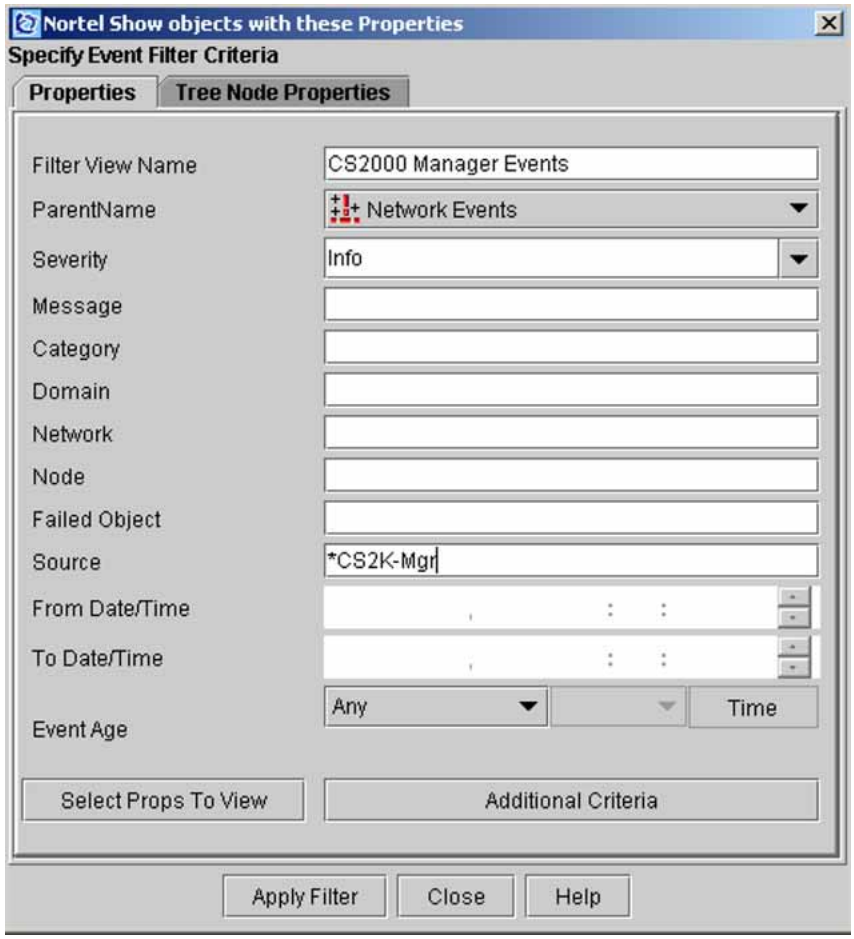
Example for creating a custom view for events

Application

Use this procedure to create a custom view for events (using the CS2000 Core Manager as a sample).

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Network Events** node under the Fault Management node in the IEMS tree.
3	Right-click and select the **Custom Views-->Add Custom View** menu command. *The Specify Event Filter Criteria window is displayed.*
4	Enter the text "CS2000 Manager Events" in the Filter View Name field.
5	Enter the text "*CS2K-Mgr" in the Source field as shown in the following figure.



6 Click the **Select Props To View** button to launch the Select Table Columns window.

7 Ensure the following text boxes are selected:

- severity
- date
- network
- node

8 Click the **OK** button to apply the changes and close the Select Table Columns window.

9 Click the **Apply Filter** button to create a custom view for events from CS 2000 devices.

10 Click the **Close** button to close the dialog.

11 You have completed this procedure.

—End—

Configuring northbound fault feeds

The IEMS standardizes the fault interfaces from the EMSs, NEs, applications, and platforms that it manages. It receives events from these interfaces and converts them into a common format. The IEMS supports the following northbound event interfaces:

- SCC2
- SNMP
- Customerlog SYSLOG
- NTSTD

Providing a common set of northbound OSS interfaces that are based on common standards simplifies the effort for third-party vendors to integrate and monitor the event stream from a Nortel office.

This section describes the configuration of the northbound fault feeds and fault filter.

Configuring SCC2 northbound fault feeds

The IEMS aggregates the event streams received from the EMSs, NEs, applications, and platforms that it manages. It normalizes the events received from these streams and forwards the events over its northbound interfaces such as SCC2, SNMP, SYSLOG, and NTSTD. Clients who wish to monitor the IEMS SCC2 event stream must have their host address configured through the SCC2 host configuration interface. The procedures in this sub-section describe how to configure the northbound SCC2 interface. The SCC2 northbound fault feed contains logs for all events (fault and regular information).

Configuring the SCC2 fault feed hosts

Application

Use this procedure to configure the SCC2 northbound fault feed.

Action

To configure the SCC2 northbound fault feed, follow these steps:

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.
3	Select the **SCC2** node under OSS Config node. *The SCC2 Host Configuration GUI is displayed.*
4	Enter the IP address of the host (to which the northbound fault feeds need to be forwarded) in the IP address field.
5	Click the **Add** button to add the IP address to the list of northbound host.
6	Click the **Apply** button to save the settings. Click the **Apply** button after adding the IP address to the list. Otherwise, the added IP address is not saved.
7	Close the dialog using the **Exit tool** button to return to the IEMS Client.
8	You have completed this procedure.

—End—

Removing a SCC2 fault feed host

Application

Use this procedure to remove the SCC2 fault feed host.

Action

Step	Action
	At the IEMS workstation
1	Select the required SCC2 fault feed host in the SCC2 Host Configuration window.
2	Click the **Delete** button to remove the IP address.
3	Click the **Apply** button to save the settings.
4	You have completed this procedure.

—End—

Viewing the SCC2 logs

Application

Use this procedure to view the SCC2 logs in the IEMS Server running on host named succession-sol1 (for example)

The SCC2 logs can be viewed within the IEMS Server. Before viewing the SCC2 logs, the host IP address from the machine trying to view the logs must be added in the SCC2 Configuration GUI as specified in the "Configuring the SCC2 fault feed hosts" (page 46).

Action

To view the SCC2 logs in the IEMS Server running on host named succession-sol1 (for example), follow these steps:

Step	Action
	At the IEMS workstation
1	Connect to the host on which IEMS server is running using telnet.
2	Enter the following command in the command prompt:

```
telnet succession-sol1 8556
```

The succession-sol1 specified in this command is the virtual host name.

3 You have completed this procedure.

—End—

Configuring SNMP northbound fault feeds

Clients who wish to monitor the IEMS SNMP trap event stream must have their host address configured through the SNMP northbound OSS configuration interface. This procedures in this sub-section describe how to configure the northbound SNMP interface.

Adding an SNMP fault feed host

Application

Use this procedure to add SNMP northbound fault feeds.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.
3	Select the **SNMP** node under OSS Config tree. *The SNMP Configuration GUI is displayed.* By default, the following attribute values are used for configuring SNMP northbound fault feed. The administrator can change the above attribute values. Refer to "Changing attributes for SNMP fault feeds" in *IEMS Administration and Security*, NN10336-611 to modify these values. • SNMP port: 8001 • read community: public • write community: public • SNMP version: v2c
4	Enter the manager host IP address (to which the northbound fault feeds need to be forwarded) in the Manager Host field.
5	Enter the port (in which the SNMP fault feeds are sent) in the Manager Port field.
6	Enter the manager community in the Manager Community field.

7 Click the **Add** button to add the manager host and port to the northbound host table.

8 Click the **Apply** button to save the settings.

Click the **Apply** button after adding the host configuration details to the list. Otherwise, the added host configuration details are not saved.

9 Click the **exit tool** button to close the dialog.

10 You have completed this procedure.

—End—

Removing SNMP fault feed hosts

Application

Use this procedure to remove an SNMP fault feed host

Action

Step	Action
	At the SNMP Configuration window
1	Select the required SNMP fault feed host details from the table in the SNMP Host Configuration window.
2	Click the **Remove** button to remove the required SNMP Fault Feed host details.
3	Click the **Apply** button to save the settings.
4	You have completed this procedure.

—End—

Modifying SNMP fault feed hosts

Application

Use this procedure to modify existing SNMP fault feed host details in the list.

Action

Step	Action
	At the SNMP Configuration window

1 Select the required manager host details row in the northbound host table.

2 Modify the manager host IP address (to which the northbound fault feeds need to be forwarded) in the Manager Host field.

3 Modify the port (in which the SNMP fault feeds are sent) in the Manager Port field.

4 Modify the manager community in the Manager Community field.

5 Click the **Modify** button to modify the host details in northbound host table.

6 You have completed this procedure.

—End—

Configuring and viewing SYSLOG customerlogs

Application

Use this procedure to route a syslog to a remote host, turn off syslog re-direction, or view a customerlog syslog configuration entry using the SPFS CLI tool. The syslog fault feeds contain three types of logs.

- Customerlog
- Audit log
- Security log

The customerlogs are stored in the /var/log directory of the system on which the IEMS server is running. The log is written to file "iemsCustomerlog", moved and rotated through the same file name with an extension name ranging from ".0" to ".7" as these log files grow and are recycled after 7 days based on the option set using the CLI tool. The current log is always written to the "iemsCustomerlog" file.

The local7.notice syslog facility is reserved to handle the consolidated IEMS customerlog event stream.

Prerequisites

To perform this procedure:

- you must have administration privileges.
- the remote Syslog client must be in service.

Action

Step	Action
	At your workstation
1	Telnet to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the server where IEMS resides
2	When prompted, enter your user ID and password.
3	Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Enter the following at the command prompt.

```
#cli
```

A response similar to the following is displayed:

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Select your next step.

If you want to	Do
route a syslog to a remote host client	go to the next step.
turn off syslog re-direction to a remote host	go to the next step.
view a customerlog	go to step 17

7 Enter the number next to the "Configuration" option.

A response similar to the following is displayed:

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Succession Element Configuration
14 - chg_tz (Change Timezone)
15 - login_session_timeout (Login Session Timeout
Configuration)
16 - snmp_poller (SNMP Poller Configuration)
X - exit
select -
```

8 Enter the number next to the "Syslog Configuration" option.

A response similar to the following is displayed:

```
Syslog Configuration
  1 - list_syslog (List a system's syslog
configuration)
  2 - add_syslog (Add a syslog configuration entry)
  3 - del_syslog (Remove a syslog configuration entry)
  4 - route_syslog_on (Route syslog to remote host)
  5 - route_syslog_off (Turn off syslog re-direction
to a remote host)
  X - exit
 select -
```

9 Select your next step.

If you want to	Do
route a syslog to a remote host client	go to the next step.
turn off syslog re-direction to a remote host	go to step 13.

10 Enter the number next to the "route_syslog_on" option.

A response similar to the following is displayed:

```
=== Executing "route_syslog_on"
Available facilities are:
local1.notice
local7.notice
Please enter the facility to be routed:  local7.notice
Facility:  local7.notice
Enter IP address to route logs to:
```

11 Enter the IP address to which the syslog logs are to be routed.

A response similar to the following is displayed:

```
Enter IP address to route logs to:191.142.106.26
191.142.106.26 is alive
=== "route_syslog_on" completed successfully
```

ATTENTION

Do not specify the IP address in the client GUI or the command prompt UI, with an octet which is prefixed with a zero. An IP address whose octet ranges from 0 to 255, when prefixed with zero, such as 010, is interpreted as an octal number and is passed as an "8", which results in incorrect addressing.

ATTENTION

The IP address to which the syslog is routed cannot be redirected to the IEMS server because the first entry for the local7.notice syslog facility already directs the IEMS syslogs to the file /var/log/iemsCustomerlog.

12 Go to step 19.

13 Enter the number next to the "route_syslog_off" option.

A response similar to the following is displayed:

```
=== Executing "route_syslog_off"
Available facilities are:
local1.notice
local7.notice
Please enter the facility to be routed:  local7.notice
Facility:  local7.notice
Enter IP address:
```

14 Enter the remote host IP address.

A response similar to the following is displayed:

```
Enter IP address:191.142.106.26
191.142.106.26 is alive
=== "route_syslog_on" completed successfully
```

15 Enter "X" and press the Enter key to exit the CLI.

16 Go to step 19.

17 Change directory to /var/log by entering:

```
# cd /var/log
```

18 Type the following command (for example) and press the Enter key to view the customer logs in real time. Note that you have to press Ctrl+c to cancel this command.

```
# tail -f iemsCustomerlog
```

19 You have completed this procedure.

—End—

Configuring NTSTD northbound fault feeds

The IEMS aggregates the event streams received from the EMSs, NEs, applications, and platforms that it manages. It normalizes the events received from these streams and forwards the events over its northbound interfaces (such as SCC2, NTSTD, SNMP, and SYSLOG). Clients who wish to monitor the IEMS NTSTD event stream must have their host IP address configured through the NTSTD host configuration interface. This sub-section provides procedures on how to configure the NTSTD host. NTSTD northbound fault feed contains logs for all events, that is, fault and regular information.

Adding NTSTD fault feed hosts

Application

Use this procedure to add the NTSTD northbound fault feed.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.
3	Select the **NTSTD** node under the OSS Config tree. *The NTSTD Host Configuration GUI is displayed in the right-side frame.*
4	Enter the IP address of the host (to which the northbound fault feeds need to be forwarded) in the Manager Host field.
5	Enter the office identifier of the host in the Office Identifier field.
6	Click the **Add** button to add the details to the list of northbound host.
7	Click the **Apply** button to save the settings. You must select **Apply** after adding the host configuration details to the list. Otherwise, the added host configuration details are not saved.
8	Click the **exit tool** button to close the window.
9	You have completed this procedure.

—End—

Modifying NTSTD fault feed hosts

Application

Use this procedure to modify the existing NTSTD host in the NTSTD Host Configuration.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.
3	Select the **NTSTD** node under OSS Config tree. *The NTSTD Host Configuration GUI is displayed in the right-side frame.*
4	Select the row from the table for which you want to modify.
5	Modify the IP address of the host in the Manager Host field.
6	Modify the office identifier of the host in the Office Identifier field.
7	Click the **Modify** button to add the details to the list of northbound host.
8	Click the **Apply** button to save the settings. You must select **Apply** after adding the host configuration details to the list. Otherwise, the added host configuration details are not saved.
9	Click the **exit tool** button to close the window.
10	You have completed this procedure.

—End—

Removing NTSTD fault feed hosts

Application

Use this procedure to remove the NTSTD Fault Feed Host.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the required row with NTSTD fault feed host from the table.
3	Click the **Remove** button to remove the IP address.
4	Click the **Apply** button to save the settings.
5	You have completed this procedure.

—End—

Viewing the NTSTD logs

Application

Use this procedure to view the NTSTD logs in the IEMS Server running in host named succession-sol1 (for example).

The NTSTD logs in the IEMS Server are viewed with telnet session (with port 8555) to the host in which IEMS Server is running. Before viewing the NTSTD logs, the host IP address from which you are trying to view the logs must be added to the NTSTD Configuration GUI as specified in the "Adding NTSTD fault feed hosts" (page 56).

Action

Step	Action
	At the IEMS workstation
1	Connect to the host on which IEMS server is running using telnet.
2	Enter the following command in the command prompt: `telnet succession-sol1 8555`
3	You have completed this procedure.

—End—

Configuring the northbound fault filter

IEMS normalizes the events received from streams and forwards the events over its northbound interfaces (such as NTSTD, SNMP, SCC2, and Customerlog). The events to each northbound interface can be filtered based on the given criteria. This sub-section provides procedures to add, modify and remove the northbound fault filter.

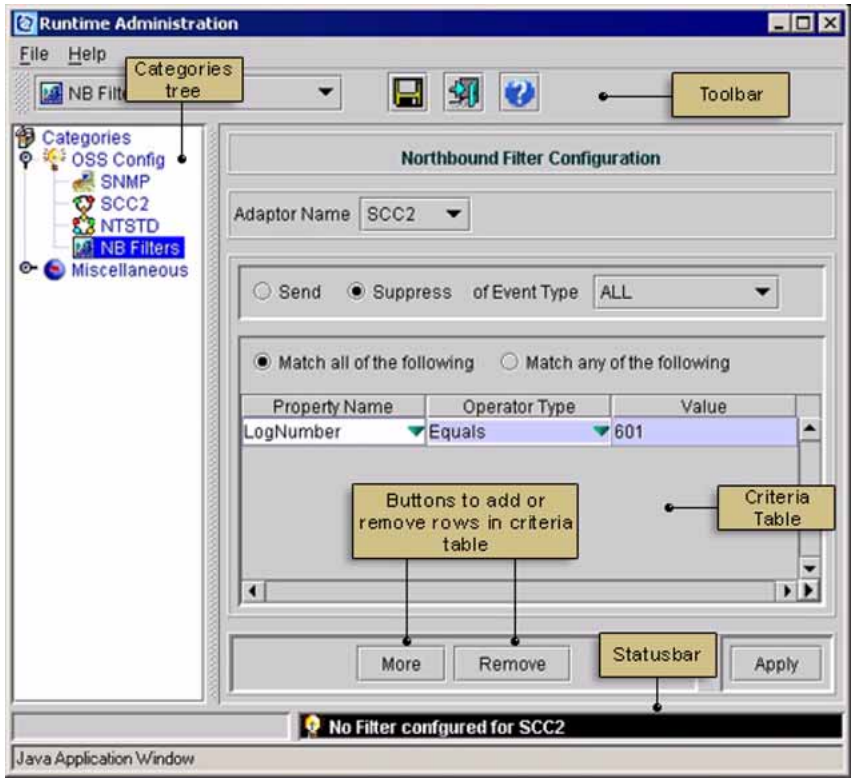
Launching the Northbound Filter Configuration GUI

Application

Use this procedure to launch the Northbound Filter Configuration GUI.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Launch the Runtime Administration window using the **Tools-->Runtime Administration** menu command.
3	Select the **NB Filters** node under the OSS Config tree. *The Northbound Filter Configuration GUI is displayed in the right-side frame as in the following figure.*



4 Close the dialog using the **close tool** button to return to IEMS Client.

5 You have completed this procedure.

—End—

Adding a northbound fault filter

Application

Use this procedure to add the criteria for the Northbound Fault Filter.

This procedure can be repeated for each of the northbound event stream types such as SCC2, NTSTD, SNMP, and Custlog. All the clients connecting or monitoring the IEMS northbound events over a particular event stream (for example, SCC2) share the common event stream type filter type definitions.

Action

Step	Action
	In the Northbound Filter Configuration GUI

1 Select the adaptor name from the Adaptor Name list box for which the Northbound filter has to be configured.

2 Select the **Send** option to send the events to northbound based on criteria in the Criteria table.

OR

Select the **Suppress** option to suppress the events being sent to northbound based on criteria in the Criteria table.

3 Select the type of event from the Event Type list box, which needs to satisfy the criteria in the Criteria table. The description of options in the Event Type list box are listed in the following table.

Description of options in the Event Type list box

Event type	Description
ALL	All the events are sent to northbound based on the criteria given in the Criteria table.
ALARMABLE	The events that are propagated to alarms sent to the northbound stream based on the criteria given in the Criteria table.
NON ALARMABLE	The events that are not propagated to alarms sent to the northbound stream based on the criteria given in the Criteria table.

4 Select the **Match all of the following** option to specify that all the criterion given in the Criteria table must match.

OR

Select the **Match any of the following** option to specify that any one of the criterion given in the Criteria table must match.

5 Click the **More** button to add a row to the Criteria table.

6 Select the property name from the list box in the row of the PropertyName column. For a description of properties, refer to the following table.

Description of event properties

Property name	Description
LogName	The log name of the event is either present in the event sent by the component or inserted by IEMS.
LogNumber	The log number of the event.
EquipmentIdentifier	The component name or IP address that raised the event.
NEType	The type of object such as Element Manager, platform, EMS, or NE.

7 Select the operator type from the list box in the row of the OperatorType column.

8 Enter the value which the criterion must satisfy in the field under the Value column and press the Enter key.

9 Repeat step 5 to step 8 to add more rows to the Criteria table.

10 Click the **Apply** button to save the details.

If you do not click **Apply** after adding or updating criteria in the Northbound Configuration GUI, the details are not saved.

If you select any other node in the Runtime Administration window before clicking the **Apply** button, a dialog opens with the message "You have made some changes. Would you like to apply the changes to the Server". Click the **Yes** button to save the changes.

11 You have completed this procedure.

—End—

Modifying a northbound fault filter

Application

Use this procedure to modify the existing Northbound Fault Filter criteria.

This procedure can be repeated for each of the northbound event stream types such as SCC2, NTSTD, SNMP, and Custlog. All the clients connecting or monitoring the IEMS northbound events over a particular event stream (e.g., SCC2) share the common event stream type filter type definitions.

Action

Step	Action
	In the Northbound Filter Configuration GUI
1	Select the adaptor name from the Adaptor Name list box for which the Northbound filter has to be configured.
2	Select the **Send** option to send the events to northbound based on criteria in the Criteria table. OR Select the **Suppress** option to suppress the events being sent to northbound based on criteria in the Criteria table.

3 Select the type of events from the Event Type list box, which needs to satisfy the criteria in the Criteria table. For description of options in the Event Type list box, refer to "Description of options in the Event Type list box" (page 61) table.

4 Select the **Match all of the following** option to specify that all the criterion given in the Criteria table must match.

OR

Select the **Match any of the following** option to specify that any one of the criterion given in the Criteria table must match.

5 In the existing rows in the Criteria table, modify the property name from the list box in the row of the PropertyName column. For description of properties, refer to "Description of event properties" (page 61) table.

6 Modify the operator type from the list box in the row of the OperatorType column.

7 Modify the value which the criterion must satisfy in the field under the Value column and press the Enter key.

8 Click the **Apply** button to save the details.

If you do not click **Apply** after adding or updating criteria in the Northbound Configuration GUI, the details are not saved.

If you select any other node in the Runtime Administration window before clicking the **Apply** button, a dialog opens with the message "You have made some changes. Would you like to apply the changes to the Server". Click the **Yes** button to save the changes.

9 You have completed this procedure.

—End—

Removing a northbound fault filter

Application

Use this procedure to remove the existing Northbound Fault Filter criteria.

This procedure can be repeated for each of the northbound event stream types such as SCC2, NTSTD, SNMP, and Custlog. All the clients connecting or monitoring the IEMS northbound events over a particular event stream (e.g., SCC2) share the common event stream type filter type definitions.

Action

Step	Action
	In the Northbound Filter Configuration GUI
1	Select the adaptor name from the Adaptor Name list box for which the Northbound filter has to be configured.
2	Select the required row which must be removed.
3	Click the **Remove** button. *The selected row is removed from Criteria table.*
4	Click the **Apply** button to save the details. If you do not click the **Apply** button after adding or updating criteria in the Northbound Configuration GUI, the details are not saved. If you select any other node in the Runtime Administration window before clicking the **Apply** button, a dialog opens with the message "You have made some changes. Would you like to apply the changes to the Server". Click the **Yes** button to save the changes.
	—End—

Working with alarms

The IEMS alarm browser provides a consolidated real-time view of the events that have occurred in a CS 2000 central office. It provides a tool to view and page through the alarms from the EMs, NEs, platforms, and applications in a common graphical interface. Alarms are generated when a fault is detected in a network device. The devices forward these alarms to the IEMS. The alarms have one of the following severities:

- Critical
- Major
- Minor
- Warning

The significance of the background color of the rows in the Alarms panel for each severity level is listed in the following table.

Color	Severity level
	Critical
	Major
	Minor
	Warning

The Alarms browser provides a wide range of features to manage and view alarms in a centralized location. To access the Alarms browser, select the Alarms panel (under the Fault Management node) in the IEMS tree.

This section includes the following sub-sections:

- "Navigating the alarms database using Web Client" (page 115): The IEMS Alarm browser provides user interfaces to navigate through the active alarm list. This sub-section describes these user interfaces.
- "Searching for alarms" (page 81): This sub-section describes how to search for an alarm or set of alarms from the IEMS alarm database.
- "Creating a custom view for alarms" (page 85): This sub-section describes the details of creating and modifying a custom alarm view.
- "Viewing alarm details" (page 67): This sub-section describes the IEMS Alarm Details graphical interface.
- "Saving, printing, deleting, and viewing alarms" (page 83): This sub-section describes the saving an alarm, printing alarms, and viewing events related to alarms.
- "Viewing the Alarm Count panel" (page 78): The Alarm Count Panel shows the number of alarms, severity, and their associated categories. This sub-section provides details for the Alarm Count Panel.

  All the events from the CS 2000 Core Manager are added as stateless events in IEMS. These events are not correlated to alarms.

Viewing alarm details

Application

Use this procedure to view alarm details.

You can view the full details of any alarm by double-clicking on the alarm in the Alarms panel. Alternatively, you can select an alarm from the Alarm Viewer, then select the Details option in the View menu. On selecting an alarm in the Alarms table, the corresponding row turns to a gray color. The Alarm details window shows the other failures in the same group, the history of the failure, and user notes.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Alarms** panel under the Fault Management node in the IEMS tree.
3	Double-click the required alarm for details required. *The Alarm details window opens.* The following table describes the properties displayed in the Alarm details window.

Property	Description
Message	Important additional information about the alarm.
Failure object	The specific entity that caused the alarm (in the source specified by the Source field of the alarm).
Source	The object name with which this alarm is related.
Owner	The name of the user who has acknowledged the corresponding alarm is displayed in this field. If it is not acknowledged by any of the users, this field is blank

Property	Description
Category	The category of the alarm. The alarm category can be one of the following: • communications • qualityOfService • processionError • equipment • environmental • other
Created	The date and time when the alarm was first created.
Modified	The date and time when the alarm was last modified.
Group	The alarm group.
Severity	The severity of the alarm.
Other alarms in this group	Lists other alarms in this group.
Annotations for this alarm	Displays any notes for this alarm.
Acknowledge or Unacknowledge	You can acknowledge or unacknowledge the alarm by clicking the **Acknowledge** or **Unacknowledge** button. Acknowledging an alarm helps to allocate an alarm to a work group or a user. The system records an alarm annotation entry against the name of the user who unacknowledged it.
Annotate	Click the **Annotate** button to add notes to the alarm.
Refresh	The details of the alarms can be refreshed using the **Refresh** button.
Properties	Click the **Properties** button to open a window containing the user properties specified for the alarm. This window is non-editable and is for information purposes only.
View history	The **View history** button is reserved for future use.
Merge	Click the **Merge** button to view the alarm annotations and alarm history simultaneously.

4 You have completed this procedure.

—End—

Alarm clearing in the IEMS

The alarm state of the alarms that are logged in the IEMS are owned by the devices that raised them. The alarms can be cleared in IEMS in one of the following ways.

- The device sends an alarm clear event to the IEMS for an alarm that it previously raised.
- A manual clear is performed by a craftperson in the IEMS alarm browser on an outstanding alarm.
- A manual deletion is performed by a craftperson in the IEMS alarm browser on an outstanding alarm.
- The IEMS alarms clearing job is run automatically.
- IEMS alarm resynchronization
- An IEMS NB agent clear is requested.
- A craftperson executes the /opt/nortel/iems/current/bin/purgeTempData.sh script.

The following sub-sections provide a detailed description of these alarm clearing mechanisms.

The device sends a clear for the associated alarm

The majority of devices managed by the IEMS do support a stateful alarm model. This implies that they do support the ability to send an explicit alarm clear event to clear an alarm that they had previously raised.

IEMS manual alarm clearing in IEMS

The IEMS supports the ability to perform a manual clear on alarms in its JWS active alarm browser. This capability is only supported on alarms from devices that do not support the ability for the IEMS to re-synchronize with the devices active alarm states. The devices that support this manual clear functionality in the IEMS are:

- SAM21 manager
- QCA
- NPM
- ERS 8600

Note that the ability to perform this manual clear on an alarm is controlled by the 'alarmClear' attribute in the IEMS alarm browser. The value of this attribute can be displayed by including the 'alarmClear' attribute in a custom alarm view (refer to select properties to view when creating a custom alarm

view). If the value of the alarmClear attribute is set to anything other than 1 or 2 a manual clear can be performed on the associated alarm. In addition, note that performing a manual clear on an alarm in the IEMS browser clears the alarm instance from the IEMS alarm view but it does not modify the alarm state in the device that raised the original alarm.

When a craftperson performs a manual clear, the IEMS generates an IEMS 605 event which is forwarded to configured northbound OSS systems to notify them that a manual clear occurred. For a description of the IEMS 605 event, refer to *Carrier Voice over IP Fault Management Logs Reference manual*, NN10275-909.

To manually clear alarms, see the procedure for "Clearing alarms raised by managed objects" (page 74).

Manual deletion in IEMS

In addition to supporting the ability to perform a manual clear on an alarm in the IEMS alarm browser the IEMS also supports the ability to perform a manual delete. While both a manual clear and delete are similar in their end result they do have some subtle differences. These include:

- A manual delete can be performed on any alarm in the IEMS alarm browser.
- A manual delete does not generate an IEMS 605 event.
- Compared to the manual clear, the delete removes the instance from the IEMS alarm view but it does not modify the alarm state in the device that raised the original alarm.

To delete alarms from the IEMS database, see "Saving, printing, deleting, and viewing alarms" (page 83).

IEMS alarms clearing job

The alarm clearing job allows you to configure an age-based clearing policy based on the managed device type in IEMS. By default, the ERS 8600 is included in the alarms clearing job as some of the alarms raised from the ERS 8600 do not have an associated clear event. By default all alarms older than seven days are cleared. Note that alarms cleared by this policy are removed from the IEMS alarm view but it does not modify the alarm state in the device that raised the original alarm. If an alarm is present on the originating device when the alarm clearing job runs, the ERS 8600 does not resend the alarm. This policy should only be applied to device types that do not explicitly clear all the alarms that they raise.

Nortel recommends that the IEMS alarms clearing job is only used for devices that do not explicitly send clears for all the alarms they raise.

For more details see "Modifying the alarms clearing job" in *IEMS Performance Management*, NN10327-711.

Alarm resynchronization

For devices that support alarm state resynchronization, the IEMS can synchronize the alarms in the IEMS database with notifications in the corresponding managed objects (element managers or NEs). IEMS resynchronizes the alarms at the following stages:

- when a managed object supporting alarm resynchronization is added in IEMS
- at IEMS server startup
- when IEMS regains communication with managed object supporting alarm resynchronization
- when there are missed notifications in IEMS. (This option is limited to the managed objects which send sequence numbers with its notifications.)

You can also manually resynchronize the alarms. The resynchronization of alarms is supported for the following managed objects:

- element managers
  - APS Manager
  - Session Server Lines Manager
  - MCS Manager (and objects in the MCS sub node under the Element Managers topology)
  - FPM (and objects in the FPM sub node under the Element Managers topology)
  - GWC Manager
  - MG 9000 Manager
  - Multiservice Data Manager
  - UAS Manager
  - CICM Manager
  - Core Element Manager (CEM)
  - UMUX Network Element Manager (UNEM)

  When the alarms are resynchronized for an element manager, the alarms of devices which are managed by the corresponding element manager are resynchronized automatically.
- NEs
  - Universal Signaling Point

  - STORM
  - CICM
  - Session Server - Lines
  - Session Server - Trunks
  - MAS
  - Call Agent Core (supported for CEM)
  - Call Agent Core Platform (supported for CEM)
  - GWC
  - UMUX Network Element Manager (UNEM)
  - MG 3200
  - MG 9000 (via MG 9000 Corba interface)
  - MG 2000
  - MSS 15000 (via MDM ASCII interface)
  - MG 7480/15000 (via MDM ASCII interface)
  - Universal Audio Server (UAS)

- Platforms
  - SPFS

For more details, see the procedure for "Resynchronizing active alarms" (page 75).

IEMS NB agent clear request

The IEMS mediates the events it receives from its managed devices in a Carrier VoIP CS2000 office and provides the ability to forward these events in a consolidated stream to a northbound OSS system. Among the interfaces supported by the IEMS is a northbound SNMP interface. This interface supports the ability for a northbound SNMP manager to clear outstanding alarms in the IEMS alarm view. Compared to the manual clearing policy, the IEMS NB agent clears are only supported for alarms instances in the IEMS where its alarmClear attribute is not set to 1 or 2. For more details about this clearing policy, refer to the *OSS Advance Feature Guide* for a more detailed description of this clearing policy.

Running the PurgeTempData.sh script

The purgeTempData script can be used to clear the event history, alarm, and collected performance data from the IEMS database. To use the command on the IEMS server the craftperson must have root access.

Sample responses

Sample responses with the IEMS application server running are as follows:

```
>:/opt/nortel/iems/current/bin> ./purgeTempData.sh

This will purge all Events, Alarms and Performance data in
the IEMS Database.

Do you want to continue ?[yes | No] :  yes

Checking IEMS server status

!!!!!!  IEMS Server is running.  Kindly purge data after
shutting down the IEMS server.  !!!!!!
```

Sample responses when the IEMS application server has stopped are as follows:

```
>:/opt/nortel/iems/current/bin> ./purgeTempData.sh

This will purge all Events, Alarms and Performance data in
the IEMS Database.

Do you want to continue ?[yes | No] :  yes

Checking IEMS server status

Time taken to complete is :  35 seconds.

Deleting event state files...
```

Clearing alarms raised by managed objects

Application

Use this procedure to clear alarms raised by managed objects.

Fault messages from objects in networks are received by IEMS and displayed in the Network Events panel. The events are propagated to alarms in the IEMS which are displayed in the Alarms panel. The alarms in the Alarms panel have severities (displayed in Severity column), such as Critical, Major, Minor, Warning, Info, and Clear. This procedure describes how to clear alarms.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Alarms** panel under the Fault Management node in the IEMS tree.
3	Select a required alarm row from the Alarms table on the right-hand side panel.
4	Select the **View-->Clear** menu command to change the severity of selected alarm to clear. *Once the alarm severity is changed to clear, the corresponding alarm row is removed from the Alarms panel.* If an alarm is cleared, IEMS changes the severity of the alarm to clear, and generates an event and adds it to the Events database.
5	You have completed this procedure.
	—End—

Resynchronizing active alarms

IEMS can synchronize the alarms in the IEMS database with notifications in the corresponding managed objects (element managers or NEs). IEMS resynchronizes the alarms at the following stages:

- when a managed object supporting alarm resynchronization is added in IEMS
- at IEMS server startup
- when IEMS regains communication with managed object supporting alarm resynchronization
- when there are missed notifications in IEMS. (This option is limited to the managed objects which send sequence numbers with its notifications.)

You can also manually resynchronize the alarms. The resynchronization of alarms is supported for the following managed objects:

- element managers
  - APS Manager
  - MCS Manager (and objects in the MCS sub node under the Element Managers topology)
  - FPM (and objects in the FPM sub node under the Element Managers topology)
  - GWC Manager
  - MG 9000 Manager
  - Multiservice Data Manager
  - UAS Manager
  - CICM Manager
  - Core Element Manager (CEM)
  - UMUX Network Element Manager (UNEM)
- NEs
  - Universal Signaling Point
  - STORM
  - CICM
  - Session Server - Lines
  - Session Server - Trunks
  - MAS

When the alarms are resynchronized for an element manager, the alarms of devices which are managed by the corresponding element manager are resynchronized automatically.

The alarms can be resynchronized manually using one of the following GUIs:

- Topology
- Inventory

Application

Use this procedure to resynchronize the alarms for an object in the topology or inventory GUI.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111. The managed objects listed above that have alarms in the IEMS database in synchronization with the managed objects do not require alarm resynchronization. Hence those object map symbols do not have the **Resynchronize Alarms** menu item in the popup menu for resynchronization.
2	Select your next step.

If you want to resynchronize alarms for an object in the	Do
topology GUI	step 3
inventory GUI	step 7

3	Select the required panel (Network Elements or Element Managers) under the **IEMS Topologies** node in the IEMS tree.
4	Select the required EMS/NE map symbol in the selected topology panel for which resynchronizing alarms is required.
5	Right-click the map symbol and select the **Resynchronize Alarms** menu item from the popup menu to resynchronize the alarms. OR

Select the **<Object-specific menu>-->Resynchronize Alarms** command, where the <Object-specific menu> menu indicates the dynamic menu for the selected EMS/NE in the topology.

6 You have completed this procedure.

7 Select the Inventory panel in the IEMS tree. The Navigation toolbar is located in the top part of the Inventory panel on the right-hand side of the IEMS client.

8 Select a row of required NE in the **Inventory** table for which resynchronizing alarms is required.

9 Right-click any part of the row and select the **Resynchronize Alarms** menu item to resynchronize the alarms

OR

Select the **<Object-specific menu>-->Resynchronize Alarms** menu command, where **<Object-specific menu>** indicates the dynamic menu for the selected EMS/NE row in the Inventory table.

10 You have completed this procedure.

—End—

Viewing the Alarm Count panel

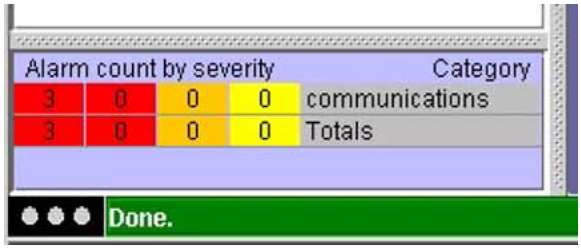
Application

Use this procedure to view the Alarm Count panel.

The Alarm Count panel provides a means of summarizing the alarms generated by the IEMS. The summary gives the number of alarms that have been generated under categories and severity levels.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Alarms Count** panel, which is below the IEMS tree. *The Alarms Count panel is displayed.*



The Alarm Count panel displays the count of alarm as a table. Each row corresponds to a specific category of alarms. Thus, the number of rows corresponds to the number of categories that are configured for viewing, plus a Totals row at the bottom. The number of columns corresponds to the number of severity levels configured for viewing (Critical, Major, Minor or Warning, the last column that shows the category name). The system counts the alarms by severity. When a new alarm is generated, the count is automatically incremented under the appropriate severity column. The Totals row displays the column (severity) totals for alarms of all categories.

For example, the above figure gives the following information:

First Row

- 43 alarms generated in the category Topology, of which
  - 13 alarms have the severity Major

— 30 alarms have the severity Clear

Last Row

- 43 alarms generated in all the categories, of which
  - — 13 alarms have the severity Major
  - — 30 alarms have the severity Clear

3 To view alarm counts of selected categories, refer to the appropriate row.

For example, the user might be interested in the alarms in categories ABC and XYZ:

- First row corresponding to the category ABC
- Second row corresponding to the category XYZ
- Third row corresponding to the total of these categories
- Fourth (last) row corresponding to the total of all categories

4 To view alarms of a specific severity, click on the count displayed for that severity. (For example, if you want to see only the Critical alarms, click on the count in the first column.)

5 To view alarms of a specific category, click on the category name to display all the alarms under that particular category. (For example, if you want to see only the alarms of the topology category, click on "Category".)

6 To view alarms of a specific severity and category, click on the intersection of the required severity column and category row. (For example, to view the alarms with severity Major and belonging to the category Topology, click on the count at the intersection of the Major column and Topology row.)

7 You have completed this procedure.

—End—

Navigating the alarms database using Java Web Start Client

Application

Use this procedure to navigate the alarms database, to view the severity of alarms and to sort data using Java Web Start Client.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Alarms** panel in the IEMS tree. *The navigation toolbar is displayed in the top part of the Alarms panel.* The ways in which the alarms database can be navigated are as follows: • **Viewing the range:** The range of rows that are displayed in the table. It is placed above the Alarms panel. You can select the default page length from the Page Length list box. • **Using the Navigator buttons:** The four navigator buttons, first, previous, next, and last, are located at the top of the internal frame. • **Sorting the data:** The data can be sorted based on the column type and the details can be viewed in ascending or descending order. For details, refer to "Sorting data in Java Web Client" in *IEMS Overview*, NN10329-111 • **Reordering the columns:** The columns can be reordered by dragging a column header and moving it to the required place in the table.
3	You have completed this procedure
	—End—

Searching for alarms

Application

Use this procedure to search for alarms.

This procedure describes how to search for one or more alarms in the Alarms database. The search is performed on the entire database and is not restricted to the displayed page alone. The search can be based on criteria, for example, a particular property or a group of alarms.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Alarms** panel under Fault Management node in the IEMS tree.
3	Select the **Edit-->Search** menu command to launch the Search dialog. Alternatively, you can open the Search dialog from the toolbar using the **Find** button.
4	To specify whether the search is to satisfy any of the search criteria or all the criteria, select the option **Match any of the following** or **Match all of the following**.
5	To specify whether the search is to be on one or more criteria, use the **More** and **Fewer** buttons. The **More** button allows you to add criteria, and the **Fewer** button allows you to delete them. These buttons cause the system to display a window containing three options. The first option lists the existing column headers in the Alarms table. The second option lists two sets of criteria: • Normal Criteria — starts with — doesn’t start with — ends with — doesn’t end with

— contains

— doesn't contain

— equals

— not equals

- Date / Time criteria
  - — is before
  - — is after
  - — equals
  - — not equals

The third option is a date/time field for entering specific values. This data must be entered in the following order: month, day, year, hour, minute, second, and AM/PM (which you can select using the up and down arrows).

6 You have completed this procedure.

—End—

Saving, printing, deleting, and viewing alarms

Action

Use this procedure to do the following:

- Save alarms
- Print alarms
- Delete alarms
- View events related to alarms

Application

Step	Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.

2 Select the **Alarms** panel under the Fault Management node in the IEMS tree.

3 Select your next step.

If you want to	Do
save alarms	step 4
print alarms	step 6
delete alarms	step 8
view events related to an alarm	step 12

4 To save the current range of alarm data displayed in the current custom view, select **Save to File** in the Actions menu.

The system saves the alarm data in the same location as the IEMS server. The file is saved in the directory /opt/nortel/iems/current/logs/alertlogs. The data is saved in text format with each value in each column separated by ":" (colon).

```
Critical:  IEMS: 398:null:  communications:  Jul
25,2003 04:06:31 AM: null
```

5 You have completed this procedure.

6 To print the current range of alarm data displayed in the current custom view, select **Print** in the Actions menu. The IEMS server

must have a configured printer to execute this action. The system sends the output to the default printer.

7 You have completed this procedure.

8 To delete alarms from the database, select the required alarm(s). Hold down the Ctrl key to select more than one row.

9 Select **Delete** from the Edit menu.

10 Click the **OK** button in the confirmation dialog box.

11 You have completed this procedure.

12 To view the related events for an alarm, select the required alarm(s). Hold down the Ctrl key to select more than one row.

13 Select **Events** from the View menu.

The system displays all the events relating to the selected alarm.

14 You have completed this procedure.

—End—

Creating a custom view for alarms

A custom view is a subset of data satisfying given criteria.

Custom view creation involves the following steps:

- defining the search criteria for filtering the data
- specifying how to view the filtered data

"Custom Views" menu has the menu items to create, rename, modify, remove, and save the custom view state.

Custom views have the following features:

- displayed alarms according to specific criteria
- dynamic data updates
- use of the same custom view name at different levels
- customizable columns (properties to view)
- editable column and sort order
- custom view properties can be saved
- custom views can be modified or renamed

Using the features in custom view

To use the custom view features, select the Custom View menu or toolbar buttons. The following table describes the five custom view commands:

Features in Custom Views for alarms

Tool button in Toolbar	Menu bar option	Shortcut	Description
	Custom Views--> Add Custom View	Ctrl+N	Adds a new custom view with specific criteria.
	Custom Views--> Remove Custom View	Ctrl+D	Removes a custom view. The parent custom view (Alarms) cannot be removed.

Tool button in Toolbar	Menu bar option	Shortcut	Description
	Custom Views--> Modify Custom View	Ctrl+M	Modifies a custom view.
	Custom Views--> Save Custom View State	Ctrl+S	Saves the current state of the custom view (properties such as column order, sort order).
	Custom Views--> Rename Custom View	F2	Renames a custom view.

Adding or modifying a custom view

The "Add Custom View" and "Modify Custom View" options cause the system to display a Custom View property sheet. You can customize the custom view properties in the Tree node properties tab by completing the form with the required criteria. When you submit the form, the system creates the new or modified custom view. The tree on the left side of the main window shows the changes.

Removing a custom view

The "Remove Custom View" option removes the currently selected custom view. If this is a parent custom view with one or more dependent child custom views, the complete set of parent and child custom views are removed. The main parent custom view (default - Alarms) cannot be removed. When you select the "Remove Custom View" option, the system prompts you for confirmation before carrying out the action.

Saving a custom view state

The "Save Custom View State" option saves the current state of the custom view, including properties such as the column order, the sorted alarms, and the first and last viewed alarms.

Renaming a custom view

The "Rename Custom View" option renames the current custom view. While renaming the custom view, if you change your mind and want to retain the old name, press the Esc key before completing the rename operation.

Setting the search criteria for a custom view of alarms

Application

Use this procedure to set the search criteria for a custom view of alarms.

The search criteria to create a custom view of alarms is set using the Specify alarm filter criteria form and Tree Node properties of Specify alarm criteria window. This sub-section describes the procedure how to specify the search criteria in the Specify alarm filter criteria form, and provides information on filling out the Tree Node Properties form.

Action

Step	Action

At the IEMS workstation

1 Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.

2 Select the **Alarms** node under the Fault Management node in the IEMS tree.

3 Right-click the **Alarms** node and select the **Custom Views-->Add Custom View** menu command.

The Specify Alarm Filter Criteria window is displayed.

4 Fill in the fields as required.

The following table lists the fields.

Property	Description
Filter View Name	Type the name of the custom view.
Parent name	In the drop-down list, select the object in the navigation tree, under which this custom view is to be added. The default is Alarms.
Severity	In the drop-down list, select the severity of the alarm to be included in the view. Multiple severities can be assigned; separate the severities with commas.

Property	Description
Previous Severity	In the drop-down list, select the previous severity of the alarms to be viewed. For example, if you want to view alarms that were previously minor and then changed to critical, select Minor in this field. Multiple severities can be assigned; separate the severities with commas.
Owner	Type the name of the owner with whom the alarm is associated. To create a custom view for alarms that has no owner, type "NULL" in this field.
Category	Type the category of the alarms in this field. The categories of alarms are: • communications • qualityOfService • processingError • equipment • environmental • others
Group	Type the name by which the alarms are grouped.
Message	Type any important additional information regarding the alarm. If you want to view the alarms with a particular message, type all or part of the message in this field.
Failure Object	Type the specific entity in the source of the alarm that is primarily responsible for the occurrence of this alarm.
Source	Type the source of the alarm.
From Date/Time (modified)	Type the start date and/or time for selecting modified alarms. All Date/Time data must be entered in the order month, day, year, hour, minute, second, and AM/PM which you can select using the up and down arrows.
To Date/Time (modified)	Type the end date and/or time for selecting modified alarms. All Date/Time data must be entered in the order month, day, year, hour, minute, second, and AM/PM which you can select using the up and down arrows.
From Date/Time (created)	Type the start date and/or time for selecting modified alarms.
To Date/Time (created)	Type the end date and/or time for selecting modified alarms.

Property	Description
GroupViewMode	In the drop-down list, select the method for grouping the alarms: • max - the alarms of maximum severity are grouped and displayed at the top of the list. • latest - the newest alarms are grouped and displayed at the top of the list. • none - the alarms are not grouped The Grouping alarms feature does not function in the current release of IEMS.
Alarms Age (modified time)	The age of an alarm denotes the time lapsed since the last modification of the alarm in the IEMS Server. Use the fields to specify criteria based on the age of the alarm. The age can be specified in minutes, hours, days, today, yesterday, or all these criteria together.

If all the above parameters (except Filter View Name) are left blank, the system sets them to the default value "all". For Date/Time properties, the default value is the current date and time.

5 Specify other properties by selecting the **Select Props To View** button.

6 Select the check boxes against the column names which have to be displayed in the Alarms table.

7 Click the Additional table columns button to invoke the User defined table columns dialog.

8 Select the check boxes against the column names or click the **More** button to specify any other column not displayed in the window. The other column names which can be specified in the User defined table columns dialog must be as listed in the Property Name column of the following table.

Display name (can be modified)	Property name
Event label	eventLabel
Log name	logName
Probable cause	probableCause
Specific problem	specificProblem
Event type	eventType

9 Click the **Additional criteria** button in the custom view properties form to specify additional criteria for viewing the filtered data.

The Criteria dialog is displayed.

10 Fill the property fields according to the following table.

Property	Property name
Severity	severity
Owner	owner
Entity	entity
Message	message
Source	source
Date or time	modTime
Category	category
Group name	groupName
Previous severity	previousSeverity
Create time	createTime
Log key	logKey
Probable cause	probableCause
Equipment identifier	equipmentIdentifier

11 Select the **Tree Node Properties** tab in the Specify Alarm Filter Criteria window. The tree node properties determine the way the subset of data is presented.

12 Fill in the property fields according to the following table.

Property	Description
Frame Title	The name to be displayed on the title bar of the custom view internal frame. Type the required name.
Menu File Name	The panel-specific menu file name for the Alarms panel. Do not modify this field.
Icon File	The icon required for the custom view. This icon is visible in the tree as well as in the title bar of the internal frame. The icon file must be in PNG format and must be present under the /opt/nortel/iems/current/ folder or any of its sub-folders. Type the required file name.
Table Popup Menu	The file name of the menu used to display a contextual menu for the objects displayed in the Alarms table. Do not modify this field.

Property	Description
Tree Popup Menu	The file name of the menu used to display a contextual menu for the Alarms node in the IEMS tree. Do not modify this field.
Node Index	The position of the custom view in relation to previously added views. If this field is left blank, the system adds the view at the end of the current list of custom views. Type the required value.

13 You have completed this procedure.

—End—

Example for creating a custom view for alarms

Application

Use this procedure to create a custom view of the alarms from a CS 2000 device. For details of the properties available for filtering alarms, refer to "Setting the search criteria for a custom view of alarms" (page 87).

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Alarms** node under Fault Management node in the IEMS tree.
3	Right-click the **Alarms** node and select the **Custom Views-->Add Custom View** menu command. *The Specify alarm filter criteria window opens.*
4	Enter the text **CS 2000 Manager Alarms** in Filter View Name field.
5	Enter the text **CS2K-Mgr** in the Source field. The wild card "*" used in the Source value "*CS2K-Mgr" causes all the object names ending with "CS2K-Mgr" to be filtered and displayed in the custom view.
6	Click the **Select props to view** button. *The Select table columns window opens.*
7	Check the following text boxes (if not selected) • Severity • Owner • Source • Category • Date/Time
8	Click the **OK** button to apply the changes and click the **Close** button to close the Select table columns window.
9	Click the **Apply filter** button to create a custom view.

You can modify the search criteria for a custom view after the view is created. To modify the search criteria, right-click the custom view. In the Custom Views menu, select **Modify Custom View**. This opens the Specify alarm filter criteria window.

To remove a custom view, right-click the custom view and select **Custom Views-->Remove Custom View**.

10 You have completed this procedure.

—End—

Working with events in Web Client

The following sub-sections describe the operations available in the IEMS Events page of Web Client.

Viewing event details using Web Client

Application

Use this procedure to view event details. Event details can be viewed in the IEMS Web Client.

Action

Step	Action

At IEMS workstation

1 Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.

2 Select the **Fault Management** tab in the Web Client.

3 Select the **Network Events** node in the Module tree (if not already selected).

4 In the Network Events table, click the icon or link under the Severity column for the event.

The properties are listed in the Event Properties page.

Property	Description
Log Name	Displays the log name of the event. The log name is either present in the event, sent by component or inserted by IEMS.
Log Number	Displays the log number.
Failure Object	Displays the specific entity that caused the alarm (in the source specified by the Source field of the event).
Source	Displays the object name with which this event is associated.
Severity	Displays the severity of the event.
Id	Displays the unique ID of the event object. This ID is sequential and IEMS assigns the ID for each event.
Message	Displays any important additional information about the event.

Property	Description
Category	Displays the category, useful for categorizing alarms or events. The category can be one of the following: • communications • qualityOfService • processionError • equipment • environmental • other • others
Created	Displays the time stamp of the event.
Node	Displays the name or IP address of the device which generated the event.
sequenceNumber	Displays the sequence number of the event.
equipmentIdentifier	Displays the managed object display name or IP address that raised the event.
neType	Displays the network element type where the event was raised.
eventLabel	Displays the label of the event.
logKey	Displays the log number of the event.
eventType	Displays the type of event. For example, "FLT" is displayed for fault.
componentID	Displays the ID of the component.
alarmClear	Identifies whether the alarm can be manually cleared. stateless (0) - the alarm is stateless. other (1) - the manual clear status is either unknown or not one of the specified values. forbidden (2) - this alarm cannot be manually cleared. required (3) - this alarm has no corresponding clear so must be manually cleared. optional (4) - this alarm does have a corresponding clear but can also be manually cleared.
notificationID	Displays the notification ID of the received event.
probableCause	Displays the probable cause of the event.

Property	Description
BodyText	Displays the time stamp of the event, component ID, specific cause of the event, and description of the event. The text displayed here varies depending on the device.
specificProblem	Displays information about the specific problem raised.
eCoreNodeName	Displays the originating node where the log node name report is generated. It is contained in the header if the ecore_format office parameter in the OFCVAR table is enabled. An eight-character field. This attribute is applicable for the NTSTD and SSC2 log formats.
officeIdentifier	Displays the switch that generates the identifier log. This is displayed if the log_office_id parameter in the OFCVAR table on the call server is datafilled. 0-12 character optional field. This attribute is applicable for the NTSTD and SSC2 log formats.

5 You have completed this procedure.

—End—

Navigating the events database using Web Client

Application

Use this procedure to navigate, sort, and set the view range for the events database.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Select the **Fault Management** tab in Web Client.
3	Select the **Network Events** view in the Module tree. *The events from managed objects are displayed in the Network Events page in the right-hand side.The navigator buttons First, Previous, Next, and Last are located below the module menus.*
4	Select your next step.

If you want to	
customize the number of events displayed on each page	go to the next step
customize the columns	go to step 7
sort events	go to step 11

5	To customize the number of events displayed on each page, select the required page count from the entries per page list box. By default, 50 events are shown per page in the Network Events table. *The selected number of events is displayed on each page.*
6	You have completed this procedure.
7	To customize the columns, click Customize Columns menu in the module menus area to launch the Customize Columns window.
8	Using the --> and <-- arrow buttons move the columns required to be viewed in the Displayed columns list.

9 Click **Apply** to save the settings and close the window.

10 You have completed this procedure.

11 To sort events, click the required column header in the table to sort in the column in ascending order. Click the column order again to sort it in descending order. If the arrow is facing upward, it means that the column is sorted in ascending order. If the arrow is facing downward, it means the column is sorted in descending order.

By default, the events in the Network Events table are displayed in the order of precedence based on the Date or Time and Event ID and in descending order. Events are assigned IDs and these are based on the date and time they are generated. Hence these two properties are interrelated.

Example

If you need to sort the events based on its status, click the Status column header. If the arrow is facing upward, the events are sorted based on its status and the default order of precedence is Critical, Major, Minor, Warning, Clear, and info. If the arrow is facing downward, the events are sorted based on descending order of the same column; click the Status column header again to sort in ascending order.

12 You have completed this procedure.

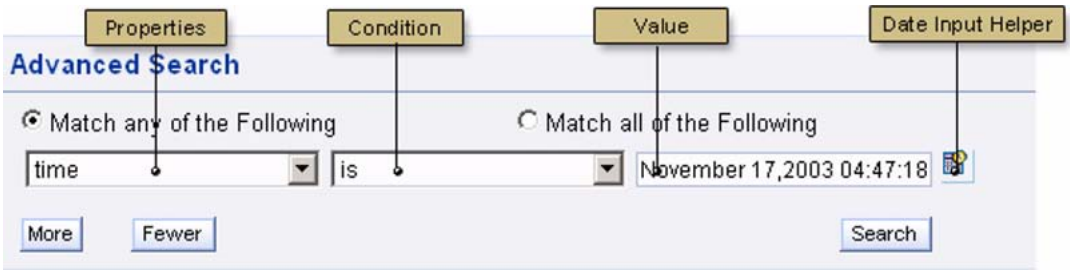
—End—

Searching for events using Web Client

Application

Use this procedure to search for events.

The search option in Web Client facilitates searching for one or more events. The search operation is performed on the entire database and is not restricted to the displayed view alone. You can search for a required event based on a general condition or a unique criteria. The fields in the Advanced Search page is labelled in the figure below:



Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Select the **Fault Management** tab in Web Client.
3	Select the **Network Events** view in the Module tree (if not selected). *The events from managed objects are displayed in the Network Events page in the right-hand side.*
4	Click the **Search** menu item in the Module Menus area. *The Advanced Search page is displayed.*
5	Select the **Match any of the Following** if you want to perform a search operation that satisfies any of the matching criteria that you specify. If you need all the matching criteria to be satisfied for your search operation, select **Match all of the Following**.
6	Select the specific property from the Properties list box that you want the search to be based on.

7 Select the specific condition in the Condition field that you want your search to be restricted to.

8 Enter the exact information you are looking for in the Value field.

Example
If you have selected severity in the Properties list box, then you need to specify the severity value here. For example, critical, major or other severities.

9 If you have selected property related to date or time, follow these sub-steps:

a. Click the **Date Input Helper** button (next to Value field). By default, the current system month, year, date, and time are displayed when the Date Input Helper is launched.

b. Select the required month from the Month list box. By default, current system month is displayed.

c. Select the required year from the Year list box. By default, the current system year is displayed.

d. Click the required date in the calendar. The calendar is based on the month you select and by default the current system date is highlighted.

e. Enter the time in Time field and select **AM** or **PM** from the adjacent list box. By default, the system time is displayed.

f. Click the **Apply** button to return back to the Advanced Search page with the provided date and time details in Date Input Helper.

10 Click the **More** button and repeat step 3 to step 5 if you want to specify additional criteria.

11 Click the **Fewer** button if you want to remove the criteria that were last added.

12 Click the **Search** button to begin the search based on the given criteria.

The events satisfying the configured criteria set are displayed.

The default search results display length shows a maximum of 1000 events. To change the default display length, update the searchViewLength parameter in the /opt/nortel/iems/current/WEB-INF/web.xml file and restart the webserver and client.

13 You have completed this procedure.

—End—

Working with the Network Events view using Web Client

The events in the Network Events page can be numerous and hence difficulty arises in identifying events of your interest. A search can be performed to locate the events you are looking for, but if you are looking for a lot of events that satisfy a certain set of criteria, then use the Add custom view, Modify View Criteria, and Remove View options. These options provide only the events you want in that view, and helps you to avoid doing a search every time.

A custom view that you create is a subset of data that satisfies a given criteria from a larger collection. By creating new views, data can be easily filtered and displayed.

Navigating to the Events database

Application

Use this procedure to navigate to the Events database.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Switch to the **Fault Management** tab in Web Client.
3	Select the **Network Events** view in the Module tree (if not selected). *The events from managed objects are displayed in the Network Events page in the right-hand side.*
4	You have completed this procedure.
	—End—

Adding a custom view

Application

Use this procedure to add a custom view.

A custom view can be added or created by specifying criteria and providing a name for the view. The views you create enable you to quickly monitor the managed objects. Multiple views can also be created to display a variety of information.

Example
You can create a new view named "MasterEvents" which shows only events in a particular network. Within this "MasterEvents" view, you can create more views. For example, ME1 can have a different set of criteria, say only critical events in that particular network. Deleting MasterEvents view deletes its custom views (ME1, ME2, etc.) as well.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Network Events** view in the Module tree (if not selected).
2	Click the **Add custom view** menu item in the Module Menus area. *The Add Event Custom View page is launched.*
3	Enter the custom view name in the Child view name field (mandatory).
4	Enter the details for the following fields. Refer to the "Setting the search criteria for a custom view of events" (page 35) module for using the fields listed below: • Severity • Source • Failure Object • Message • Category • Node • Network • Events generated after • Events generated before • Event Age
5	Click the **Submit** button to create a custom view with the details provided.

A custom view is created with the specified name and a view is added under the Network Events node in the Web Client tree.

6 You have completed this procedure.

—End—

Modifying a custom view

Application

Use this procedure to modify a custom view.

A view can be modified to change the criteria that were set, or you can rename the view.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the child view node under the **Network Events** node that has to be modified.
2	Click the **Edit View Criteria** menu item in the Module Menus area. *The Edit Event View Criteria page is launched.*
3	Modify the child view name in the Custom view name field (if required).
4	Modify the details for the following fields. Refer to the "Setting the search criteria for a custom view of events" (page 35) module for using the fields listed below: • Severity • Failure Object • Message • Category • Node • Network • Events generated after • Events generated before • Event Age

5 Click the **Submit** button to modify the custom view with the details provided.

6 You have completed this procedure.

—End—

Removing a custom view

Application

Use this procedure to remove a custom view.

A custom view can be removed from the Network Events when it is not required.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the custom view node under the **Network Events** node that has to be removed.
2	Click the **Remove View** menu item in the Module Menus area. *A dialog is launched confirming whether you want to remove the child view.*
3	Click the **Yes** button to remove the selected custom view. *The selected custom view is removed.*
4	You have completed this procedure.

—End—

Saving, printing and viewing related alarms of events using Web Client

In Web Client, you can save and print events and view alarms related to an event. The save option is used to save the current range of event data displayed in the page. The print option prints the current range of event data displayed in the page. Alarms that are generated from the corresponding events can also be viewed. This sub-section describes the procedures for the following operations:

- "Saving events" (page 108)
- "Printing events" (page 109)
- "Viewing related alarms" (page 110)

Navigating to the Events Database

Application

Use this procedure to navigate to Events Database.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Switch to the **Fault Management** tab in Web Client.
3	Select the **Network Events** view in the Module tree (if not selected). *The events from managed objects are displayed in the Network Events page in the right-hand side.*
4	You have completed this procedure.

—End—

Saving events

Application

Use this procedure to save the events displayed in the Network events frame as an HTML file.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Network Events** view in the Module tree (if not selected).
2	Right-click the Network Events node and select the **Open in New Window menu** item to open the Network Events panel in a new browser window.
3	Save the Network Events page (opened in new window) as an HTML file locally using **File-->Save As...** menu command
4	You have completed this procedure.

—End—

Printing events

Application

Use this procedure to print events.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Network Events** view in the Module tree (if not selected). You need to have a printer configured in the system where you are performing the print operation.
2	Click the **Print Version** menu item located above the Events List View. *A new page is launched with the list of events is displayed.*
3	Click the **Print** button in the new page launched to print the events in that page.
4	You have completed this procedure.

—End—

Viewing related alarms

Application

Use this procedure to view related alarms.

Events are propagated to alarms based on their significance that require your attention. From the Events view, you can view the alarm that has been propagated from an event.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Network Events** view in the Module tree (if not selected).
2	Select the check box of the required events in the Network Events page. To view related alarms for more than one event, select multiple check boxes.
3	Select the **View Alarms** from the Operations list box above the column header. *The Alarms page with all the alarms related to those events are displayed, and they are displayed in a descending order based on the time of their modification.*
4	You have completed this procedure.
	—End—

Working with alarms in Web Client

Alarms are generated when a failure or fault is detected in the network devices. The generated events are converted to alarms based on their significance. This section includes procedures on how to perform tasks for alarms.

Viewing alarm details using Web Client

Application

Use this procedure to view alarm details.

The alarm details can be viewed in the IEMS Web Client.

Action

Step	Action
	At IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Click the **Fault Management** tab in the Web Client.
3	Select the **Alarms** view in the Module tree (if not selected).
4	In the alarms table, click the icon or link in the Severity column for the alarm. *The properties and their values are listed in the Alarms table.* For a description of the properties, refer to the following table.

Property	Description
Log Name	Displays the log name of the event. The log name is either present in the event sent by the component or inserted by IEMS.
Log Number	Displays the log number of the event.
Failure object	The specific entity that caused the alarm (in the source specified by the Source field of the alarm).
Source	The object name with which the alarm is associated.
Created	The date and time when the alarm was first created.
Last Updated	The date and time when the alarm was last updated.
Severity	The severity of the alarm.
Message	Any additional information about the event or alarm.

Property	Description
Category	The category of the alarm. The alarm category can be one of the following: • communications • qualityOfService • processionError • equipment • environmental • other
Owner	The name of the user who has acknowledged the corresponding alarm is displayed in this field. If it is not acknowledged by any of the users, this field is blank
Priority	This field is reserved for future use.
sequenceNumber	Displays the sequence number of the alarm.
alarmIndex	Displays a unique numeric ID that is generated for each alarm.
equipmentIdentifier	Displays the equipment where the alarm was raised.
neType	Displays the network element type where the alarm was raised.
eventLabel	Displays the label of the alarm or event.
logKey	Displays the number of the log.
eventType	Displays the type of the alarm or event.
alarmClear	Identifies whether the alarm can be manually cleared. stateless (0) - the alarm is stateless. other (1) - the manual clear status is either unknown or not one of the specified values. forbidden (2) - this alarm cannot be manually cleared. required (3) - this alarm has no corresponding clear so must be manually cleared. optional (4) - this alarm does have a corresponding clear but can also be manually cleared.
componentID	Displays the name of the component that raised the alarm.
notificationID	Displays the notification ID of the received event.
probableCause	Displays the probable cause of the alarm.

Property	Description
bodyText	Displays the log details related to the alarm.
specificProblem	Displays information about the specific problem raised.
Events	Click this link to display any events related to this alarm.
Acknowledge or Unacknowledge	Click this link to acknowledge or unacknowledge the alarm. Acknowledging an alarm helps to allocate an alarm to a work group or a user. The system records an alarm annotation entry against the name of the user who unacknowledged it.
Annotate	Click this link to add notes to the alarm.

5 Click the **Annotation & History** link to view the annotation and history details of the alarm (if any).

6 You have completed this procedure.

—End—

Navigating the alarms database using Web Client

Application

Use this procedure to navigate, sort, and set the view range for the alarms database using Web Client.

Action

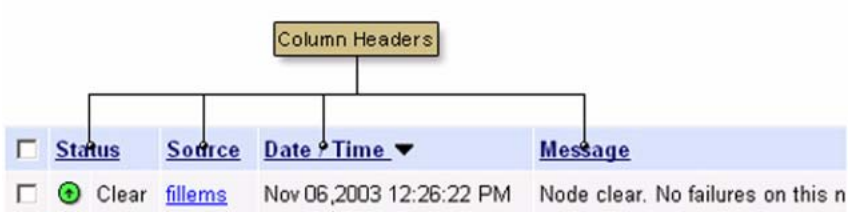
Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Select the Fault Management tab in Web Client.
3	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page on the right-hand side..The navigator buttons First, Previous, Next, and Last are located below the module menus.*
4	Select your next step.

If you want to	
customize the number of events displayed on each page	go to step 5
customize the columns	go to step 7
sort alarms	go to step 11

5	To customize the number of alarms displayed on each page, select the required page count from the entries per page list box. By default, 25 alarms are shown per page in the Alarms table. *The corresponding number of alarms is displayed on each page.*
6	Go to step 12.
7	To show or hide columns, click the Customize Columns menu item in the module menus area to launch the Customize Columns window.
8	Click the **-->** or **<--** buttons to move the columns required to be viewed in Displayed Columns list.
9	Click the **Apply** button to save the settings and close the window.

10 Go to step 12.

11 To sort the alarms, click the required column header in the table to sort the column in the ascending order. Click the column order again to sort it in descending order. If the arrow is facing upward, it means that the column is sorted in ascending order. If the arrow is facing downward, it means that column is sorted in descending order.



By default, in the Alarms page, the alarms are displayed in the order of precedence based on time and in descending order.

Example

If you need to sort the alarms based on their status, click the **Status** column header. This sorts the alarms based on their status, and the default order of precedence is Critical, Major, Minor, and Warning. For descending order of the same column, click the Status column header again.

12 You have completed this procedure.

—End—

Viewing alarm counts using Web Client

Application

Use this procedure to view alarm counts.

The Alarm Count Panel is displayed below the Module Tree which enables you to view a summary of all the alarms generated by IEMS. The summary gives the number of alarms that are generated under categories and severity levels, and this panel is automatically refreshed every 30 seconds.

The Alarm Count panel is presented in a tabular format for easy viewing. Each row corresponds to a specific category of alarms. The number of rows corresponds to the number of alarm categories. The last row provides the total number of alarms for each severity level. An alarm can have the following severity levels:

- Critical
- Major
- Minor
- Warning

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Switch to the **Fault Management** tab in Web Client. *The Alarms Count Panel is located below the Module tree.* The alarm count is based on severity. When a new alarm is generated, the count is updated automatically under the appropriate severity column. You can view all the alarms under a specific severity or a specific category.
3	To view all alarms with a specific severity, click the count in the Total row that corresponds to the specific severity of the alarms you want to view. For example, if you want to view all the critical alarms, click the total count in the first (red) column.
4	To view all alarms for a specific category, click the category name of the alarms you want to view.

For example, if you want to view all the alarms in the topology category, click Topology in the Category column.

5 To view all alarms with a specific severity level for a specific category, click the count corresponding to the specific severity and category of the alarms you want to view.

For example, if you want to view all the critical alarms in the topology category, click the count in the first (red) column and in the Topology row.

6 You have completed this procedure.

—End—

Searching for alarms using Web Client

Application

Use this procedure to search for alarms.

The Search option in Web Client facilitates searching for one or more alarms. The search operation is performed on the entire database and it is not restricted to the displayed page alone. You can search for a required alarm based on a general condition or a unique criterion.

Action

Step	Action
	At IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Switch to the **Fault Management** tab in Web Client.
3	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page on the right-hand side.*
4	Refer to "Searching for events using Web Client" (page 101) since the search for alarms is the same as explained in that procedure.
5	You have completed this procedure.

—End—

Using operations in alarms using Web Client

You can view annotations and alarm history, view related events, view related alarms, print alarms, delete alarms, clear alarms, and perform other operations. Refer to the following procedures for details on operations such as:

- "Adding comments to alarms" (page 120)
- "Viewing annotations and alarm history" (page 121)
- "Viewing related alarms" (page 122)
- "Printing alarms" (page 122)
- "Saving alarms as an HTML file in Web Client" (page 123)

Navigating to the Alarms Database

Application

Use this procedure to navigate to the Alarms Database in the Web Client.

Action

Step	Action
	At IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Select the Fault Management tab in Web Client.
3	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page in the right-hand side.*
4	You have completed this procedure.

—End—

Adding comments to alarms

Application

Use this procedure to add annotations for an alarm.

It is important to track any action you have taken to fix an alarm or any new information you have gathered about the alarm. The Annotate option can be used to add notes to an alarm for future reference.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page in the right-hand side.*
2	Click the equipment identifier of the managed object for which the alarm details are required in the Alarms table. The properties and their values are listed in the Alarm Properties page. For description of properties, refer to Property table of "Viewing event details" (page 8).
3	Click the **Annotate** menu item in the module menus area to launch the Annotate page in a new window.
4	Enter the required message in the Message text area.
5	Click the **Annotate** button to annotate the selected alarm.
6	You have completed this procedure.

—End—

Viewing annotations and alarm history

Application

Use this procedure to view annotations and the history of an alarm.

The history of the alarms gives the complete information on the status of the alarms, such as when they are added or updated. For example, when a critical alarm is generated, the Alarms view displays the current status of the alarm. If the problem has been fixed, an alarm with clear severity updates the one with critical severity.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page in the right-hand side.*
2	Click the icon in the **Status** column of the alarm in the Alarms table.

3 Click the **Annotation & History** tab to view the annotation and history details of alarm (if any).

4 Click the **Merge History** item in the Annotation & History page to view the annotations and history together in the order of precedence based on time.

5 To return to the separate views of annotation and history, click the Annotation & History menu.

6 You have completed this procedure.

—End—

Viewing related alarms

Application

Use this procedure to view the related alarms for an alarm of a managed object.

The alarms generated for the same managed object can be viewed using this option.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page in the right-hand side.*
2	Click the equipment identifier of the managed object for which the alarm details are required in the Alarms table.
3	Click the **Related Alarms** tab to launch the Related Alarms page. *The alarms are listed in the page; if no alarms are present, the "No Other Failures in this Group" message is displayed.*
4	You have completed this procedure.

—End—

Printing alarms

Application

Use this procedure to print the alarms.

Action

Step	Action
	At the Fault Management tab of Web Client
1	Select the **Alarms** view in the Module tree. *The alarms are displayed in the Alarms page in the right-hand side.*
2	Click **Print version** menu item in the Module menus area to launch the Alarms page in a new window. *The printable format of alarms is displayed in this page.*
3	Click the **Print** button. *Your operating system's print options are launched.* *The Printing Alarms page helps to gather information on all alarms or those of your interest.* **Example** The Alarms List View can be customized by adding or removing columns using the Customize Columns option, order the alarms by sorting, or by create new views. Use the print option to get the printable version of the Alarms page.
4	You have completed this procedure.
	—End—

Saving alarms as an HTML file in Web Client

Application

Use this procedure to save the displayed alarms as an HTML file.

Action

Step	Action
	At IEMS workstation
1	Refer to "Launching the IEMS Web Client" to launch the IEMS Client.
2	Select the **Alarms** node under the Fault Management node in the IEMS tree.

3 Right-click the **Alarms** node and select **Open** in the New Window menu item.

The Alarms frame opens in a new browser window.

4 Save the **Alarms** page as HTML file in the local using **File-->Save As...** menu command.

The file is saved in the directory /opt/nortel/iems/current/state.

5 You have completed this procedure.

—End—

Working with the alarm view in Web Client

The alarms in the Alarms List View can be numerous and, hence, it is difficult to identify the data of your interest. You can use the Search option to locate the alarms you are looking for. But if you are looking for many alarms that satisfy a certain set of criteria, you can use the Add Custom View, Edit View Criteria, and Remove View options. This helps you to retrieve only the alarms you want to view in that custom view, instead of doing a search every time.

A custom view that you create is a subset of data that satisfies a given criterion from a larger collection. By creating new views, the data is easily filtered and displayed, and allows you to sort through a large amount of alarms data.

Navigating to the Alarms Database

Application

Use this procedure to navigate to the Alarms Database in the Web Client.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to "Launching IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Switch to the **Fault Management** tab in Web Client.
3	Select the **Alarms** node in the Module tree. *The alarms are displayed in the Alarms page in the right-hand side*.
4	You have completed this procedure.

—End—

Adding a new view

Application

Use this procedure to add an alarm view.

You can add or create a new view by specifying criteria and providing a name for the view. The views you create enable you to quickly monitor the managed objects. You can create multiple views that display a variety of information.

Example
You can create a new view named MasterAlarms which shows only alarms in a particular managed object. Within this MasterAlarms view, you can create more views. For example, MA1 can have a different set of criteria, say only critical alarms in that particular network. Deleting MasterAlarms deletes its custom views (MA1, MA2, and so on).

Action

Step	Action
	At the Fault Management tab of IEMS
1	Click the **Add Custom View** menu item in the Module menus area. *The Add Alarm Custom View page opens, listing the options to create the custom view.*
2	Enter the required criteria in the fields available. For information on each of the fields in this form, refer to "Setting the search criteria for a custom view of alarms" (page 87). Wildcard characters can be used to specify the matching criteria. For information on the wildcard characters that can be used, refer to "Custom View Filtering Criteria" in *IEMS Overview*, NN10329-111. If none of the fields is filled in (except for Custom view name), then by default all the fields are set with the value 'all'.
3	Click the **Submit** button after configuring the criteria.
4	You have completed this procedure.
	—End—

Modifying a view

Application

Use this procedure to modify an alarm view.

A view can be modified to change the criteria that were set or to rename the view.

Action

Step	Action
	At the Fault Management tab of IEMS

1 Click the required view under the **Alarms** tree in the Module tree.

2 Click the **Edit View Criteria** menu item in the Module menus area.

The custom view form is displayed with the configurations (made at the time of creation or last modification).

For information on each of the fields in this form, refer to "Setting the search criteria for a custom view of alarms" (page 87). Wildcard characters can be used to specify the matching criteria. For information on the wildcard characters that can be used, refer to "Using custom view filtering criteria" in *IEMS Overview*, NN10329-111.

3 Click the **Submit** button to update the changes.

4 :You have completed this procedure.

—End—

Removing a view

Application

Use this procedure to remove an alarm view.

A view can be deleted from the Alarms List View when you do not require it anymore.

Action

Step	Action
	At the Fault Management tab of IEMS
1	Click the required view under the **Alarms** tree in the Module tree. The parent node Alarms cannot be deleted from the Fault Management tree. Only those views created under this parent node can be deleted.
2	Click the **Remove View** menu item in the Module menus area. *A dialog is launched to confirm the operation. Click the Yes button to remove the view.*
3	You have completed this procedure.

—End—

Replacing a failed SPFS-based server

Application

Use the following procedure when an SPFS-based server has failed and you need to replace it. This procedure provides the instructions for a one-server configuration or a two server configuration.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core Billing Manager (CBM)

Prerequisites

You must have a replacement server.

ATTENTION

Ensure that no provisioning activities are in progress, or scheduled to take place during this procedure.

You must have the root user ID and password to log into the system.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform fault-admin actions.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration, NN10358-611*
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration, NN10358-611*
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration, NN10358-611*

Action

Perform the steps under one of the headings that follow to complete this procedure.

- "Replacing an SPFS-based server (one-server configuration)" (page 129)
- "Replacing one server in an HA configuration" (page 129)
- "Replacing both servers in an HA configuration" (page 130)

Replacing an SPFS-based server (one-server configuration)

Step	Action
	At the COAM frame
1	Disconnect and remove the failed server.
2	Connect and power up the replacement server.
3	Restore the file systems and oracle data from backup media. If required, refer to procedure Routing customer logs to a remote host. Restoring the oracle data does not apply to the CBM as it does not use an oracle database. You have completed this procedure.

—End—

Replacing one server in an HA configuration

Step	Action
	At the COAM frame

1 Disconnect and remove the failed server.

2 Connect and power up the replacement server.

3 Clone the image of the active server onto the server you just replaced. If required, refer to procedure Routing customer logs to a remote host.

You have completed this procedure.

—End—

Replacing both servers in an HA configuration

Step	Action

At the COAM frame

1 Disconnect and remove one failed server.

2 Connect and power up the replacement server.

3 Restore the file systems and oracle data from backup media on the server you just replaced. If required, refer to procedure Routing customer logs to a remote host.

Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

4 Disconnect and remove the other failed server.

5 Connect and power up the replacement server.

6 Clone the image of the active server onto the server you just replaced. If required, refer to procedure Routing customer logs to a remote host.

You have completed this procedure.

—End—

Monitoring and viewing Certificate Manager security logs

Application

Use this procedure to monitor logs produced by the Certificate Manager application in real-time or to view Certificate Manager security logs.

Prerequisites

This procedure has the following prerequisites:

- Certificate Manager must be installed.

Action

Step	Action

At your workstation

1 Log in to the Certificate Manager server using one of the following methods:

If using	Do
telnet (unsecure)	go to step 2
ssh (secure)	go to step 3

2 Complete the following sub-steps to log in using telnet.

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the hostname or IP address of the Certificate Manager server

b. When prompted, enter you user ID and password.

c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d. When prompted, enter the root password.

Continue with step 4.

3 Complete the following sub-steps to log in using ssh (secure).

ATTENTION
Use the following command only if your workstation platform supports ssh. Otherwise, the command fails.

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the hostname or IP address of the server

b. When prompted, enter the root password.

At the Certificate Manager client

4 Access the directory level where the security log files reside by entering

```
$ cd /var/log
```

5 Use the following table to determine your next step.

If you want to	Do
view a log file	step 6
monitor Certificate Manager logs in real-time	step 14

6 List the directory content by typing

```
$ ls
```

and pressing the enter key.

The system displays a list of different log files, such as, customerlog, securitylog, and so on. These files are appended with numbers, for example “customerlog.0”. The files with the lower numbers are the newer files and the current file does not have an extension.

7 If the file that you want to view is zipped (has an extention .gz), unzip it using the following command. The most recent file does not have an extension. Otherwise, go to the next step.

Unzip the file by typing

```
$ gunzip <log_filename.gz>
```

and pressing the enter key.

where

log_filename.gz is the name of the log file you want to unzip

Example

```
$ gunzip securitylog.1.gz
```

The file changes to a readable file securitylog.1.

8 Use the following table to determine your next step.

If you want to view	Do
the entire content of a log file	step 9
specific content of a log file	step 11

9 Display the entire content of a log file by typing

```
$ cat <log_filename> |more
```

and pressing the enter key.

where

log_filename is the name of the log file you want to display. See the first table below for specific examples.

Example

```
$ cat customerlog.0 |more
```

Press the space bar to scroll through the file if it is larger than the screen can display.

10 Go to step 12.

11 Search and display specific content of a log file by typing

```
$ cat <log_filename> |grep <search_string>
```

and pressing the enter key.

where

search_string is the text you want to search for, for example KRB (to search for logs associated with the Kerberos application)

Example

```
cat customerlog.0 |grep GWC309
```

or

```
cat securitylog.1 |grep KRB_LOG
```

12 To print the contents of this file, contact your site system administrator for assistance with using UNIX print commands and with locating a printer connected to your network.

13 You have completed this procedure.

14 Enter the following command to view the Certificate Manager securitylog files.

```
$ tail -f securitylog | grep -i PK
```

The system displays the latest contents of the securitylog file for the Certificate Manager logs and is updated automatically.

For details of all Certificate Manager log files, see *Carrier Voice over IP Fault Management Logs Reference Guide*, NN10275-909.

15 You have completed this procedure.

—End—

Logs and operational measurements supported by CEM

Logs

For logs generated by the core and sent to the CEM and then to the IEMS, see the following table.

Log numbers	Documentation reference
ESA120, ESA121	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
ATM300, ATM301, ATM501, ATM600, ATM605	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
XPKT806, XPKT807	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
BITS300, BITS310, BITS500, BITS600, BITS601, BITS610	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
BOOT101	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
C7UP104, C7UP109, C7UP113, C7UP114, C7UP120, C7UP130, C7UP310	*CDMA/TDMA Logs Reference Manual*, 411-2131-510
CARR300, CARR310, CARR320, CARR330, CARR331, CARR340, CARR341, CARR500, CARR501, CARR510, CARR511, CARR512, CARR800, CARR801, CARR811	*CDMA/TDMA Logs Reference Manual*, 411-2131-510
CCMT301, CCMT501, CCMT502, CCMT601	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
DPTM500, DPTM501, DPTM502, DPTM503, DPTM504, DPTM550, DPTM560, DPTM700, DPTM701	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
ENET308, ENET311	*North American DMS-100 Log Report Reference Manual*, 297-8021-840

Log numbers	Documentation reference
EXT102, EXT108	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
IWBM500, IWBM501, IWBM603, IWBM800, IWBM801, IWBM802, IWBM803	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
LINK300	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
NODE300, NODE303, NODE323, NODE326, NODE450, NODE500, NODE600	*GSM NSS/UMTS VCN OAM Reference Manual*, 411-8111-511 *Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
QCA201, QCA202, QCA203, QCA300, QCA301, QCA302, QCA305, QCA310, QCA315, QCA322, QCA399	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
SDM300, SDM301, SDM302, SDM303, SDM306, SDM308, SDM309, SDM314, SDM315, SDM317, SDM321, SDM327, SDM500, SDM501, SDM502, SDM503, SDM504, SDM505, SDM550, SDM600, SDM601, SDM602, SDM603, SDM604, SDM608, SDM609, SDM617, SDM621, SDM627, SDM630, SDM650, SDM700	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
SDMB300, SDMB310, SDMB315, SDMB316, SDMB320, SDMB321, SDMB350, SDMB355, SDMB360, SDMB365, SDMB367, SDMB375, SDMB380, SDMB390, SDMB400, SDMB530, SDMB531, SDMB550, SDMB600, SDMB610, SDMB615, SDMB620, SDMB621, SDMB625, SDMB650, SDMB655, SDMB660, SDMB675, SDMB680, SDMB820	*Carrier Voice over IP Fault Management Logs Reference,* NN10275-909
SOS701, SOS702, SOS703	*XA-Core Reference Manual*, 297-8991-810

Log numbers	Documentation reference
SPM301, SPM310, SPM311, SPM312, SPM313, SPM314, SPM330, SPM331, SPM332, SPM334, SPM335, SPM336, SPM337, SPM338, SPM339, SPM340, SPM341, SPM342, SPM344, SPM350, SPM352, SPM353, SPM352, SPM355, SPM356, SPM357, SPM370, SPM370, SPM399, SPM500, SPM501, SPM510, SPM600, SPM619, SPM630, SPM637, SPM638, SPM641, SPM642, SPM644, SPM650, SPM651, SPM652, SPM653, SPM654, SPM655, SPM656, SPM657, SPM658, SPM660, SPM661, SPM625, SPM670, SPM700, SPM701, SPM702, SPM703, SPM704, SPM705, SPM706, SPM707, SPM708, SPM709, SPM710	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909
TMN301, TMN302, TMN304, TMN303, TMN304, TMN309, TMN311, TMN600, TMN601, TMN604, TMN605	*Carrier Voice over IP Fault Management Logs Reference,* NN10275-909
TRK882	*North American DMS-100 Log Report Reference Manual*, 297-8021-840
XAC300, XAC302, XAC303, XAC304, XAC305, XAC306, XAC307, XAC308, XAC309, XAC310, XAC312, XAC320, XAC321, XAC322, XAC323, XAC324, XAC325, XAC326, XAC327, XAC329, XAC330, XAC333, XAC400, XAC413, XAC415, XAC418, XAC420, XAC600, XAC601, XAC602, XAC603, XAC604, XAC605, XAC606, XAC607, XAC608, XAC609, XAC610, XAC612, XAC613, XAC614, XAC615, XAC618, XAC619, XAC620, XAC622, XAC623, XAC624, XAC625, XAC626, XAC627, XAC628, XAC629, XAC630, XAC631, XAC632, XAC633, XAC634, XAC635, XAC640, XAC641, XAC801, XAC814	*XA-Core Reference Manual*, 297-8991-810
XACP300, XACP500, XACP600	*XA-Core Reference Manual*, 297-8991-810

Log reports CSEM300 and CSEM600

Log reports CSEM300 and CSEM600 address a change of format for northbound events on the log feeds of IEMS when used in conjunction with CEM. Log reports CSEM300 and CSEM600 act as an envelope to contain

Communication Server 2000 (CS 2000) and SuperNode Data Manager (SDM) logs. The logs in IEMS are encapsulated inside the log reports CSEM300 and CSEM600 in the northbound NT STD and SCC2 feeds. Log report CSEM300 indicates alarm sets and alarm clears for these logs. Log report CSEM600 indicates INFO and unmapped logs for these logs.

Log numbers	Documentation reference
CSEM300, CSEM600	*Carrier Voice over IP Fault Management Logs Reference*, NN10275-909

Suppressed logs

When the Store and Forward service is enabled, the logs in the following table are disabled at the Core for the SDM/CBM log stream. These logs are not available through the Log Delivery application. For the procedure to unsuppress these logs, see "Specifying the logs delivered from the CM to the core manager" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

Suppressed logs

Logs that are DELREPed by the SAF service at the Core
AUTH, CAFT, CALM, CDPD, CHIP, CLFL, CPER, CPRT, CTID, DEPS, DFA, DIM, DROP, ERV, ESNF, FCEL, FRAU, FRS, GAME, HMT, IOGA, IS41, LAM, MBPG, MCD2, MCD3, MCDR, MIWF, MLNP, MTX, NCAS, NOPT, OCC, OM2, OMGA, OTAF, PCO, PVAL, RAD, RFES, RFP, RFPE, RPC, RRIF, RSSI, SMO, SMS, SMT, SPRF, SSR, TIER, TUPL, X75

Operational Measurements

For performance management functionality, all of CS 2000 OMs are supported. OM groups can be selected and exported in tab delimited format or switch format.

For details of CS 2000 OMs that are available through the CEM interface, refer to the following documents:

- *XA-Core Reference Manual*, 297-8991-810
- *DMS-SPM Feature Description Reference Manual*, 297-1771-330
- *DMS-100 Family Extended Peripheral Module Operational Measurements Reference Manual*, 297-8321-814
- *DMS-GSP Operational Measurements Reference Manual*, 297-2651-814
- *DMS SuperNode Signaling Transfer Point Operational Measurements Reference Manual*, 297-8101-814

- *DMS SuperNode STP/SSP Integrated Node Operational Measurements Reference Manual*, 297-8083-814
- *Carrier VoIP Performance Management Operational Measurements Reference*, NN10264-709

Automated backup and restore

The Automatic Backup and Accelerated restore feature, referred to as ’remote backup’ is specific to geographically-dispersed configurations.

The Automatic Backup and Accelerated restore feature, referred to as ’remote backup’ will remotely backup all data on the ’target’ unit. This provides a standby backup system ready to provide service should the primary system or cluster be unavailable for an extended period of time (for example, catastrophic site loss).

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup which can be scheduled to automatically occur from once a day to four times per day. This tool also provides a facility for manually initiating a backup and monitoring its progress. The standby server has an identical copy of files from the last backup, so it can become the primary system via changing the boot pointer and rebooting. When the primary site is again available, the remote backup feature can be reused to transfer current system configuration back to the primary site and system.

For details about geographic survivability and remote backup, refer to *Carrier VoIP Solutions Disaster Recovery Procedures*, NN10450-900.

For more information and procedures on IEMS backup and restore, see "Backup and restore" in *IEMS Administration and Security*, NN10336-611.

Carrier VoIP

IEMS Fault Management

Publication: NN10334-911
Document status: Standard
Document version: 04.02
Document date: 20 October 2006

To provide feedback or report a problem in this document , go to

http://www.nortel.com/documentfeedback

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.