Carrier VoIP

IEMS Configuration

NN10330-511

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

Copyright © 2006, Nortel Networks
All Rights Reserved.

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

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

Contents

IEMS Configuration 7

Working with IEMS topologies in the JWS client 9

Adding objects to topology 11

Adding an EMS platform 15
Adding a Server Platform Foundation Software (SPFS) platform 16
Adding a SuperNode Data Manager platform (SDM platform) 19

Adding element managers 21
Adding an Audio Provisioning Server Manager (APS Manager) 22
Adding a Core Element Manager 25
Adding a CICM Manager 28
Adding a Communication Server 2000 Core Manager 32
Adding a Fault and Performance Manager 37
Adding a Gateway Controller Manager 41
Adding an MCS/CSE Manager for MCS/CSE and Media Portal 44
Adding an MCS Manager for SSLines 49
Configuring Session Managers for SSH launch 56
Configuring provisioning clients 58
Adding a Multiservice Data Manager 60
Determining the associated MDM platform 65
Adding a Multiservice Gateway 9000 Manager 68
Adding a SAM21 Manager 71
Adding a UMUX Network Element Manager 74
Adding a Universal Audio Server Manager 77

Adding EMS applications 81
Adding an Audio Provisioning Server application 82
Adding a Certificate Manager application 84
Adding a Line Maintenance Manager application 86
Adding a Network Patch Manager application 88
Adding an OSSGate application 90
Adding a QoS Collector application 93
Adding a Synchronized Backup Restore Manager application 95

Copyright © 2006, Nortel Networks

Adding a Trunk Maintenance Manager application 97

Adding network elements 99
Adding a CICM NE 100
Adding a GWC NE 104
Adding CS 2000 Core and Call Agent Core NEs 106
Adding an Ethernet Routing Switch 8600 NE 108
Configuring the ERS 8600 to send events and alarms to the IEMS 111
Configuring the Ethernet Routing Switch 8600 for IEMS 116
Adding MCS/CSE and Media Portal NEs 129
Adding a Media Application Server 131
Adding a Media Gateway 3200 NE 135
Adding Media Gateway 7480/15000/20000 and MSS 15000 NEs 138
Adding an MG 9000 NE 140
Adding a Media Server 2000 142
Adding a SAM21 NE 145
Adding an SSTrunks NE 147
Adding an SSLines NE 151
Adding a STORM NE 153
Configuring STORM for IEMS 157
Adding a UAS NE 159
Adding a UMUX NE 161
Adding a Universal Signaling Point NE 163
Editing object properties 167
Editing platform object properties 168
Editing element manager object properties 170
Editing EMS application object properties 173
Editing NE object properties 175

Configuring and maintaining MS 2000 devices 177
Configuring parameters for MS 2000 NEs 179
Configuring SNMP setup for MS 2000 NEs 182
Configuring the passwords for the MS 2000 NEs 186
Configuring automated backup of the INI file 189
Locking or unlocking the MS 2000 node 191
Backing up the INI file 192
Resetting the MS 2000 NE 193
Uploading the load files to the IEMS server 195

Configuring and maintaining the MG 3200 devices 197
Configuring IKE parameters for MG 3200 NEs 199
Configuring IPSec parameters for MG 3200 NEs 204
Enabling and disabling the IPSec for MG 3200 209
Configuring automated backup of the INI file for MG 3200 211
Resetting the MG 3200 NE 213

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Working with CEM managed nodes 215
Creating a CEM managed node instance 216
Deleting a CEM managed node instance 220

Using topology operations 223
Editing and viewing object properties using Java Web Client 224
Updating status of objects manually 230
Managing objects 233
Unmanaging objects 235
Adding a custom topology node 237
Searching for objects in the topology view 242
Viewing the SAM21 cards 243
Partitioning the NEs discovered by MDM 244
Zooming the topology view 246
Using toolbars in the Topology view 248
Grouping and ordering map symbols 251
Deleting object and traces 254
Changing the topology layout 255
Changing topology background 256

Working with the inventory panel 257
Navigating inventory panel 258
Searching EMS/NE from inventory panel 260
Resynchronizing inventory for element managers 262
Identifying problems of objects in the inventory panel 264
Dumping inventory details of IEMS 266

Creating a custom view for the inventory panel 271
Setting custom views for inventory: matching criteria 274
Example for creating a custom view for inventory 277

Working with topologies in Web Client 281

Adding objects to the topology in Web Client 283

Adding platforms using Web Client 285
Adding an MDM platform using Web Client 286
Adding an SPFS platform using Web Client 287

Adding element managers in Web Client 289
Adding an APS Manager using Web Client 290
Adding a CEM using Web Client 292
Adding a CICM Manager using Web Client 293
Adding a CS 2000 Core Manager using Web Client 296
Adding a Fault and Performance Manager using Web Client 299
Adding a GWC Manager using Web Client 301

Copyright © 2006, Nortel Networks

Nortel Networks Confidential

Adding an MCS Manager for MCS/CSE and Media Portal using Web Client 302
Adding an MCS Manager for SSLines using Web Client 305
Adding an MDM using Web Client 308
Adding an MG 9000 Manager using Web Client 311
Adding a SAM21 Manager using Web Client 313
Adding a UAS Manager using Web Client 314
Adding a UNEM using Web Client 316

Adding EMS applications in Web Client 319
Adding an LMM application using Web Client 320
Adding an NPM application using Web Client 321
Adding an OSSGate application using Web Client 322
Adding a QCA using Web Client 323
Adding an SBRM application using Web Client 324
Adding a TMM application using Web Client 325
Adding a Certificate Manager application using Web Client 326

Adding network elements in Web Client 329
Adding a CICM NE using Web Client 330
Adding an Ethernet Routing Switch 8600 NE using Web Client 333
Adding an MAS NE using Web Client 335
Adding an MG 3200 NE using Web Client 338
Adding an MS 2000 NE using Web Client 340
Adding a STORM NE using Web Client 342
Adding an SSTrunks NE using Web Client 345
Adding a USP NE using Web Client 348

Using topology operations in Web Client 351
Editing and viewing object properties using Web Client 352
Using other operations in the Web Client topology 355

Working with the inventory in Web Client 359
Viewing managed object details 360
Navigating the inventory view 361
Searching for objects in the inventory view 363
Adding, modifying, or removing an inventory view 364
Using other operations in the inventory view 366
Configuring traps for SNMP-based devices 368
Description of SNMP attributes 369

Automated backup and restore 371

Copyright © 2006, Nortel Networks

IEMS Configuration

New in this release

Feature changes

There are the following 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 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.

- IEMS supports MDM's security interface changes

  The MDM client is moving from a PAM Radius client to a PAM IS Client. You do not need to configure the Radius secret for (I)SN09 or later versions of MDM.

Introduction

IEMS provides GUIs to perform configuration operations. These tasks can be done from the Java Web Start Client and Web Client GUIs.

Copyright © 2006, Nortel Networks

Nortel Networks Confidential

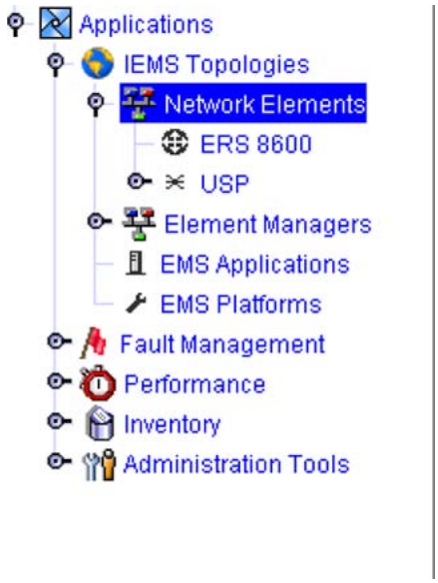
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Working with IEMS topologies in the JWS client

The topology represents the Element Management Systems (EMSs), Network Elements (NEs), platforms, and applications that are being managed by IEMS. A topology node consists of one or more of the following objects:

- symbols that represent managed resources
- topology links that represent the connection between resources
- groups that represent a set of resources grouped logically
- containers that contain resources within them

The IEMS Topologies tree is shown in the following figure:



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

For more information about launching applications from IEMS, about the icons for each object and whether the objects support GUI or command line applications, see "Launching applications from IEMS" in *IEMS Overview*, NN10329-111.

Copyright © 2006, Nortel Networks

Adding objects to topology

This section describes how to add a map symbol from your IEMS Client. A map symbol can be associated with a managed object representing its status. Some objects can be automatically added to the IEMS topology, while others have to be manually added. For details of the mode of discovery for each object, see "Launching applications from IEMS" in *IEMS Overview*, NN10329-111.

Adding a map symbol

Application

Use this procedure to add a map symbol in the IEMS client.

Action

Step	Action
	At the IEMS Client
1	Launch the Add EMS/NE wizard using the menu command **Tools-->Add--><Object to be added>**, where <Object to be added> can be an EMS platform, EMS/NE, or Application.
2	Enter the details of the object added.
3	Click the **Next** button.
4	Enter the fault interface details if any.
5	Click the **Next** button.
6	Enter the performance interface details if any.
7	Click the **Finish** button. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Launching the Add Object wizard

The Add Object wizard can be launched using any of the methods in the following table:

Methods to open the EMS/NE wizard

Managed object to be added	From the menu bar	Shortcut key
Element managers or NEs	Tools-->Add-->EMS/NE	Ctrl+Shift+E
EMS applications	Tools-->Add-->Application	Ctrl+Shift+A
EMS platforms	Tools-->Add-->Platform	Ctrl+Shift+P

Providing object details

The add object wizard allows the addition of an EMS platform, an Element Manager, an EMS application, or an NE to the IEMS topology. The following listing provides descriptions for the required fields that need to be completed.

Field	Description
Host Name/IP Address	The field for the host name or IP address of the element manager.
Time Zone	A list box to select the time zone associated with the object.
Display Name	Enter the display name to be displayed in the topology for the map symbol.
Type	Select the type of object to be added to the database from the list box.

Click the **Next** button to proceed to the Fault Interface details screen.

Providing fault interface details

After providing the object details, the Fault Interface details associated with the object must be provided. If the message stating "No Fault Interface" is displayed, proceed to next step.

The fields in the Details panel change according to the selected object (element manager, EMS, platform, or NE).

Providing performance interface details

The Performance Interface details associated with the object must be provided in the Performance Details of the wizard. If the message stating "No Performance Interface" is displayed, proceed to next step.

The fields in the Performance Interface screen change according to the selected object (element manager, EMS, platform or NE).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Click the **Finish** button to add the required object to the IEMS topology. If successful, the following message is shown in the status bar of the wizard:

If the object host DNS is not resolved, the object is added to the topology with the provided details, and the status bar shows the following message:

If the object is not added in the topology, the status bar of the wizard shows the following message:

If the host name or IP address specified in the Host Name/IP Address field is invalid, the status bar of the wizard shows the following message:

The added object name and its IP address can be viewed in the log messages displayed in the Security Log window invoked through the **Tools** menu command.

If the map symbols are moved in the topology panel, then the objects are added to the same topology panel. The added map symbols may overlap with existing map symbols; hence to rearrange the map symbols properly, select the **View-->Refresh** menu command.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an EMS platform

The Nortel element management systems are deployed in a Nortel platform. IEMS provides an interface to provision and manage these system platforms. This section provides the procedures to add these platforms to the IEMS topology. The platforms that can be managed by IEMS are listed below:

- SPFS
- SDM

The SDM platforms are automatically discovered by IEMS and added to the topology. The discovered SDM platform map symbols can be viewed under **EMS Platforms->SDM** in the IEMS Topologies tree. They can also be viewed by selecting **EMS Platforms** under IEMS Topologies, then right-clicking on the grouped SDM map symbol in the IEMS display panel and selecting **View Children**.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Server Platform Foundation Software (SPFS) platform

Application

Use this procedure to add the SPFS platform to the topology using the IEMS Java Web Start Client.

The SPFS platform is the run-time environment for various Nortel EMSs and applications.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for the SPFS platform in IEMS.

Tasks supported in IEMS for the SPFS platform

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Launching corresponding applications	Yes	No
Security		

Copyright © 2006, Nortel Networks

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Centralized authentication and authorization (RADIUS client)	Yes	No
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->Platform** menu command to invoke the Add Platform wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **SPFS** from the Device Type list box.
5	Select the mode from the Mode list box. If **Simplex** item is selected from Mode list box, perform sub-step step 5 a and proceed to step 6. If **Duplex** item is selected from the Mode list box, follow these steps: a. Enter the IP address of the active unit in the Unit 0 field. b. Enter the IP address of the inactive unit in the Unit 1 field.
6	Select the version of the device from the Device Version list box.
7	Check the Radius Secret field to enable the RADIUS secret password and enter RADIUS secret password in the Radius Secret field. If the Radius Secret field is checked and the password is not entered, the wizard displays "Enter the radius secret" error.
8	Click the **Next** button.
9	Enter the port value **2222** (in which the SPFS communicates with IEMS) in the Port field.
10	Enter the community in the Community field.
11	Select the SNMP version **v2c** from the Version list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

12 Click the **Next** button.

13 Enter the port value `1161` in the Port field.

14 Enter the community in the Community field.

15 Select the SNMP version **v1** from the Version list box.

16 Click the **Finish** button to add the SPFS platform.

Once the SPFS platform is added, a message that reads "Successfully added to database" appears in the status bar.

*The SPFS platform with the specified name is added as a map symbol under the grouped SPFS map symbol in the EMS Platforms display panel. It is also added under **EMS Platforms->SPFS** in the IEMS Topologies tree.*

IEMS correlates events received only from the SPFS SNMP interface. The non-SNMP interfaces such as SYSLOG must be disabled using the "disable local logging" option from CLI. For details, refer to "Disabling local logging of SPFS platform faults" section of *ATM/IP Solution-level Fault Management*, NN10408-900.

17 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a SuperNode Data Manager platform (SDM platform)

IEMS adds the SuperNode Data Manager (SDM) platform automatically when adding the CS 2000 Manager (with the platform as SDM) to the IEMS topology. The SDM platform is added as a map symbol under the grouped SDM map symbol in the EMS Platforms display panel. It is also added under **EMS Platforms->SDM** in the IEMS Topologies tree.

The following list provides the operations available for the SDM platform in the IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	Yes	No
Other operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding element managers

IEMS provides an integration point for the various element managers. It allows a centralized point not only to launch the element managers, but also the ability to view the faults from these systems in a common graphical interface. This section describes how to add the element managers.

When the element managers are added to the IEMS topology, the NEs managed by these element managers are discovered automatically and added to the IEMS topology.

IEMS supports dynamic updates for some of the element managers. The IEMS topology is updated based on the objects managed by the corresponding element managers. IEMS supports dynamic topology updates for the following element managers:

- Audio Provisioning Server Manager
- Universal Audio Server Manager
- GWC Manager

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 an invalid IP address.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an Audio Provisioning Server Manager (APS Manager)

Application

Use this procedure to add the APS Manager to the IEMS topology using the IEMS Java Web Start Client.

The Audio Provisioning Server (APS) is used to provision the encoded mu-law and a-law announcements that the UAS network element plays. On provisioning, the APS Manager IEMS discovers the APS applications configured in the CMT server. After an APS Manager is added to the IEMS topology, the associated APS application is added as a map symbol under the grouped APS map symbol in the EMS Applications display panel. It is also added under **EMS Application->APS** in the IEMS Topologies tree.

The following list provides the operations available for the APS Manager in the IEMS.

Tasks supported in IEMS for APS Manager

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		

Copyright © 2006, Nortel Networks

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard. The IP address must be the primary IP address of the CMT platform.
4	Select **EMS** from the Type list box.
5	Select **APS Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Next** button. *The channel name and the administrator name are displayed in various fields.*
9	Click the **Next** button. *"No Performance Interface" message is displayed.*
10	Click the **Finish** button to add the APS Manager. *Once the APS Manager is added, a message that says "Successfully added to database" appears in the status bar.* *The APS Manager with the specified name is added as a map symbol to the Element Managers display panel. In addition, a topology node named APS Manager with the specified display name*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

in brackets is added under the **Element Managers** *topology node in the IEMS Topologies tree. Also, IEMS automatically discovers the associated APS application and adds it as a map symbol under the grouped APS map symbol in the EMS Applications display panel. IEMS also adds it under* **EMS Application->APS** *in the IEMS Topologies tree.*

You have completed this procedure.

—End—

The APS Manager can be added using the IEMS Web Client. For details, refer to "Adding an APS Manager using Web Client" (page 290) procedure.

Copyright © 2006, Nortel Networks

Adding a Core Element Manager

Application

Use this procedure to add a Core Element Manager (CEM Manager) in IEMS topology.

ATTENTION

If both the CS 2000 Core Manager and CEM Manager are installed, a degradation in the performance of IEMS results and duplicate logs are generated. Either CS 2000 Core Manager or CEM Manager, but not both, should be used to manage the devices.

When CEM is added to the IEMS topology, the CS 2000, CS 2000 Core, MTX (Mobile Telephone Exchange), MSC (Mobile Switching Center), HLR (Home Location Register), and TRI network elements are automatically discovered and added as map symbols under their corresponding grouped map symbol in the Network Elements display panel. They are also added under their corresponding network element under Network Elements in the IEMS Topologies tree.

The Core Element Manager is only supported in wireless markets and available with selected versions of Carrier VoIP platforms. Hence, Core Element Manager is available in selected sites of Carrier VoIP platforms.

The following list provides the operations available for CEM Manager in IEMS.

Tasks supported in IEMS for CEM Manager

Task in IEMS	Availability	
	Java Web Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Client	Web Client
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Prerequisites

Before performing this procedure ensure that the Store and Forward (SAF) process on the SDM/CBM is in service. For more information, see *CS 2000 Core Manager Overview*, NN10018-111.

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **CEM Mgr** from the Device Type list box.
6	Select the associated platform from the Platform list box or retain the default value **None** if it does not belong to any platform.
7	Click the **Next** button. If CS 2000 Manager is already added in the IEMS, the message as in the following screen shot is displayed. If you want to continue, click the **Yes** button.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The CEM Manager port is displayed in the CEM Port field.

8 Click the **Next** button.

A "No Performance Interface" message is displayed.

9 Click the **Finish** button to add the CEM Manager.

Once the CEM Manager is added, a message that says *"Successfully added to database"* appears in the status bar.

The CEM with the specified name is added as a map symbol to the Element Managers topology panel. In addition, a topology node named***Core Element Manager*** with the specified display name in brackets is added under the ***Element Managers*** topology node in the IEMS Topologies tree.

10 If a CS 2000 Core Manager is already installed, remove the CS 2000 Core Manager.

11 You have completed this procedure.

—End—

The CEM can be added using IEMS Web Client. For details, refer to "Adding a CS 2000 Core Manager using Web Client" (page 296) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a CICM Manager

Application

Use this procedure to add the Centrex IP Client Manager (CICM) using IEMS Java Web Start Client. CICM Manager manages CICM NEs.

Only a single pair of CICM Managers must be added on each Carrier VoIP network.

For details to configure SNMP-based devices that are managed by IEMS to send their SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Adding CICM Manager using Java Web Start client

The following list provides the operations available for CICM Manager in IEMS.

Tasks supported in IEMS for CICM Manager

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		

Copyright © 2006, Nortel Networks

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Prerequisites

For IEMS to receive CICM fault and performance data

CICM Manager must be configured to send fault data to IEMS. The CICM has a script called **preboot** which is used to configure the CICM with IEMS server virtual IP address and port for sending the fault data to IEMS; without this configuration, IEMS receives no faults from CICM.

For launching CICM Manager

The prerequisites for launching the CICM Manager are:

- The HTTPS proxy must be configured using the SPFS CLI tool for launching CICM Manager from the IEMS client. To configure the Apache Web Server on an SPFS-based server for the HTTPS proxy, see "Configuring the Apache Web Server for HTTPS proxy" in *Nortel ATM/IP Solution-level Configuration*, NN10409-500. To configure the HTTPS proxy for CICM Manager, refer to *CICM Configuration*, NN10240-511.
- CICM Manager can be launched only in Microsoft Windows with default browser configured as Microsoft Internet Explorer.

Action

Step	Action
	At the IEMS workstation
1	Launch IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *IEMS Overview*, NN10329-111.
2	Select the **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard. In the Carrier VoIP platform HA configuration the host name or IP is the devices primary virtual host name or IP.
4	Select **EMS** from the Type list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Select **CICM Manager** from the Device Type list box.

6 Select the version of the device from the Device Version list box.

7 Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.

8 Select the manager unit mode from the Mode list box. If **Duplex** mode is selected, follow these steps:

If mode selected is	Do
Simplex	follow step 11
Duplex	follow step 9

9 Enter the IP address of Card B host in the Card B IP Address field.

10 Enter the display name of Card B host in the Card B Display Name field.

11 Enter the card location in the Card Location field.

12 Enter the IP address of Card A host in the Card A IP Address field.

13 Go to step 15.

14 Enter the card location in the Card Location field.

15 Click the **Next** button.

16 Enter the port (in which the EMS communicates with IEMS) in the Port field or retain the default value as "161".

17 Enter the community in the Community field.

18 Select the SNMP version from the Version list box. If you select **v3** from the Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoProv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

19 Click the **Next** button.

20 Perform step 16 to step 18.

21 Click the **Finish** button.

Once the CICM Manager is added, a "Successfully added to database" message appears in the status bar.

*The CICM Manager is added as a map symbol to the Element Managers topology panel. In addition, a topology node named **CICM Manager** with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.*

You have completed this procedure.

—End—

The CICM Manager can be added using IEMS Web Client. For details, refer to "Adding a CICM NE using Web Client" (page 330).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Communication Server 2000 Core Manager

Application

Use this procedure to add a Communication Server 2000 (CS 2000) Core Manager to the IEMS topology using the IEMS Java Web Start Client.

The CS 2000 Core Manager residing on the SPFS platform is known as Core Billing Manager (CBM).

CS 2000 Core Manager manages CS 2000 Core and Call Agent Core NEs.

Configuring the CS 2000 Core Manager logroute

While configuring the CS 2000 Core Manager logroute, ensure the following:

- Logroute on the associated SDM must be configured for TCPIN.
- Logroute on the associated SDM must be configured with ECORE set to OFF.
- Logroute on a CS 2000 Core Manager with a pre SDM20 software load version: the associated SDM log format must be set to STD or SCC2.
- Logroute on a CS 2000 Core Manager with a SDM20 or greater software load version: the associated SDM log format must be set to STD_OLD or SCC2_OLD.
- Logroute on a CS 2000 Core Manager residing on the SPFS platform or CBM, the associated log format must be set to SCC2 (not NTSTD).
- Logroute on a CS 2000 Core Manager residing on a SDM/CBM must be set to SCC2 (not NTSTD) as the associated log format.

Configuring the log format

The end of log format for the NTSTD and SCC2 feeds can be configured in IEMS by modifying the MLDefaultParams.xml file under the /opt/nortel/iems/current/conf folder. The SCC2 end of log format is specified in "SCC2_MESSAGE ENDOFLOG" parameter and NTSTD end of log format is specified in "NTSTD_MESSAGE ENDOFLOG" parameter. The end of log format must be using the X character format and be separated with colon (":"). The default end of log format values in MLDefaultParams.xml file are:

- SCC2_MESSAGE ENDOFLOG="0A:0D:20:0A:0D"
- NTSTD_MESSAGE ENDOFLOG="0A:19:0A:0D"

If the end of log format is changed in the MLDefaultParams.conf, the IEMS server requires restart to reflect the changes.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

IEMS polls periodically to check the CS 2000 platform object status. If the data is not received between two status polls, IEMS disconnects and reconnects the CS 2000 Core Manager. If the reconnect attempt raises an error, the CS 2000 Core Manager and its corresponding components turn to an unknown object status in IEMS. The map symbols of these objects will turn to a gray background.

It is suggested that the polling interval for the CS 2000 Core Manager object in IEMS retains (or is left near to) the default value (300 seconds). Reducing this significantly can result in frequent and unnecessary attempts to reconnect to the CS 2000 Core Manager fault feed.

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

The following list provides the operations available for CS 2000 Core Manager in IEMS.

Tasks supported in IEMS for CS 2000 Core Manager

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events	Yes	Yes
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **CS2K Core Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Select the NE type **CS 2000 Core** or **Call Agent Core** from the Managing NE Type list box. By default, "CS 2000 Core" is selected in the list box. If you select CS 2000 Core from the Managing NE Type list box, enter the CS 2000 Core device IP address in the CS 2000 Core IP Address field. If you select Call Agent Core from the Managing NE Type list box, follow these steps: a. Select the mode from the Mode list box. If "Duplex" item is selected, perform sub-step b and proceed to step 10. b. Type the valid IP address of the active unit in the Active Unit IP field. c. Type the valid IP address of the inactive unit in the Inactive Unit IP field.
9	Enter the display for the NE in the NE Display Name editable list box or select a value from the NE Display Name editable list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 Check the **Radius Secret** checkbox to enable the RADIUS secret password and enter RADIUS secret password in the Radius Secret field.

If the Radius Secret field is checked and the password is not entered, the wizard displays "Enter the radius secret" error.
To configure Radius Secret refer to:

- *IEMS Administration and Security*, NN10336-611
- *ATM/IP Solution-Level Administration and Security*, NN10402-600.

11 Click the **Next** button.

If CEM is already added in the IEMS, the message as in the following screen shot is displayed. If you want to continue, click the **Yes** button.

12 Refer to Configuring the CS 2000 Core Manager logroute. Check the **NTSTD Port** or **SCC2 Port** and change the Port (if required).

13 Click the **Next** button.

A "No Performance Interface" message is displayed.

14 Click the **Finish** button to add the CS 2000 Core Manager.

Once the CS 2000 Core Manager is added, a message that reads "Successfully added to database" appears in the status bar.

*The CS 2000 Core Manager with the specified name is added as a map symbol to the Element Managers topology panel. In addition, a topology node named **CS 2000 Manager** with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.*

*If you selected NE type **Call Agent Core** from the Managing NE Type list box, the Call Agent Core NE is discovered and the corresponding Call Agent platform is discovered automatically and added. The Call Agent Core NE node is added in the Call Agent Core topology node (under the Networks Elements node) in the IEMS Topologies tree. The Call Agent platform is added in the Call Agent Platform topology node (under the Networks Elements-->Call Agent Core node) in the IEMS Topologies tree.*

You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

The CS 2000 Manager can be added using IEMS Web Client. For details, refer to "Adding a CS 2000 Core Manager using Web Client" (page 296) procedure.

Copyright © 2006, Nortel Networks

Adding a Fault and Performance Manager

Application

Use this procedure to add the Fault and Performance Manager (FPM) to the IEMS topology using IEMS Java Web Start Client.

The FPM can be added using IEMS Web Client. For details, refer to ""Adding a Fault and Performance Manager using Web Client" (page 299)".

The following list provides the operations available for FPM in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Prerequisites

To add an FPM, the corresponding MCS Manager must be added to the IEMS topology.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** dialog.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **FPM Mgr** from the Device Type list box.
6	Select the version in the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	From the MCS Managers list box, select the MCS Manager to which the FPM corresponds.
9	Select the mode of the device from the Mode list box. If **Duplex** mode is selected, enter the primary IP address and secondary IP address in the Instance 0 and Instance 1 fields respectively.
10	Enter the user name of the device in the User Name field.
11	Click the **Next** button.
12	Enter the port value through which the EMS communicates with IEMS in the Port field. The port value is <FPM device base port number>+17. For example, if the FPM device port is 65400, then the port number is 65417.
13	Enter the community in the Community field.
14	Select the SNMP version **v2c** from the Version list box. The port value and SNMP version are dependent on the FPM configuration which is added.
15	Click the **Next** button.
16	In the Directory Name field, enter the directory name where the CSV file is present in the device.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Wildcard support is available for this field. In general, the FPM operational measurement (OM) files resides in "/var/mcp/oss/om/MCP_4.0/<fault-performance manager instance id>/<network element instance id>/<file format option name>" folder.

Example

"/var/mcp/oss/om/MCP_4.0/FPM1_0/*/csv-file" where * is a wildcard representing "network element instance ID".

If the FPM is in duplex mode, then the performance data collection jobs should continue and the OM files should be collected from the currently active physical unit IP. The OM directory path for the two physical units are different and hence when a SWACT takes place in the FPM host, the directory from which the OM files should be collected will differ. As only one path can be given when configuring the FPM, the wildcard * can be used when specifying the directory path so that the different directory paths in the units are handled. This way, collection of the OM files can happen even after a SWACT had taken place.

Example

"/var/mcp/oss/om/MCP_4.0/FPM1_*/*/csv-file"

17 In the File Name field, enter the file mask of the CSV file present in the device.

Wildcard support is available for this field.

Example

If the file names start with "CSVOM" string, you can enter the value "CSVOM*.csv".

18 Enter the user name for SFTP-PULL in the User ID field.

19 Enter the password in the Password field.

20 Click the **Finish** button to add the FPM.

Once the FPM is added, a message appears in the status bar as shown below:

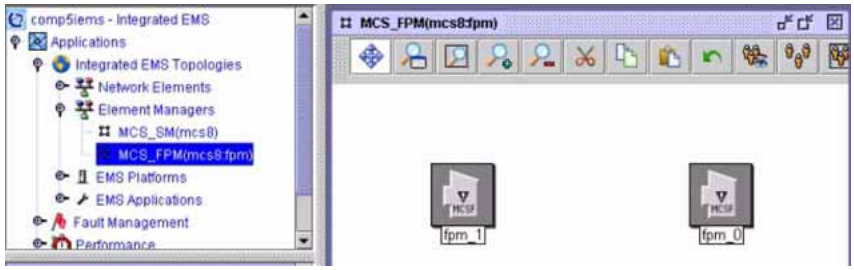
*The FPM with the specified display name is added as a map symbol to the **Element Managers** topology panel. A topology node named MCS_FPM with the parent MCS and FPM display name in brackets is added under the Element Managers topology node in the IEMS tree. If the duplex mode is selected while adding the FPM, you can find the primary and secondary units added in this MCS_FPM (<MCS display name>:<FPM display name>) node similar to the following figure.*

Example

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

mcs8:fpm as in the following figure.

This also applies to the Web Client.



You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks

Nortel Networks Confidential

Adding a Gateway Controller Manager

Application

Use this procedure to add the Gateway Controller (GWC) Manager to the IEMS topology using IEMS Java Web Start Client.

The GWC Manager manages GWC NEs. After a GWC Manager is added to the IEMS topology, each NE managed by that GWC Manager is discovered automatically and added as a map symbol under the grouped GWC map symbol in the Network Elements display panel. They are also added under **Network Elements->GWC** in the IEMS Topologies tree..

The following list provides the operations available for GWC Manager in IEMS.

Tasks supported in IEMS for GWC Manager

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **GWC Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value **None** if it does not belong to any platform.
8	Click the **Next** button. *The channel name and the administrator name are displayed in various fields.*
9	Click the **Next** button. *A "No Performance Interface" message is displayed.* The performance interface details for GWC NEs are taken by default in IEMS. The default values are listed below: • SNMP version = v2c • SNMP community = public • SNMP port = 161
10	Click the **Finish** button to add the GWC Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Once the GWC Manager is added, a message that says "Successfully added to database" appears in the status bar as shown below:

The GWC Manager with the specified name is added as a map symbol to the Element Managers topology panel. In addition, a topology node named GWC Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.

You have completed this procedure.

—End—

The GWC Manager can be added using IEMS Web Client. For details, refer to "Adding a GWC Manager using Web Client" (page 301) procedure.

Copyright © 2006, Nortel Networks

Adding an MCS/CSE Manager for MCS/CSE and Media Portal

Application

Use this procedure to add the Multimedia Communication Server Manager (MCS Manager) to the IEMS topology using IEMS Java Web Start Client. The MCS Manager is also known as the MCS System Manager (MCS SM) or MCS 5200.

The MCS Manager can be added using IEMS Web Client. For details, refer to "Adding an MCS Manager for MCS/CSE and Media Portal using Web Client" (page 302).

When you add an MCS Manager, the following changes are made in the IEMS display:

- the MCS Manager is added as a node under the Element Managers node in the IEMS Topologies tree (MCS_SM<display name>)
- the MCS Manager is added in simplex mode as a map symbol to the Element Managers topology panel (MCS icon with display name)
- the MCS Manager is added in duplex mode as map symbols for the primary and secondary SM servers (<MCS Manager display name>_0 and <MCS Manager display name>_1)
- the MCS 5200 or RTP Media Portal NE is added as a node under the Network Elements node in the IEMS Topologies tree (MCS 5200 or RTP Media Portal)
- the MCS 5200 or RTP Media Portal NE is added as a map symbol to the Element Managers topology panel (MCS icon<parent Element Manager display name>)

When adding MCS Manager 7.0 in IEMS, both the active and inactive MCS Managers must be added as separate objects in the IEMS topology. The logical IP address of the active or inactive MCS Manager host must be entered in the **Host Name/IP Address** of Add EMS/NE wizard.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The following list provides the operations available for MCS Manager in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Prerequisites

The following sections list the MCS Manager configuration references required to integrate with the IEMS.

Fault interface

Refer to "SNMP information" and "Configuring an SNMP Manager" in *System Manager Overview*, NN10030-111. The MCS SNMP trap destination must be configured in the device for the IEMS to manage its fault interface.

Configuration interface

No additional configuration is required.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Performance management

No additional configuration is required.

Security configuration

No additional configuration is required.

MCS Client launch

MCS client launch is available only on a PC that has MCS software installed. For details of how to install the software, refer to *MCS System Management Console User Guide*, NN10247-111. MCS Client software can be launched only in Microsoft Windows platforms.

The requirements for launching the MCP Management Console from the MCS system manager are:

- The client workstation must have the correct JRE version installed. For details, see "System requirements" in *IEMS Overview*, NN10329-111.
- The MCP System Management Console can be launched only for Microsoft Windows platform-based client workstations.

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 **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** dialog.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **EMS** from the Type list box.
5	Select **MCS Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Select the NE type from the Managing NE Type list box. By default, **MCS/CSE MX** is selected in the list box.
9	Select the mode of the device from the Mode list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If **Duplex** mode is selected, enter the primary IP address and secondary IP address in the Instance 0 and Instance 1 fields respectively.

10 Enter the user name of the device in the User Name field.

11 Click the **Next** button.

12 In the Port field, enter the port value (through which the EMS communicates with IEMS). For details see "Configuring traps for SNMP-based devices" (page 368).

13 Enter the community in the Community field.

14 Select the SNMP version **v2c** from the Version list box.

The port value and the SNMP version are dependent on the MCS Manager configuration that is added.

15 Click the **Next** button.

16 In the Directory Name field, enter the directory name where the CSV file is present in the device.

For MCS Manager 4.0, wildcard support is available for this field. In general, the MCS System Manager operational measurement (OM) files resides in "/var/mcp/oss/om/MCP_4.0/<fault-performance manager instance ID>/<network element instance ID>/<file format option name>" folder.

Example

"/var/mcp/oss/om/MCP_4.0/SM_0/*/csv/" where * is a wildcard representing "network element instance ID".

If the MCS System Manager is in duplex mode, then the performance data collection jobs continue and the OM files are collected from the currently active logical unit IP. The OM directory path for the two logical units are different and hence when a SWACT takes place in the MCS System Manager host, the directory from which the OM files are collected differs. As only one path can be given when configuring the MCS System Manager, the wildcard * can be used when specifying the directory path so that the different directory paths in the units are handled. In this way, collection of the OM files can happen even after a SWACT has taken place.

Example

"/var/mcp/oss/om/MCP_4.0/FPM1_*/*/csv-file"

Performance metrics are collected from both servers during a SWACT.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

17 In the File Name field, enter the file mask of the CSV file present in the device.

Wildcard support is available for this field.

Example

If the file names start with "CSVOM" string, you can enter the value "CSVOM*.closed".

18 Enter the user name for SFTP-PULL account in the User ID field.

19 Enter the password in the Password field.

20 Click the **Finish** button to add the MCS Manager.

Once the MCS Manager is added, a *"Successfully added to database"* message appears in the status bar.

After adding an MCS Manager, the fault interface and performance details are associated to corresponding logical SM servers that are added in the MCS SM(XXX) node (MCS SM node with the parent MCS Manager display name) under the Element Managers topology. The fault interface and performance details can be modified for the MCS Manager map symbol in the Element Managers topology.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MCS Manager for SSLines

Application

Use this procedure to add an MCS Manager for SSLines to the IEMS topology using IEMS Java Web Start Client.

The MCS Manager for SSLines can be added using IEMS Web Client. For details, refer to "Adding an MCS Manager for SSLines using Web Client" (page 305).

MCS Manager for SSLines manages SSLines NEs. When you add an MCS Manager for SSLines, the associated SSLines is added as a map symbol under the grouped SSLines map symbol in the Network Elements display panel. Also, an SSLines NE is added under **Network Elements->SSLines** in the IEMS Topologies tree. The MCS Manager for SSLines is added as a logical system manager server map symbol in the Element Managers topology. The logical MCS system managers (SM) are added as map symbols in the MCS SM topology (with the parent SSLines display name in brackets).

When adding an MCS Manager for SSLines in IEMS, both the active and inactive MCS Managers must be added as separate objects in the IEMS topology. The logical IP address of the active or inactive MCS Manager host must be entered in the **Host Name/IP Address** of the Add EMS/NE wizard.

The following list provides the operations available for the MCS Manager for SSLines in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Prerequisites

The following sections list the MCS Manager configuration references required to integrate with the IEMS.

Fault interface

Refer to "SNMP information" and "Configuring an SNMP Manager" in *Nortel System Manager Fundamentals*, NN10030-111. The MCS SNMP trap destination must be configured in the device for the IEMS to manage its fault interface.

Configuration interface

To configure the Apache Web Server on an SPFS-based server for HTTPS proxy, see "Configuring the Apache Web Server for HTTPS proxy" in *ATM/IP Solution-level Configuration*, NN10409-500.

To configure the HTTPS proxy for SSLines, see *Session Server Lines - SIP Voice Basics*, NN10437-111.

Performance management

No additional configuration is required.

Security configuration

No additional configuration is required.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

MCS Client launch

MCS client launch is available only on a PC that has MCS software installed. For details of how to install the software, refer to *Nortel System Management Console User Guide*, NN10247-111. MCS Client software can be launched only in Microsoft Windows platforms.

The requirements for launching the MCP Management Console from the MCS system manager are:

- The client workstation must have the correct JRE version installed. For details, see "System requirements" in *IEMS Overview*, NN10329-111.
- The MCP System Management Console can be launched only for Microsoft Windows platform-based client workstations.

To launch the MCP Provisioning Client from the Element Manager for SSLines, you must configure the IEMS with the IP addresses for the provisioning servers. Refer to "Configuring provisioning clients" (page 58).

To launch the Session and System Manager Command Line from the Element Manager for SSLines, you must configure the IEMS with the IP addresses for the Session Manager and System Manager servers. Refer to "Configuring Session Managers for SSH launch" (page 56).

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 **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** dialog.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **EMS** from the Type list box.
5	Select **SSLines Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Enter the primary IP address and secondary IP address in the Instance 0 and Instance 1 fields respectively.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

9 Enter the user name of the device in the User Name field.

10 Click the **Next** button.

11 In the Port field, enter the port value (through which the EMS communicates with IEMS). For details see SNMP Information in *Nortel System Manager Fundamentals*, NN10030-111.

12 Enter the community in the Community field.

13 Select the SNMP version **v2c** from the Version list box.

The port value and the SNMP version are dependent on the MCS Manager for SSLines configuration that is added.

14 Click the **Next** button.

15 In the Directory Name field, enter the directory name where the CSV file is present in the device.

For MCS Manager for SSLines, wildcard support is available for this field. In general, the MCS System Manager operational measurement (OM) files resides in the /var/mcp/oss/om/MCP_<release_number>/SM_*/*/csv folder.

Example

/var/mcp/oss/om/MCP_9.1/SM_*/*/csv/" where * is a wildcard representing "network element instance ID".

If the MCS System Manager is in duplex mode, then the performance data collection jobs should continue and the OM files should be collected from the currently active logical unit IP. The OM directory path for the two logical units are different and hence when a SWACT takes place in the MCS System Manager host, the directory from which the OM files should be collected will differ. As only one path can be given when configuring the MCS System Manager, the wildcard * can be used when specifying the directory path so that the different directory paths in the units are handled. In this way, collection of the OM files can happen even after a SWACT had taken place.

Example

/var/mcp/oss/om/MCP_9.1/FPM1_*/*/csv-file

Performance metrics will be collected from both servers during a SWACT.

16 In the File Name field, enter the file mask of the CSV file present in the device.

Wildcard support is available for this field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Example

If the file names start with "CSVOM" string, you can enter the value *.closed.

17 Enter the user name for SFTP-PULL account in the User ID field.

18 Enter the password in the Password field.

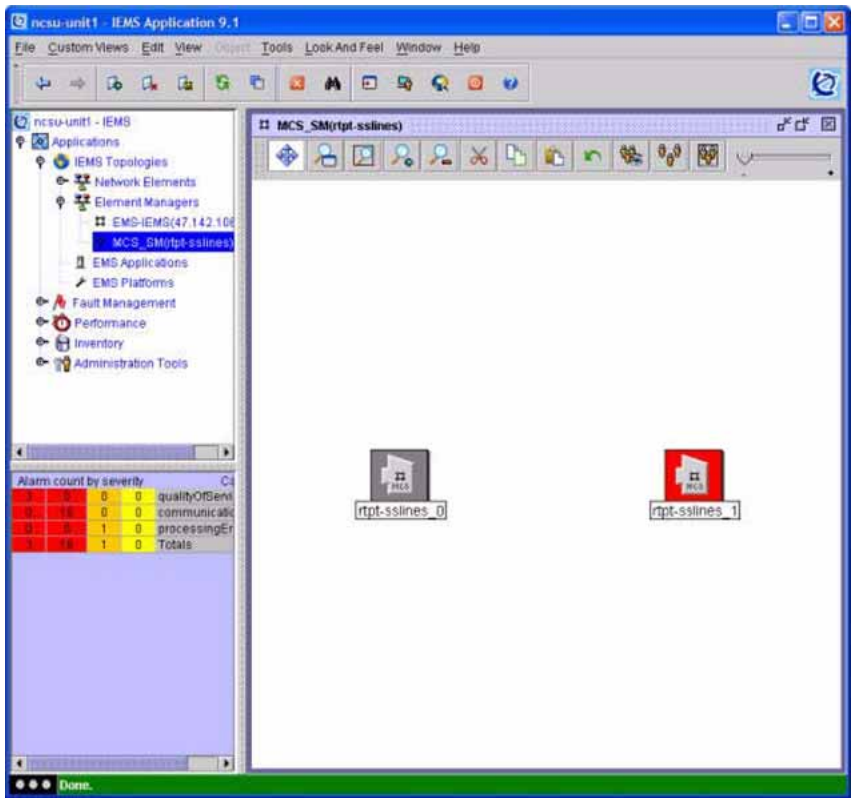
19 Click the **Finish** button to add the MCS Manager for SSLines.

Once the MCS Manager for SSLines is added, a "Successfully added to database" message appears in the status bar.

After adding an MCS Manager for SSLines, the fault interface and performance details are associated to corresponding logical SM servers that are added in the MCS SM(XXX) node (MCS SM node with the parent SSLines display name) under the Element Managers topology. The fault interface and performance details can be modified for MCS Manager map symbol in the Element Managers topology.

The MCS Manager with the specified name is added as a logical SM server map symbol to the Element Managers topology panel. The MCS SM (with the specified SSLines display name in brackets) is added under the Element Managers topology node of the IEMS Topologies tree. The logical MCS SM servers are added as map symbols in the topology node named ***MCS SM(XXXSSLines)*** *(with the specified display name in brackets). When adding an MCS Manager in duplex mode, the primary and secondary logical SM servers are added as map symbols in the MCS SM(XXXSSLines) node present under the Element Managers topology node of the IEMS Topologies tree similar to the following screen shot.*

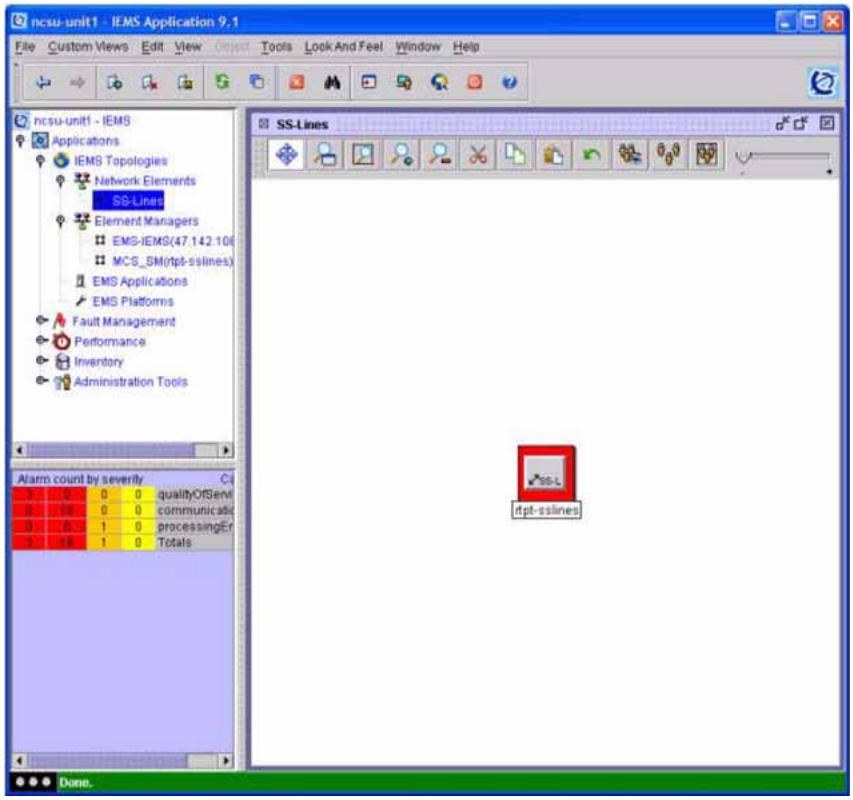
Copyright © 2006, Nortel Networks



The primary and secondary logical SM server map symbols display names are "<MCS Manager for SSLines display name>_0" and "<MCS Manager for SSLines display name>_1" respectively (similar to the preceding screen shot).

The SSLines NE added under the Network Elements node is similar to the following screen shot:

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



This also applies to the Web Client.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks

Nortel Networks Confidential

Configuring Session Managers for SSH launch

Application

Use this procedure to configure the Session Managers Platform Command Line for SSH launch.

After you configure the IEMS with the IP addresses for the Session Manager and System Manager servers, you can use SSH to launch the Session and System Manager Command Line from the element manager for SSLines. Refer to Launching applications for MCS Manager in *IEMS Overview*, NN10329-111.

Prerequisites

Only the Session Managers that have been previously configured with IP addresses can be used in this procedure and added to the IEMS database.

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 **MCS_SM** under **Element Managers** in the IEMS tree and right-click the MCS_SM map symbol for SSLines.
3	Select the **Configure Session Mgr Platform Command Line Launch** tool. *The Configure Session Mgr Platform Command Line dialog appears.*
4	Click the **Add Session Manager** button. *The IP address pairs for Session Managers that have been previously configured with IP addresses are displayed.* If Session Managers have not been configured, one pair of IP addresses with blank values is displayed.
5	Select the Session Manager pair. *The IP address pair appears in the Configure Session Managers dialog.* You can configure up to three Session Manager pairs.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

6 Select your next step.

If you want to	Do
add another IP pair	steps 7 and 8
remove an IP pair	step 10
configure the IP pair	step 12

7 To add another IP pair, click the **Add Session Manager** button.

One pair of Session Managers is displayed.

8 Select the Session Manager pair.

The IP address pair appears in the Configure Session Managers dialog.

9 Go to step 13.

10 To remove an IP pair, click the **Remove Session Manager** button.

The bottom pair is removed from the list.

11 Go to step 13.

12 Click the **OK** button.

The configuration is sent to the server.

13 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring provisioning clients

Application

Use this procedure to configure provisioning clients.

After you configure the IEMS with the IP addresses for the provisioning servers, you can launch the MCP Provisioning Client from the element manager for SSLines.

To launch the MCP Provisioning Client, refer to Launching applications for MCS Manager in *IEMS Overview*, NN10329-111.

Prerequisites

To configure Provisioning Clients, you must:

- add an SSLines Manager, refer to "Adding an MCS Manager for SSLines" (page 49).
- know the IP addresses for the provisioning servers.

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 **MCS_SM** under **Element Managers** in the IEMS tree and right-click the MCS_SM map symbol for SSLines.
3	Select the **Configure Provisioning Clients** tool. *The Configure Provisioning Clients dialog appears.*
4	Enter the IP addresses of the provisioning servers.
5	Click the **OK** button. *After the IP addresses are configured, a dialog appears.* `Configure Provisioning Clients Succeeded. Please restart WEBSERVER to have changes take effect.`
6	Click the **OK** button.
7	On the SPFS platform, restart the WEBSERVER by typing **`servrestart WEBSERVER`**

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

8 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Multiservice Data Manager

Application

Use this procedure to add a Multiservice Data Manager (MDM) using IEMS Java Web Start Client.

When an MDM is added to the topology, the associated Media Gateway 7480/15000/20000 and MSS 15000 NEs are discovered by IEMS and are each added as a map symbol under their corresponding grouped map symbol in the Network Elements display panel. Also, each MG 7480/15000/20000 and MSS 15000 NEs is added under its corresponding NE under **Network Elements** in the IEMS Topologies tree.

Adding an MDM using Java Web Start Client

The following list provides the operations available for MDM in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other applications		
Launching corresponding applications	Yes	No

Prerequisites

Determine the associated MDM platform before performing this procedure. See "Determining the associated MDM platform" (page 65).

Requirements for launching MDM

The requirements for launching the MDM are as follows:

- MDM launch on a UNIX platform requires the user to log in to the MDM GUI Server UNIX shell. For details on how to launch the client GUI, refer to the *MDM Installer Guide*, 241-6001-100.
- MDM launch on a PC requires a UNIX emulation package such as Exceed. For information on installing and configuring Exceed refer to Exceed documentation. For details of the specific command used to launch via Exceed, refer to the *MDM Installer guide*, NN2416001-100 and the *MDM Customization Administrator guide*, NN2416001-301.
- The X11 Client launch requires X server needs to be run in the client machine. In the case of Solaris/Linux, Xserver runs by default. In the case of Windows, Hummingbird or Exceed is used as Xserver.
- To launch MDM Manager or X11 Client, the client-server IP address must be provisioned. Refer to "Provisioning client-server IP address for MDM Manager" in Launching applications for MDM in *IEMS Overview*, NN10329-111.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to "Launching the IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Select the **Tools-->Add-->EMS/NE** menu command. *The Add EMS/NE wizard opens.*
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Select **MDM** from the Device Type list box.

6 Select the version of the device from the Device Version list box.

7 Based on the platform determined in "Determining the associated MDM platform" (page 65), select the associated platform from the Platform list box. If the associated platform is SPFS, select the specific SPFS platform from the drop-down list.

8 Select the manager unit mode from the Mode list box.

(The MDM application can run in a simplex or duplex mode. In the simplex mode, MDM application is configured in one machine while in the duplex mode the application is configured to run in two machines. In the duplex mode, when the current machine is down, the IEMS switches over to the alternate [or secondary] machine).

If the mode is	Do
simplex	follow step 10 to step 14 and proceed to step 17
duplex	follow step 9 to step 20

9 In the Unit 1 IP Address/Host Name field, enter the secondary machine IP address in which the MDM application has to run.

Do not specify the IP address 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 an invalid IP address.

10 Click the **Next** button.

The Configure MDM Centralized Account dialog box opens.

11 Enter the user name and password in the Configure MDM Centralized Account dialog box for the centralized account common to all MDM devices.

The user name entered in Configure MDM Centralized Account dialog must be an user belonging to the "emsadm" group.

The centralized account screen is displayed only the first time an MDM device is added to the IEMS. You can change the centralized account user name and password at any time using procedure "Changing the MDM centralized security account Information".

12 Click the **OK** button.

13 In the Port field of the Primary panel, enter the port in which log messages are sent by the MDM element manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

14 Enter the user identification in the User ID field of the Primary panel.

15 In the Port field of the Secondary panel, enter the port in which log messages are sent by MDM element manager.

16 Enter the user identification in the User ID field of the Secondary panel.

17 Click the **Next** button.

18 Enter the port in the Five Min Collection Port field.

(The port configured in this field is scheduled to collect data every five minutes from the NEs [managed by the MDM application]. The default port is 1646).

19 Enter the port in the Thirty Min Collection Port field. (The port configured in this field is scheduled to collect data every thirty minutes from the NEs [managed by the MDM application]. The default port is 1647).

20 Click the **Finish** button. This adds the MDM with the provided details.

Once the MDM is added, a "Successfully added to database" message appears in the status bar. The MDM with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named MDM with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.

If an MDM is added in duplex mode, then map symbols of both the primary and secondary MDM units are displayed in the corresponding MDM panel. The added units can be identified by the display name which is appended with Unit-0 for the primary unit and Unit-1 for the secondary unit.

All the MG 7480/15000/20000 and MSS 15000 NEs managed by the added MDM application are added as map symbols under the Network Elements topology node. The VSP cards that are automatically discovered by MDM are added as map symbols in the corresponding topology nodes under the MG 7480/15000/20000 node. The NEs unknown to MDM are added under the MSS/MG Unknown node.

For the NEs and MDM automatically discovered by MDM, the display name of the map symbol is appended with the parent MDM name in brackets.

21 After the MDM is added, provision the client-server IP address. For details see "Launching applications for MDM" in *IEMS Overview*, NN10329-111.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

22 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks

Determining the associated MDM platform

Application

Use this procedure to determine the associated Multiservice Data Manager (MDM) platform before adding an MDM to the IEMS topology.

Understanding the underlying platform for MDM

Before you add an MDM device to the topology, it is important to first determine the associated platform of this MDM

The following table shows the possible options for associated platforms for an MDM device depending on its device version.

Support platform		
MDM device version	**MDM platform**	**SPFS platform**
(I)SN08	supported	not supported
(I)SN09U	supported	supported

For a MDM device associated with a MDM platform, the IEMS creates the associated MDM platform automatically when the MDM is added to IEMS inventory.

For a MDM device associated with a SPFS platform, the following actions are necessary before adding this MDM to IEMS:

- On the IEMS, manually add the associated SPFS platform to IEMS topology.
- On SPFS, manually configure the SPFS platform to send SNMP traps to the IEMS.
- On SPFS, disable the local non-SNMP interfaces for the SPFS platform.

Prerequisites

No prerequisites are required to perform this procedure.

Action

Step	Action
	At the IEMS workstation
1	Log into the MDM server.
2	Telnet to the active server by typing `> telnet <server>`

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

and pressing the Enter key.

where

server is the IP address or host name of the MDM server.

3 When prompted, enter your user ID and password.

4 Type the following to determine the MDM platform:

```
echo $SSPFS_VERSION
```

and pressing the Enter key.

5 Select your next step according to the response.

If the response is	Do
SSPFS_VERSION: Undefined variable	The MDM is associated with the MDM platform. Go to the next step.
09.0 or 09.1	The MDM is associated with an SPFS platform. Go to step 8.

6 The MDM is associated with the MDM platform. This platform is automatically added when the MDM is added to the IEMS topology.

7 You have completed this procedure. To add the MDM, see Adding a Multiservice Data Manager.

8 On the IEMS, manually add the associated SPFS platform to the IEMS topology. For details, see "Adding a Server Platform Foundation Software (SPFS) platform" (page 16). If the MDM is simplex, add a simplex SPFS platform. Otherwise, if the MDM is duplex, add a duplex SPFS platform where the IP addresses of unit 0 and unit 1 of the SPFS platform correspond to the IP addresses of unit 0 and unit 1 of the MDM.

9 On SPFS, manually configure the SPFS platform to send SNMP traps to the IEMS. For details refer to "Configuring traps for SNMP-based devices" (page 368).

10 On SPFS, disable the local non-SNMP interfaces for the SPFS platform. For details, refer to "Disabling local logging of SPFS platform faults" in *ATM/IP Solution level Fault Management* NN01408-900.

11 You have completed this procedure.

To add the MDM to the IEMS topology, see Adding a Multiservice Data Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Multiservice Gateway 9000 Manager

Application

Use this procedure to add a Multiservice Gateway 9000 (MG 9000) Manager to the IEMS topology using the IEMS Java Web Start Client.

Multiservice Gateway 9000 (MG 9000) Manager manages MG 9000 NEs. After adding an MG 9000 Manager to the IEMS topology, the NEs managed by the MG 9000 Manager are automatically discovered and added as map symbols under the grouped MG9K map symbol in the Network Elements display panel, and also under **Network Elements->MG9K** in the IEMS Topologies tree.

The following list provides the operations available for MG 9000 Manager in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

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 **Tool-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **EMS** from the Type list box.
5	Select **MG9K Mgr** from the Device Type list box.
6	Select the associated platform from the Platform list box or retain the default value **None** if it does not belong to any platform.
7	Select the version of the device from the Device Version list box.
8	Enter the valid IP address in MG9K Mid Tier IP field. The IP address of the Mid Tier existing between IEMS and MG 9000 Manager must be provided here.
9	Click the **Next** button. *The channel name and the administrator name are displayed in various fields.*
10	Enter the valid subnet value with version in the **Subnet (with version)** field.
11	Click the **Next** button.
12	Enter the user name for SFTP-PULL in the User ID field.
13	Enter the password in the Password field.
14	Click the **Finish** button to add the MG 9000 Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Once the MG 9000 Manager is added, a message that reads "Successfully added to database" appears in the status bar.

The MG 9000 Manager with the specified name is added as a map symbol to the Element Managers topology panel. In addition, a topology node named MG 9000 Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.

You have completed this procedure.

—End—

The MG 9000 Manager can be added using IEMS Web Client. For details, refer to "Adding an MG 9000 Manager using Web Client" (page 311) procedure.

Copyright © 2006, Nortel Networks

Adding a SAM21 Manager

Application

Use this procedure to add a SAM21 Manager to the IEMS topology using the IEMS Java Web Start Client.

SAM21 is the acronym for Services Application Module, 21 slot. The SAM21 Manager manages SAM21 NEs. After a SAM21 Manager is added to the IEMS topology, the associated NEs managed by that SAM21 Manager are discovered automatically and added as map symbols under the grouped SAM21 map symbol in the Network Elements display panel, and also under **Network Elements->SAM21** in the IEMS Topologies tree. In addition, the SAM21 Cards are discovered automatically and added under the corresponding SAM21NEs. Refer to the "Viewing the SAM21 cards" (page 243) procedure to view the SAM21 cards.

The following list provides the operations available for a SAM21 Manager in IEMS.

Tasks supported in IEMS for a SAM21 Manager

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		

Copyright © 2006, Nortel Networks

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **SAM21 Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Next** button. *In the Syslog Details panel, a list of fields is displayed showing the location of various log files such as Customer Log File, Audit Log File, and Security Log File.*
9	Click the **Next** button. *A "No Performance Interface" message is displayed.* The performance interface details for SAM21 NEs are taken by default in IEMS. The default values are listed below: • SNMP version = v2c • SNMP community = public • SNMP port = 161

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 Click the **Finish** button to add the SAM21 Manager.

Once the SAM21 Manager is added, a message that says "Successfully added to database" appears in the status bar.

*The SAM21 Manager with the specified name is added as a map symbol to the Element Managers topology panel. In addition, a topology node named **SAM21 Manager** with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.*

You have completed this procedure.

—End—

The SAM21 Manager can be added using IEMS Web Client. For details, refer to "Adding a SAM21 Manager using Web Client" (page 313) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a UMUX Network Element Manager

Application

Use this procedure to add the UMUX Network Element Manager (UNEM) to the IEMS topology using the IEMS Java Web Start Client.

UNEM manages UMUX 1500, UMUX 1200, and UMUX 900 NEs in the Universal Multiplexer (UMUX) network. When you add an UNEM, the managed NEs are automatically discovered and added as map symbols under the grouped UMUX-1500, UMUX1200, and UMUX-900 map symbols respectively in the Network Elements display panel. Also, they are added under **Network Elements->UMUX-1500, UMUX-1200**, and **UMUX-900** respectively in the IEMS Topologies tree. The UNEM is added as a map symbol in the Element Managers topology. Also, the UNEM is added as map symbols in the EMS-UNEM-Mgr topology (with added UNEM display name in brackets).

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Creating a CEM managed node instance" (page 216).

The following list provides the operations available for UNEM in IEMS.

Tasks supported in IEMS for UNEM

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE dialog.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **UNEM** from the Device Type list box.
6	Select the SSH enabled field if the SSH is enabled in the UNEM device.
7	Click the **Next** button.
8	In the Port field, enter the port value (in which the EMS communicates with IEMS).
9	Enter the community in the Community field.
10	Select the SNMP version **v1** from the Version list box. The port value and the SNMP version are dependent on the UNEM configuration that is added.
11	Click the **Next** button.
12	Click the **Finish** button to add the UNEM.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Once the UNEM is added, a message that says "Successfully added to database" appears in the status bar.

The UNEM with the specified name is added to the Element Managers topology panel. Also, the UNEM is added as map symbols in the topology node named EMS-UNEM-Mgr (with the specified display name in brackets).

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Universal Audio Server Manager

Application

Use this procedure to add the Universal Audio Server (UAS) Manager to the IEMS topology using the IEMS Java Web Start Client.

The UAS Manager manages UAS NEs. After a UAS Manager is added to the IEMS topology, the associated NEs managed by that UAS Manager are discovered automatically and added as map symbols under the grouped UAS map symbol in the Network Elements display panel, and also under **Network Elements->UAS** in the IEMS Topologies tree.

The following list provides the operations available for UAS Manager in IEMS.

Tasks supported in IEMS for a UAS Manager

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE dialog.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **EMS** from the Type list box.
5	Select **UAS Mgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform
8	Click the **Next** button. *The channel name and the administrator name are displayed in various fields.*
9	Click the **Next** button. *A "No Performance Interface" message is displayed.* The performance interface details for UAS NEs are taken by default in IEMS. The default values are listed below: • SNMP version = v3 • User name = v3admin • Security level = noAuthnoPriv
10	Click the **Finish** button to add the UAS Manager. *Once the UAS Manager is added, a message that says "Successfully added to database" appears in the status bar.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The UAS Manager with the specified name is added as a map symbol to the Element Managers topology panel. In addition, a topology node named UAS Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS Topologies tree.

You have completed this procedure.

—End—

The UAS Manager can be added using IEMS Web Client. For details, refer to "Adding a UAS Manager using Web Client" (page 314) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding EMS applications

EMS applications manage elements in a network. This section includes procedures on how to add the EMS applications to the IEMS topology.

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 an invalid IP address.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an Audio Provisioning Server application

Application

Use this procedure to add an Audio Provisioning Server (APS) application Manager.

IEMS discovers the Audio Provisioning Server application automatically when its corresponding APS manager is added to the IEMS topology. The APS application is added as a map symbol under the grouped APS map symbol in the EMS Applications display panel. It is also added under **EMS Application->APS** in the IEMS Topologies tree.

The following table provides the operations available for the APS application in IEMS.

Tasks supported in IEMS for the APS application

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Others operations		
Launching corresponding applications	Yes	No

Action

Refer to the "Adding an Audio Provisioning Server Manager (APS Manager)" (page 22) procedure to add an APS manager.

Copyright © 2006, Nortel Networks

Adding a Certificate Manager application

Application

Use this procedure to add a Certificate Manager application to the IEMS topology using Java Web Start Client.

Prerequisites

This procedure has the following prerequisites:

- you must belong to the emsadm group to add the Certificate Manager application.

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 **Tools-->Add-->Application** menu command to open the Add Application dialog box.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **CertMgr** from the Device Type list box.
5	Select the version of the device from the Device Version list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
7	Click the **Next** button. *The system log details are displayed.*
8	Click the **Next** button. *A message stating that no performance interface for the Certificate Manager application is displayed.*
9	Click the **Finish** button to add the Certificate Manager application. *Once the Certificate Manager application is added, a message appears in the status bar that reads "Status: Successfully added to database"*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The Certificate Manager application is added as a map symbol under the grouped CertMgr map symbol in the EMS Applications display panel. It is also added under ***EMS Applications*** in the IEMS Topologies tree.

10 Click the **Cancel** button to close the Add Application window.

11 You have completed this procedure.

—End—

The Certificate Manager application can be added using IEMS Web Client. For details, refer to "Adding a Certificate Manager application using Web Client" (page 326).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Line Maintenance Manager application

Application

Use this procedure to add the Line Maintenance Manager (LMM) application to the IEMS using the IEMS Java Web Start Client. SPFS is the parent platform for the LMM application.

The following list provides the operations available for the LMM application in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	No	No
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->Application** menu command to invoke the Add Application wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **LMM** from the Device type list box.
5	Select the version of the device from the Device Version list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
7	Click the **Next** button. *A message stating no fault interface for LMM application is displayed.*
8	Click the **Next** button. *A message stating no performance interface for LMM application is displayed.*
9	Click the **Finish** button to add the LMM application. *Once the LMM application is added, the message "Successfully added to database" appears in the status bar.* *The LMM application with the specified name is added as a map symbol under the grouped LMM map symbol in the EMS Applications display panel. It is also added under **EMS Applications->LMM** in the IEMS Topologies tree.* You have completed this procedure.
	—End—

The LMM application can be added using IEMS Web Client. For details, refer to "Adding an LMM application using Web Client" (page 320) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Network Patch Manager application

Application

Use this procedure to add the Network Patch Manager (NPM) application to the IEMS using the IEMS Java Web Start Client. SPFS is the parent platform for the NPM application.

The following list provides the operations available for the NPM application in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->Application** menu command to invoke the Add EMS Application wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **NPM** from the Device Type list box.
5	Select the version of the device from the Device Version list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform
7	Click the **Next** button. *In the Syslog Details panel, the fields displays the location of Customer Log File, Audit Log File, and Security Log File.*
8	Click the **Next** button.
9	Click the **Finish** button to add the NPM. *Once the NPM is added, the message "Successfully added to database" appears in the status bar.* *The NPM application with the specified name is added as a map symbol under the grouped NPM map symbol in the EMS Applications display panel. It is also added under **EMS Applications->NPM** in the IEMS Topologies tree.* You have completed this procedure.
	—End—

The NPM application can be added using IEMS Web Client. For details, refer to "Adding an NPM application using Web Client" (page 321) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an OSSGate application

Application

Use this procedure to add the OSSGate application to the topology using the IEMS Java Web Start Client. SPFS is the parent platform for the OSSGate application.

The following list provides the operations available for the OSSGate application in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	No	No
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->Application** menu command to invoke the Add EMS Application wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **OSSGate** from the Device Type list box.
5	Select the version of the device from the Device Version list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
7	Enter the OSSGate port in the OSSGate Port field or retain the default value as "10023". The OSSGate port must be configured to match the OSSGate port configured on the CMT platform.
8	Click the **Next** button. *A message stating no fault interface for the OSSGate application is displayed.*
9	Click the **Next** button. *A message stating no performance interface for the OSSGate application is displayed.*
10	Click the **Finish** button to add the OSSGate application. *Once the OSSGate application is added, the message "Successfully added to database" appears in the status bar.* *The OSSGate application with the specified name is added as a map symbol under the grouped OSSGate map symbol in the EMS Applications display panel. It is also added under **EMS Applications->OSSGate** in the IEMS Topologies tree.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The OSSGate application can be added using the IEMS Web Client. For details, refer to "Adding an OSSGate application using Web Client" (page 322)* procedure.

Copyright © 2006, Nortel Networks

Adding a QoS Collector application

Application

Use this procedure to add the QoS Collector application (QCA) to the IEMS topology using the IEMS Java Web Start Client. SPFS is the parent platform for the QoS Collector application.

The following list provides the operations available for the QoS Collector application in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->Application** menu command to invoke the Add EMS Application wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **QoS Collector** from the Device Type list box.
5	Select the version of the device from the Device Version list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform
7	Click the **Next** button. *In the Syslog Details panel, the list of fields displays the location of various log files such as Customer Log File, Audit Log File, and Security Log File.*
8	Click the **Next** button. *A message stating no performance interface for QoS Collector application is displayed.*
9	Click the **Finish** button to add the QoS Collector application. *Once the QoS Collector application is added, the message, "Successfully added to database", appears in the status bar.* *The QoS Collector application with the specified name is added as a map symbol under the grouped QoS Collector map symbol in the EMS Applications display panel. It is also added under **EMS Applications->QoS Collector** in the IEMS Topologies tree.* You have completed this procedure.
	—End—

The QCA can be added using IEMS Web Client. For details, refer to "Adding a QCA using Web Client" (page 323) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Synchronized Backup Restore Manager application

Application

Use this procedure to add the Synchronized Backup Restore Manager (SBRM) application to the IEMS topology using the IEMS Java Web Start Client. SPFS is the parent platform for the SBRM application.

The following table provides the operations available for the SBRM application in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	No	No
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->Application** menu command to invoke the Add EMS Application wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **SBRM** from the Device Type list box.
5	Select the version of the device from the Device Version list box.
6	Click the **Next** button. *In the Syslog Details panel, the list of fields displays the location of various log files such as Customer Log File, Audit Log File, and Security Log File.*
7	Click the **Next** button. *A message is displayed stating that there is no performance interface.*
8	Click the **Finish** button to add the SBRM application. *Once the SBRM application is added, the message, "Successfully added to database", appears in the status bar as shown below:* *The SBRM application with the specified name is added as a map symbol under the grouped SBRM map symbol in the EMS Applications display panel. It is also added under **EMS Applications->SBRM** in the IEMS Topologies tree.* You have completed this procedure.
	—End—

The SBRM can be added using IEMS Web Client. For details, refer to "Adding an SBRM application using Web Client" (page 324) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Trunk Maintenance Manager application

Application

Use this procedure to add the TMM application to the IEMS topology using the IEMS Java Web Start Client. SPFS is the parent platform for the Trunk Maintenance Manager (TMM) application.

The following list provides the operations available for the TMM application in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	No	No
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->Applicatio**n menu command to invoke the Add EMS Application wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **TMM** from the Device type list box.
5	Select the version of the device from the Device Version list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
7	Click the **Next** button. *A message stating no fault interface for TMM application is displayed.*
8	Click the **Next** button. *A message stating no performance interface for the TMM application is displayed.*
9	Click the **Finish** button to add the TMM application. *Once the TMM application is added, the message, "Successfully added to database" appears in the status bar.* *The TMM application with the specified name is added as a map symbol under the grouped TMM map symbol in the EMS Applications display panel. It is also added under* ***EMS Applications->TMM*** in the IEMS Topologies tree. You have completed this procedure.
	—End—

The TMM application can be added using IEMS Web Client. For details, refer to "Adding a TMM application using Web Client" (page 325) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding network elements

IEMS manages the fault domain and provides a centralized location to access the management interfaces for the NEs in the following procedure list.

The procedures in this section describe how to add the NEs to the topology.

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 an invalid IP address.

Refer to "Launching applications from IEMS" in *IEMS Overview*, NN10329-111 for details of which NEs are auto-discovered by their corresponding managers.

Copyright © 2006, Nortel Networks

Adding a CICM NE

Application

Use this procedure to add a Centrex IP Client (CICM) NE to the IEMS topology using Java Web Start Client. CICM NE is managed by CICM Manager.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for CICM NE in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	No
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Prerequisites

For IEMS to receive CICM fault and performance data

CICM Manager must be configured to send fault data to IEMS. The CICM has a script called **preboot** which is used to configure the CICM with the IEMS server virtual IP address and port for sending the fault data to IEMS. Without this configuration, IEMS receives no faults from the CICM.

For launching CICM Manager

The prerequisites for launching the CICM Manager are:

- CICM Manager has to be configured using the SPFS CLI tool for launching CICM Manager from IEMS Client. For details, refer to *CICM Configuration*, NN10240-511.
- CICM Manager can be launched only in Microsoft Windows with the default browser configured as Microsoft Internet Explorer.

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **NE** from the Type list box.
5	Select **CICM** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the NE unit mode from the Mode list box. If Duplex mode is selected, follow these steps: a. Enter the inactive unit IP in the Inactive Unit IP field, b. Enter the Card B IP address in the Card B IP Address field. c. Enter the Card B display name in the Card B Display Name field.
8	Enter the card location in the Card Location field. The card location entered while adding the corresponding CICM Manager must be provided in the Card Location field for CICM NE.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

9 Click the **Next** button to proceed to the Fault Interface screen in the wizard.

10 Enter the port (in which the EMS communicates with IEMS) in the Port field or retain the default value as "161".

11 Enter the community in the Community field.

12 Select the SNMP version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box. If you select the **value NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

13 Click the **Next** button to proceed to the Performance Interface screen in the wizard.

14 Repeat step 10 to step 12.

15 Click the **Finish** button to add the CICM NE.

Once the CICM NE is added, a message that reads "Successfully added to database" appears in the status bar.

The CICM network element with the specified name is added as a map symbol under the grouped CICM map symbol in the Network Elements display panel. It is also added under ***Network Elements->CICM*** *in the IEMS Topologies tree.*

You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

A CICM NE can be added using IEMS Web Client. For details, refer to "Adding a CICM NE using Web Client" (page 330).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a GWC NE

Application

IEMS discovers the GWC NEs automatically when their corresponding GWC manager is added to the IEMS topology. Each discovered GWC network element is added as a map symbol under the grouped GWC map symbol in the Network Elements display panel. They are also added under **Network Elements->GWC** in the IEMS Topologies tree.

The following list provides the operations available for GWC NE in IEMS.

Tasks supported in IEMS for a GWC NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

The resynchronization of alarms is supported through the GWC manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Action

Refer to "Adding a Gateway Controller Manager" (page 41) procedure to add a GWC manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding CS 2000 Core and Call Agent Core NEs

Application

Use this procedure to add a CS 2000 Core Manager using IEMS Java Web Start Client.

IEMS discovers the CS 2000 Core and Call Agent Core NEs automatically when its corresponding CS 2000 Core manager is added to the IEMS topology. The CS 2000 Core and Call Agent Core NEs are added as a map symbol under the grouped CS 2000 Core map symbol and grouped Call Agent Core map symbol respectively in the Network Elements display panel. Also, CS 2000 Core and Call Agent Core NEs are added under **Network Elements->CS2000 Core** and **Network Elements->Call Agent Core** respectively in the IEMS Topologies tree. When the Call Agent Core NE is added, the corresponding Call Agent platform is discovered automatically. The Call Agent platform is added in the Call Agent Platform topology node (under the Network Element-->Call Agent Core node) in the IEMS Topologies tree.

As CS 2000 Core and Call Agent Core are managed by the CS 2000 Core manager, the CS 2000 Core and Call Agent Core event correlation is against the CS 2000 Core Manager.

The following list provides the operations available for CS 2000 Core and Call Agent Core NEs in IEMS.

Tasks supported in IEMS for CS 2000 Core and Call Agent Core NEs

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events	No	No
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Action

Refer to "Adding a Communication Server 2000 Core Manager" (page 32) procedure to add a CS 2000 Core Manager.

Copyright © 2006, Nortel Networks

Adding an Ethernet Routing Switch 8600 NE

Application

Use this procedure to add the Ethernet Routing Switch (ERS) 8600 NE to the topology using the Java Web Start Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for ERS 8600 NE in IEMS.

Tasks supported in IEMS for the ERS 8600 NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	Yes	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks

Prerequisites

Ensure that a device with the same IP address is not already added. If an ERS 8600 device was added before (I)SN09, the system does not automatically reject the new device.

For IEMS to receive ERS 8600 fault and performance data

ERS 8600 NEs must be configured to send fault and performance data to IEMS; without this configuration, IEMS receives no fault and performance data from ERS 8600 NEs.

For launching ERS 8600 Device Manager

ERS 8600 Device Manager must be installed on the client machine in order to launch the GUI. For details of how to install the Device Manager, refer to *Installing ERS 8600 Switch Modules* 312749F.

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 **Tools**-->Add-->EMS/NE menu command to invoke the **Add EMS/NE** wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **NE** from the Type list box.
5	Select **ERS 8600** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Check the Radius Secret field to enable the RADIUS secret password and enter RADIUS secret password in the Radius Secret field. If the Radius Secret field is checked and the password is not entered, the wizard displays "Enter the radius secret" error.
8	Click the **Next** button.
9	Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".
10	Enter the community in the Community field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

This field must be specified for SNMP versions v1 and v2 alone and not for SNMP v3.

11 Select the SNMP version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box.

If you select the value **AuthPriv** from Security Level list box, enter the following details:

- User name
- Authentication Protocol
- Authentication Password
- Privacy Password

Value for the Context name field need not be specified as that is not used by the ERS 8600 device.

12 Click the **Next** button.

13 Repeat step 9 to step 11.

14 Click the **Finish** button to add the ERS 8600.

Once the ERS 8600 NE is added, the message "Successfully added to database" appears in the status bar.

The ERS 8600 network element with the specified name is added as a map symbol under the grouped ERS 8600 map symbol in the Network Elements display panel. It is also added under ***Network Elements->ERS 8600*** *in the IEMS Topologies tree.*

You have completed this procedure.

—End—

The ERS 8600 NE can be added using IEMS Web Client. For details, refer to "Adding an Ethernet Routing Switch 8600 NE using Web Client" (page 333).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring the ERS 8600 to send events and alarms to the IEMS

Use this procedure to add an SNMP trap destination address to the ERS 8600 to allow for events and alarms to be sent to the IEMS server, including Open Shortest Path First (OSPF) events and alarms if applicable to your office.

Prerequisites

None

Action

Perform the steps that follow to complete this procedure.

Step	Action
	At a web browser
1	Launch the Integrated EMS Java Web Start Client. Refer to procedure "Launching Integrated EMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
	At the IEMS GUI
2	Click on **Network Elements** in the IEMS topology tree.
3	Right-click on an ERS8600 map symbol and select **ERS8600 Device Manager->Open**. The first time you run the Device Manager, you will need to specify where the executable for the Device Manager is located. The file you need is jdm.exe. Use the **Browse** button to locate the file, then click **OK**. The Device Manager opens as shown in the figure that follows.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

4 From the Device menu, select **open**.

5 Enter the following information:

- the IP address for the ERS 8600 in the Device Name field
- check the v3 Enabled box
- Enter initial in the User Name field

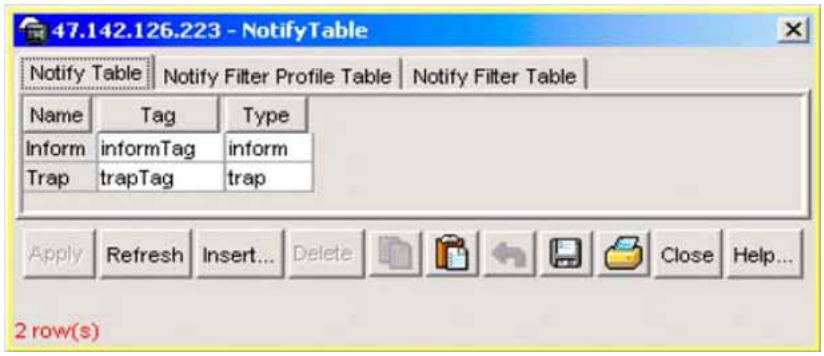
6 Click **Open**.

7 Click **Edit->SNMPv3->Notify Table**.

8 Verify the entries for Trap are as follows:

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- Tag = trapTag
- type = trap



If the entries are not present, create using **Insert**.

9 Close the Notify Table widow.

10 Click **Edit->SNMPv3->Target Table**.

11 Select the **Target Params Table** tab.

12 Verify the entries for TparamV1 and TparamV2 are present.

If the entries are not present, create using **Insert**.

13 Select the **Target Table** tab.

The Target Table tab is displayed.

14 Click **Insert**.

15 Enter the following information:

- Name = <a unique name>
- TAddress = <IEMS IP Address:162>

  For example 10.10.10.10:162

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- TagList = trapTag
- Params = TparamV2

  TparamV2 must be set if you want to use V2C traps. You must use TparamV2 on ERS8600 3.7.0 loads and higher.

16 Click **Insert**.

17 Click **Close**.

18 Click **Device->Exit**.

19 Repeat steps 3 to 18 for each ERS 8600.

At the ERS 8600

20 Determine if OSPF is enabled on the ERS 8600 by typing

```
show ip ospf info
```

and pressing the Enter key.

Example response

```
Ospf General
Ospf General
RouterId:  1.1.1.2
AdminStat:  enabled
VersionNumber:  2
AreaBdrRtrStatus:  true
ASBdrRtrStatus:  false
ExternLsaCount:  1
ExterLsaCksumSum:  29660(0x73dc)
TOSSupport:  0
OriginateNewLsas:  270
RxNewLsas:  1047
TrapEnable:  false
AutoVirtLinkEnable:  false
SpfHoldDownTime:  10
```

When the value for TrapEnable is false, OSPF events will not be sent to the IEMS. The value for TrapEnable must be true for OSPF events to be sent to the IEMS

OSPF routing must already be configured and enabled. If required, refer to *Configuring IP Routing Operations*, 314720-d.

21 Use the following table to determine your next step.

If the value for TrapEnable is	Do
false	step 22
true	you have completed this procedure

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

22 Enable OSPF by typing

```
config ip ospf trap enable
```

and pressing the Enter key.

23 Ensure OSPF is enabled on the ERS 8600 by typing

```
show ip ospf info
```

and pressing the Enter key.

Example response

```
Ospf General
RouterId:  1.1.1.2
AdminStat:  enabled
VersionNumber:  2
AreaBdrRtrStatus:  true
ASBdrRtrStatus:  false
ExternLsaCount:  1
ExterLsaCksumSum:  29660(0x73dc)
TOSSupport:  0
OriginateNewLsas:  270
RxNewLsas:  1047
TrapEnable:  true
AutoVirtLinkEnable:  false
SpfHoldDownTime:  10
```

24 Repeat step 20 to step 23 for each ERS 8600.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring the Ethernet Routing Switch 8600 for IEMS

Application

Use this procedure to configure the ERS 8600 device for IEMS.

The ERS 8600 device must be configured to establish communication with IEMS and other management applications.

Action

This procedure is made up of the following steps:

Step	Action
	At the IEMS server
1	Telnet to ERS8600 and login.
2	Load encryption modules.
3	Configure SNMP -v3.
4	Enable SSH.
5	Disable Non-secure services.
6	Verify SSH is working and disable telnet.
7	Disable SNMPv1/v2c.
8	Change default SNMPv1 community strings.
9	Change the login passwords.
10	Save the configuration.
11	Configure the ERS8600 RADIUS. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Telnet to ERS8600 and login

Telnet to login to ERS8600 configuration console to configure the device. If the ERS8600 is contained in a VLAN, telnet must be performed from a workstation such as the IEMS server. The default userid and password are rwa and rwa, respectively. The following configuration steps must be performed on the ERS8600.

Step	Action

At the IEMS server

1 Telnet the device

```
telnet 47.142.126.223
*********************************************
* Copyright (c) 2004 Nortel Networks, Inc.
*
* All Rights Reserved                        *
* Passport 8010                              *
* Software Release 3.7.0.0                   *
*********************************************
```

2 Login to the device with the given userid and password.

```
Login:  rwa
Password:***
```

The software release level must be 3.7 or greater. After successful login the prompt appears as

```
ERS8600:5#
```

3 The string shown as a prefix (in this case, ERS8600) is the mib-2 object, SNMPv2-MIB:sysName.0.It can be changed with the following command:

```
config cli prompt <new-prompt>
```

4 Display a list of commands that are available at the current context by entering:

```
?
```

It also displays a list of sub-contexts that can be entered through the sub-context name. This is similar to traversing a hierarchy of commands. The command info displays the state of current context and lists the available sub-contexts. The state of a context is a list of attributes and corresponding values. Configuration is performed through the config context. Enter the context name

```
ERS8600:5# config
```

5 Change the prompt to the following:

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

```
ERS8600:5/config#
```

You have completed this procedure.

—End—

Notes on shell cursor movement and editing:

- Left and right arrow keys move the cursor backward and forward on the command line.
- Up and down arrow keys moves backward and forward in the command stack.
- Ctrl-a moves the cursor to the beginning of the command line.
- Ctrl-e moves the cursor to the end of the command line.
- Ctrl-h is a destructive backspace. The Backspace key does nothing.
- You are always in insert mode.
- Ctrl-d is passed to telnet/ssh and closes the session.

Load encryption modules

From the config context, enter the commands,

```
load-encryption-module DES
load-encryption-module 3DES
```

Encryption modules must be loaded onto the ERS8600 flash using ftp or tftp or by use of PCMCIA slot. Refer to the applicable installation guide for ERS 8600.

If the DES encryption module is not available, then SNMPv3 –USM can not be configured.This means that authenticated and encrypted communications between OAM applications and the ERS8600 are not available. SNMP communications can only be made through v1 or v2c protocols. There is no additional configuration required to get or set communications through v1 or v2c.

If the Triple DES (3DES) encryption module is not available, then SSH cannot be configured. Telnet is the only available communications protocol for accessing the ERS8600 command line.

Configure SNMP -v3

The following tables are used to configure SNMPv3 authentication and privacy.

- USM table defines users, authentication/privacy protocols, and passwords.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- Group-Member table defines to which groups each USM user belongs.
- Group-Access table defines the access rights that each user has to the objects in the MIB tree.
- Notify table defines the types of notifications (TRAP or INFORM) that are sent.
- Target-Parm table defines which USM user receives a notification.
- Target-Address table defines the network managers that receive notifications. Each row denotes a unique manager. It has one or more references into the Notify table to determine the notification type. It also has one reference into the Target-Parm table to determine the user credentials used to send the notification.
- Community Table contains the Read and Write community strings for SNMPv1/v2c.

  The Target-Param table references the CommunityTable for sending v1/v2c traps.

Change into the snmp-v3 context by entering the context name. The new prompt is displayed as

Step	Action
	ERS8600:5/config/snmp-v3#

1	Add users iems and jdm. Create a different user for each application such that a password change made using the JDM does not break the IEMS application. The SNMPv3-USM uses an authentication protocol and password, and also a privacy protocol and password. Entering the command, the command syntax is:
	`usm create <user> <auth_prot> auth <pw1> priv <pw2>`
	where <auth_prot> is one of: sha | md5
	Enter the commands,
	`usm create iems sha auth iemspass1 priv iemspass2`
	`usm create jdm sha auth jdmpass1 priv jdmpass2`
	These two commands create the 2 users, ems and jdm, with:
	• authentication protocol of SHA-1 and authentication password of iemspass1 and jdmpass1
	• privacy password of iemspass2 and jdmpass2. The privacy encryption protocol is DES. This is the only one supported by the ERS8600.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The information above must be noted as it is used to configure both the IEMS and JDM.

Attribute	Value
User Name	iems
Authentication Protocol	sha
Authentication Password	<user specified>
Privacy Protocol	DES (only allowed value on ERS8600)
Privacy Password	<user specified>

Enter the command
```
usm info
```

The current context is displayed:
```
User/Sec Name     Engine Id    Protocol
-----------------------------------------
iems     800008E00300E07BA7B400   HMAC_SHA, DES PRIVACY
initial  800008E00300E07BA7B400   NO AUTH, NO PRIVACY
jdm      800008E00300E07BA7B400   HMAC_SHA, DES PRIVACY
```

The user name initial is a pre-configured value for SNMPv1.

2 Add user iems to vacm. This creates the group iemsgrp and adds the users iems and jdm to it. The command syntax is:

```
group-member create <user_name> <model> <group_name>
where <model> is one of:  snmpv1 | snmpv2c | usm
```

Enter the commands,
```
group-member create iems usm iemsgrp
group-member create jdm usm iemsgrp
```

3 Create an access control list for the iemsgrp. The empty double quoted string is the context name. This is equivalent to a null context. It is not used and not supported by the ERS8600. The command syntax is,

```
group-access create <group_name> <prefix> <model>
<level>
```

where

<model> is one of: snmpv1 | snmpv2c | usm
<level> is one of: noAuthNoPriv | authNoPriv | authPriv

Enter the command,
```
group-access create iemsgrp " " usm authPriv
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The <prefix> is saved as the context name but is not used in the current level of firmware.

4 Indicate the branches of the mib tree that iemsgrp is allowed to access. The command syntax is,

```
group-access view <group_name> <prefix> <level> read
<view_name> write <view_name> notify <view_name>
```

Enter the command,

```
group-access view iemsgrp " " usm authPriv read
org      write org notify org
```

Values for <view_name> can be seen with the command,

```
mib-view info
```

This defines the part of the mib tree that can be accessed. The value org specifies every object under the prefix *.iso.org*.

5 Add or verify the available notification types. There must be two pre-configured types. These can not be altered or deleted, and are sufficient for our needs. Enter the command:

```
notify info
```

The Notify Table is displayed:

```
-----------------------------------------------
NotifyName          Tag                  Type
-----------------------------------------------
inform              informTag          inform
Trap                trapTag            trap
```

If this is not correct, then add the information using the following command syntax:

```
notify create <notify_name> tag <value> type <type>
```

where

<type> is one of: trap | inform

Enter the command,

```
notify create Inform tag informTag type inform
notify create Trap tag trapTag type trap
```

6 Add target address for traps. First, we must add an entry into target-parm. The command syntax is,

```
target-param create <tparm_name> mp-model <value>
sec-level <value> sec-name <value>
```

where the value for:

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

mp-model is one of: *snmpv1* | *snmpv2c* | *usm*

sec_level is one of: noAuthNoPriv | authNoPriv | authPriv

sec-name is the usm user entered in step 1. either iems or jdm

Enter the commands,

```
target-param create TparamV3iems mp-model usm sec-level
authPriv sec-name iems target-param create TparamV3jdm
mp-model usm sec-level authPriv sec-name jdm
```

This creates a new row in the table with name TparmsV3iems referencing our iems user in the USM table. Enter the command:

target-param info

The Notify Table is displayed:

```
-----------------------------------------------
TargetName   MP Model Security Name   Sec Level
-----------------------------------------------
TparamV1        snmpv1   readview noAuthNoPriv
TparamV2       snmpv2c  readview noAuthNoPriv
TparamV3iems      usm        iems     authPriv
TparamV3jdm       usm         jdm     authPriv
```

TparamV1 and TparamV2 are pre-configured default entries for SNMP v1 and v2c. They must not be deleted.

7 Add the ip-address of the IEMS that receives the traps. Repeat for each IEMS. The command syntax is,

```
target-addr create <target_name> <ip_addr> <target_pa
rm> taglist <value>
```

Enter the command,

```
target-addr create bumrot 47.142.94.68:162
TparamV3iems taglist    trapTag
...or...
target-addr create bumrot 47.142.94.68:162
TparamV3jdm taglist    trapTag
```

This creates an entry for

- A host called bumrot. This is an arbitrary string and does not match the real host name. The ERS8600 does not use a DNS to resolve the ip-address. This must be an unique value in the table.
- The ip-address port to receive the trap. This must also be an unique value in the table.
- A reference to the user who receives the trap at the specified ip-address. This is designated through the target-parm name of TparamV3iems or TparmV3jdm.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- A reference to the kind of notification to be sent. This is designated through the notify name of the trapTag and points back to the Notify Table.

  The <ip_addr> is the primary key in this table. A trap can be sent to only one user (one target_parm) on the specified address. This means, one cannot issue both the commands listed above. The second is an error indicating a duplicate ip address

If SNMP v1/v2c traps are being configured, enter the command above but specify either TparamV1 or TparamV2 as the <target_parm>. For example, target-addr create bumrot 47.142.94.68:162 TparamV1 taglist trapTag

You have completed this procedure.

—End—

Enable SSH

Enter the config sub-context. From the config/snmp-v3 sub-context you can enter the context name, config, to jump to the correct context or enter a single period (.) to move up one context level. The new prompt is displayed as,

```
ERS8600:5/config#
```

Enter the following command,

```
bootconfig flags sshd true
sys set ssh action dsa-keygen 1024
sys set ssh action rsa-keygen 1024
sys set ssh enable
```

Disable Non-secure Services

From the config sub-context, enter the following commands,

```
bootconfig flags ftpd    false
bootconfig flags tftpd   false
bootconfig flags rlogind false
web-server disable
```

Verify SSH is working and Disable telnet

Login using SSH and from the config sub-context enter,

```
bootconfig flags telnetd false
save bootconfig
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Disable SNMPv1/v2c

Index1 and first represent the default read-only access (public) created by the SNMPv3 engine. Index2 and second represent the default read-write access (private).

Access through SNMPv1 and v2c is controlled using community strings. From the config/snmp-v3 context enter the command, community info, to display the current table. The pre-configured values for public and private community names are contained in the Security Names readview and initialview, respectively. The column designated as, name, is the community name string and is shown as a list of asterisks. The pre-configured values are "public" and "private".

```
-------------------------------------------------
         Community Table
-------------------------------------------------
Index        Name        Security Name   Transport Tag
-------------------------------------------------
Index1       ********        readview
Index2       ********        initialview
first        ********        readview
second       ********        initialview
4 out of 4 Total entries displayed
-------------------------------------------------
```

Previously existing default communities prior to a software upgrade appear as Index1 (public) and Index2 (private). You can delete those, but you can not delete the default communities first and second, however, you can change the community strings for them.

To delete Index1 and Index2, enter the commands:

```
config snmp-v3 community delete Index1
config snmp-v3 community delete Index2
```

The ERS8600 does allow the Name field to be changed with modify/remove. We can change the public community string to some real long value, but the ERS8600 is subjected to brute force attacks as the community name string is part of the SNMP PDU.

Alternatively, if the Security Name field is altered, it can effectively disable SNMPv1/v2c. The Security Name field is used to access the GroupMember table to determine authority to access various elements of the MIB tree.

To change the sec-name, enter the commands:

```
snmp-v3 community secname first new-secname was_readview
snmp-v3 community secname second new-secname was_initialview
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Now, all v1/v2c get and set requests fail VACM access checks due to inability to find the Security Name in the GroupMember table. The ERS8600 is not subjected to disruption as the Security Name is not included in the SNMP PDU.

Change default SNMPv1 community strings

This section is included if the DES encryption module cannot be loaded and SNMPv3 cannot be enabled.

The read and write community name strings of public and private must be changed. From the config/snmp-v3 context enter the command, community info, to display the current table. The pre-configured values for public and private community names are contained in the Security Names readview and initialview, respectively. The column designated as, name, is the community name string and is shown as a list of asterisks.

```
Index         Name            Security Name     Transport Tag
-----------------------------------------------------
Index1        ********         readview
Index2        ********         initialview
first         ********         readview
second        ********         initialview
```

Delete the Index1 and Index2 entries if available by entering these commands:

```
config snmp-v3 community delete Index1
config snmp-v3 community delete Index2
```

To change community strings, enter these commands:

```
snmp-v3 community commname first new-commname <publicvalue>
snmp-v3 community commname second new-commname <privatevalue>
```

Change the login passwords

Passwords are changed through the configuration context,

```
cli password.
```

It is recommended that the passwords for the rwa and rw be changed. Enter the following commands and follow the prompts:

```
cli password rw rw
cli password rwa rwa
```

Save the configuration

Enter the following commands,

```
save bootconfig
save config
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configure ERS 8600 RADIUS

RADIUS (Remote Authentication Dial-in User Service) provides a high degree of security against unauthorized access to the ERS 8600. It is based on a client-server architecture allowing a number of communication servers and clients to authenticate users identity through a central database.

The ERS 8600 operates as a client of RADIUS. The switch is responsible for passing user information to the designated RADIUS servers. Since the ERS 8600 operates in a LAN environment, user access is allowed via Telnet, Rlogin, and Console log-in. When ERS 8600 is configured with radius enable, any user of the switch presents an authentication information in the form of customized login prompt and password. Once authentication process meets all the criteria set in the radius server and switch configuration, the user is permitted to access the switch. If there is no match in any part of the criteria, then the user is rejected and denied access to the switch.

The procedure that follows configures the ERS 8600 and IEMS to allow SSH connections from the command line option of the IEMS.

Once the procedure that follows is completed, all existing user IDs and passwords that provide telnet access to the ERS 8600 will be disabled. All future access to the ERS 8600, either through telnet, ssh , or through the IEMS command line, will user user IDs and passwords created on the IEMS. Authenticating these users will be through the secure RADIUS server on the IEMS.

Step	Action
	At your workstation
1	Launch the IEMS Java Web Start Client using the iemsadm user ID and password. Refer to procedure *"Launching IEMS Java Web Start Client"* in IEMS Overview, NN10329-111.
	At the IEMS GUI
2	Select *Tools->System Administration*.
3	Click *Add User*.
4	Enter the user name, password, and groups. The user must belong to one of the following groups to have command line access to the ERS 8600: • mgcadm • mgcsprov • mgcrw • mgcmtc

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

- mgcro

5 Click *Add User*.

6 Click *Modify User profile*.

7 Enter the user name you created in the previous step, and click*Modify User*.

8 Change the Login Shell from no-access to restricted, and click *Submit*.

9 Close the System Administration page.

10 Select *PP8600* under the Network Elements topology tree.

11 Right-click on one of the PP8600 icons and select **Update Radius secret**.

12 Ensure the Radius Secret box is checked and the password is present. If not, check the Radius Secret box and enter a password.

The default password is nortelnetworks.

13 Close the Radius Secret Configuration window.

14 Repeat step 11 to step 13 for each ERS 8600. Once you have completed for each ERS 8600, proceed to step 15.

At a command prompt window

15 Establish a telnet session to one of the ERS 8600.

At the PP8600

16 Access the config radius server level.

```
config radius server
```

17 Create the RADIUS server.

```
create <ip address of the RADIUS server> secret <the
shared secret defined in the server for this switch>
port <what udp port will be used, matching the RADIUS
server's udp port configuration>
```

The IP address of the RADIUS server is the virtual IP address of the IEMS. The shared secret defined in the server is the one noted in step 12, and the default port number is 1812.

Example

```
create 12.123.45.78 secret nortelnetworks
port 1812
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

18 Set the priority in which the RADIUS server is to provide authentication.

```
set <IP address of the server> priority <choose a value
from 1 to 10>
```

The set value of 1 in the priority field defines the first server to provide authentication.

Example

```
set 12.123.45.78 usedby cli priority 1
```

19 Display and verify the RADIUS server configuration data.

```
info
```

20 Fall back to the config radius level.

```
back
```

21 Enable RADIUS.

```
enable true
```

22 Display the RADIUS configuration data.

```
info
```

23 Save the configuration.

```
save config
```

24 Repeat step 15 to step 23 for each ERS 8600.

You can now access the ERS 8600 from the command line option of the IEMS GUI. The password that is required when logging in to the ERS 8600 from the command line, is the same password you used to log in to the IEMS GUI.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding MCS/CSE and Media Portal NEs

Application

Use this procedure to add MCS/CSE and Media Portal NEs.

IEMS discovers the MCS/CSE and Media Portal NEs automatically when its corresponding MCS manager is added to the IEMS topology. The MCS/CSE or Media Portal NEs are added as a map symbol under their grouped map symbol in the Network Elements display panel. Also, MCS/CSE or Media Portal NEs are added under their respective network elements under **Network Elements** in the IEMS Topologies tree.

Tasks supported by IEMS for MCS/CSE and Media Portal NE objects

The following list provides the operations available for MCS and Media Portal NEs in IEMS.

Tasks supported in IEMS for MCS/CSE and Media Portal NEs

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

The resync of alarms is supported through the MCS manager.

Prerequisites

The following sections list the MCS/CSE and Media Portal NE configuration references required to integrate with the IEMS.

Fault interface

No additional configuration is required for MCS/CSE and Media Portal NEs.

When adding an MCS Manager for MCS/CSE and Media Portal, ensure the MCS SNMP trap destination is configured in the device for the IEMS to manage its fault interface. Refer to the "Prerequisites" section of "Adding an MCS/CSE Manager for MCS/CSE and Media Portal" (page 44).

Configuration interface

No additional configuration is required.

Performance management

No additional configuration is required.

Security configuration

No additional configuration is required.

Action

Refer to "Adding an MCS/CSE Manager for MCS/CSE and Media Portal" (page 44) procedure to add an MCS Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Media Application Server

Application

Use this procedure to add the Media Application Server (MAS) NE to the IEMS topology using Java Web Start Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

For further details on configuring the MAS, refer to *Nortel Media Application Server Configuration*, NN10455-511.

The following list provides the operations available for MAS NE in IEMS.

Tasks supported in IEMS for MAS NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	No
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Others operations		
Launching corresponding applications	Yes	No

Prerequisites

MAS must be configured to send fault data to IEMS; without this configuration, IEMS receives no fault and performance data from MAS NEs.

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 **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **NE** from the Type list box.
5	Select **MAS** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Click the **Next** button.
8	Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as 161.
9	Enter the community in the Community field.
10	Select the SNMP version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details: • User name • Context name

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

11 Click the **Next** button to proceed to the Performance Interface screen in the wizard.

12 Enter the directory name where the CSV file is getting pushed in IEMS Server from the device in the Directory Name field.

13 Enter the file mask of the CSV file getting pushed in the File Name field.

Wildcard support is available for this field.

Example
If the file names starts with "SystemOMs" string, user can enter the value "SystemOMs*.csv".

It must be ensured while configuring each MAS device that the operational measurement (OM) file names are unique. This is useful to differentiate data transmitted from each of the devices.

14 Click the **Finish** button to add the MAS NE.

Once the MAS NE is added, the message "Successfully added to database" appears in the status bar as shown below:

The MAS network element with the specified name is added as a map symbol under the grouped MAS map symbol in the Network Elements display panel. It is also added under ***Network Elements->MAS*** *in the IEMS Topologies tree.*

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The MAS NE can be added using IEMS Web Client. For details, refer to "Adding an MAS NE using Web Client" (page 335) procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Media Gateway 3200 NE

Application

Use this procedure to add Media Gateway (MG) 3200 NE to the IEMS topology using Java Web Start Client.

The Media Gateway 3200 NE can be managed using IEMS by adding it to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for an MG 3200 NE in IEMS.

Tasks supported in IEMS for an MG 3200 NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms (incremental resynchronization supported)	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

Prerequisites

For IEMS to receive MG3200 fault and performance data, MG 3200 must be configured to send fault data to IEMS. For details, refer to *MG 3200 H.248 User's Manual*, LTRT72704.

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **NE** from the Type list box.
5	Select **MG 3200** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Enter the Web server user name in the User Name field.
8	Enter the Web server password in the Web Password field.
9	Click the **Next** button.
10	Enter the Port in the Port field or retain the default value as 161.
11	Enter the Community in the Community field.
12	Enter the Write Community in the Write Community field.
13	Select the SNMP Version from the Version list box. The version must be **v2c**.
14	Click the **Next** button to proceed to the Performance Interface screen in the wizard.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

15 Enter the Port in the Port field or retain the default value as 161.

16 Enter the Community in the Community field.

17 Select the SNMP Version from the Version list box. The version must be **v2c**.

18 Click the **Finish** button to add the MG 3200 NE.

Once the MG 3200 is added, the message "Successfully added to database" appears in the status bar.

The following message is displayed when the node has been added successfully.

"In order to launch the node's client interface, the HTTPS proxy must be configured using the SPFS CLI tool".

*The MG 3200 network element with the specified name is added as a map symbol under the grouped MG 3200 map symbol in the Network Elements display panel. It is also added under **Network Elements->MG 3200** in the IEMS Topologies tree.*

To configure the HTTPS proxy in the MG 3200, refer to Configuring MG 3200 HTTPS proxy of *Nortel Media Gateway 3200 H.248 Configuration Guide*, LTRT72904.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding Media Gateway 7480/15000/20000 and MSS 15000 NEs

Application

Use this procedure to add a Media Gateway 7480/15000/20000 or Multiservice Switch 15000 NE using IEMS Java Web Start Client.

IEMS discovers the MG 7480/15000/20000 and MSS 15000 NEs automatically when their corresponding MDM is added to the IEMS topology. Each MG 7480/15000/20000 and MSS 15000 NE is added as a map symbol under the corresponding grouped map symbol in the Network Elements display panel. Also, each MG 7480/15000/20000 and MSS 15000 NE is added under the corresponding NE under **Network Elements** in the IEMS Topologies tree.

For the NEs and MDM automatically discovered by MDM, the display name of the map symbol is appended with the parent MDM name in brackets.

The following list provides the operations available for MG 7480/15000/20000 and MSS 15000 NEs in IEMS.

Tasks supported in IEMS for MG 7480/15000/20000 and MSS 15000 NEs

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties. See "Editing NE object properties" (page 175).	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

The resynchronization of alarms is supported through MDM.

Action

To add an MDM, refer to Adding a Multiservice Data Manager procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MG 9000 NE

This subsection provides the following procedures:

- Procedure to add an MG 9000 NE
- A reference for updating the RADIUS secret password

Application

Use this procedure to add an MG 9000 NE.

IEMS discovers the MG 9000 NE automatically when its corresponding MG 9000 manager is added to the IEMS topology. The MG 9000 network element is added as a map symbol under the grouped MG9K map symbol in the Network Elements display panel. It is also added under **Network Elements->MG9K** in the IEMS Topologies tree.

The following list provides the operations available for MG 9000 NE in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	No	No

The resynchronization of alarms is supported through the MG 9000 manager.

Action

Refer to the "Adding a Multiservice Gateway 9000 Manager" (page 68) procedure to add a MG 9000 manager.

To update the RADIUS secret, refer to "Configuring a default secret for RADIUS clients" in *IEMS Administration and Security*, NN10336-611.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Media Server 2000

Applications

Use this procedure to add a Media Server 2000 (MS 2000) NE to the IEMS topology using Java Web Start Client.

The Media Server 2000 NEs can be managed using IEMS by adding them to the IEMS topology. The MS 2000 NE includes the MS 2010 and MS 2020 NEs.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for MS 2000 NE in IEMS.

Tasks supported in IEMS for an MS 2000 NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms (incremental resync supported)	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Others operations		
Launching corresponding applications	Yes	No

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 **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
4	Select **NE** from the Type list box.
5	Select **MS2000** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Enter the Web server user name in the User Name field.
8	Enter the Web server password in the Web Password field.
9	Click the **Next** button.
10	Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as 161.
11	Enter the community in the Community field.
12	Enter the write community in the Write Community field.
13	Select the SNMP version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details: • User name • Context name

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

14 Click the **Next** button to proceed to the Performance Interface screen in the wizard.

15 Repeat step 10 to step 13 excluding step 12.

16 Click the **Finish** button to add the MS 2000 NE.

Once the MS 2000 is added, a message that reads "Successfully added to database" appears in the status bar.

*The MS 2000 network element with the specified name is added as a map symbol under the grouped MS 2000 map symbol in the Network Elements display panel. It is also added under **Network Elements->MS 2000** in the IEMS Topologies tree.*

You have completed this procedure.

—End—

The MS 2000 can be added using IEMS Web Client. For details, refer to "Adding an MS 2000 NE using Web Client" (page 340) procedure.

Copyright © 2006, Nortel Networks

Adding a SAM21 NE

Application

Use this procedure to add an SAM21 NE.

IEMS discovers the SAM21 NE automatically when its corresponding SAM21 manager is added to the IEMS topology. Each SAM21 network element is added as a map symbol under the grouped SAM21map symbol in the Network Elements display panel. Also, each SAM21 NE is added under **Network Elements->SAM21** in the IEMS Topologies tree.

The following list provides the operations available for SAM21 NE in IEMS.

Tasks supported in IEMS for a SAM21 NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	No	No
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The resynchronization of inventory is supported through the SAM21 manager.

Action

Refer to "Adding a SAM21 Manager" (page 71) procedure to add a SAM21 manager.

Copyright © 2006, Nortel Networks

Adding an SSTrunks NE

Application

Use this procedure to add the SSTrunks NE to the IEMS topology using IEMS Java Web Start Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for the SSTrunks NE in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	No
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Prerequisites

The following sections list the SSTrunks NE configuration references required to integrate with the IEMS.

Fault interface

Refer to "Reprovision the NCGL platform software" in *Session Server - Trunks Configuration*, NN10338-511. The SSTrunks SNMP trap destination must be configured in the device for IEMS to manage its fault interface.

Configuration interface

To configure the Apache Web Server on an SPFS-based server for HTTPS proxy, see *Session Server - Trunks Configuration*, NN10338-511.

Performance management

No additional configuration is required.

Security configuration

The security configuration is not integrated into the IEMS Centralized Security Server.

Launching SSTrunks client interface

Refer to "Add a Session Server - Trunks node to the SPFS server web proxy" in *Session Server - Trunks Configuration*, NN10338-511. To launch the SSTrunks client interface from the IEMS, you must configure the SPFS HTTPS proxy on the IEMS server.

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 **Tools-->Add-->EMS/NE** menu command to open the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **NE** from the Type list box.
5	Select **SSTrunks** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the device mode from the Mode list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

8 Click the **Next** button to proceed to the Fault Interface screen in the wizard.

9 Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".

10 Enter the community in the Community field.

11 Select the SNMP version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

12 Click the **Next** button to proceed to the Performance Interface screen in the wizard.

13 Repeat step 9 to step 11.

14 Click the **Finish** button to add the SSTrunks.

Once the SSTrunks is added, the message, "Successfully added to database", appears in the status bar.

The SSTrunks network element with the specified name is added as a map symbol under the grouped SSTrunks map symbol in the Network Elements display panel. It is also added under ***Network Elements->SSTrunks*** *in the IEMS Topologies tree.*

You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

The SSTrunks NE can be added using IEMS Web Client. For details, refer to "Adding an SSTrunks NE using Web Client" (page 345).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an SSLines NE

Application

Use this procedure to add an SSLines NE.

IEMS discovers a SSLines NE automatically when its corresponding MCS manager is added to the IEMS topology. The SSLines NE is added as a map symbol under the grouped map symbol in the Network Elements display panel. Also, an SSLines NE is added under the respective network elements under **Network Elements** in the IEMS Topologies tree.

Tasks supported by SSLines NE objects

The following list provides the operations available for SSLines NEs in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The resynchronization of alarms is supported through the MCS manager.

Prerequisites

The following sections list the SSLines NE configuration references required to integrate with the IEMS.

Fault interface:

No additional configuration is required for the SSLines NE.

When adding an MCS Manager for SSLines, ensure the MCS SNMP trap destination is configured in the device for the IEMS to manage its fault interface. Refer to the "Prerequisites" section of "Adding an MCS Manager for SSLines" (page 49).

Configuration interface:

To configure the Apache Web Server on an SPFS-based server for HTTPS proxy, see *ATM/IP Solution-level Configuration*, NN10409-500.

To configure the HTTPS proxy for SSLines, see *Session Server Lines - SIP Voice Basics*, NN10437-111.

Performance management:

No additional configuration is required.

Security configuration:

No additional configuration is required.

Action

Refer to "Adding an MCS Manager for SSLines" (page 49) procedure to add an MCS Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a STORM NE

Application

Use this procedure to add a Storage Management (STORM) NE to the IEMS topology.

STORM NEs can be managed using IEMS by adding them to the IEMS topology.

STORM-IEMS integration is not supported with the STORM dotHill configuration. The dotHill version of the STORM device does not have an SNMP agent to forward or read the faults from the STORM device. IEMS integration is only supported with the STORM-XTS configuration.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for the STORM NE in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms (incremental resync supported)	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Prerequisites

For IEMS to receive STORM fault and performance data

STORM must be configured to send fault data to IEMS. The STORM has a tool called commish which is used to configure the STORM with IEMS server virtual IP address and port for sending the fault data to IEMS; without this configuration, IEMS receives no fault data from STORM. For details, refer to "Configuring STORM for IEMS" (page 157).

For launching STORM Manager

STORM has to be configured using the SPFS CLI tool for launching STORM manager from IEMS Client. For details, refer to *ATM/IP Solution-level Configuration*, NN10409-500.

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 **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **NE** from the Type list box.
5	Select **STORM** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Click the **Next** button.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

8 Enter the port (through which the NE agent communicates with IEMS) in the Port field or retain the default value as 161.

9 Enter the SNMP Agent Community in the Community field.

10 Select SNMP version v3 from the Version list box.

11 Select the security level from SecurityLevel list box. If the value **NoAuthNoPriv** is selected from the SecurityLevel list box, enter the following details:

- User name (default STORM user name is v3admin)
- Context name

If the value **AuthNoPriv** is selected from SecurityLevel list box, enter the following details:

- User name (default STORM user name is v3admin)
- Context name
- Authentication Protocol

If the value **AuthPriv** is selected from SecurityLevel list box, enter the following details:

- User name (default STORM user name is v3admin)
- Context name
- Authentication Protocol
- Privacy Password

12 Click the **Next** button to proceed to the Performance Interface screen in the wizard.

13 Repeat step 8 to step 9.

14 Click the **Finish** button to add the STORM.

Once the STORM is added, a message that reads "Successfully added to database" appears in the status bar.

*The STORM network element with the specified name is added as a map symbol under the grouped STORM map symbol in the Network Elements display panel. It is also added under **Network Elements->STORM** in the IEMS Topologies tree.*

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The STORM can be added using IEMS Web Client. For details, refer to "Adding a STORM NE using Web Client" (page 342) procedure.

Copyright © 2006, Nortel Networks

Configuring STORM for IEMS

Application

Use this procedure to configure a STORM SAM-XTS unit to forward STORM fault information to an IEMS.

Prerequisites

This procedure requires administrator privilege.

Action

Step	Action

At the IEMS workstation

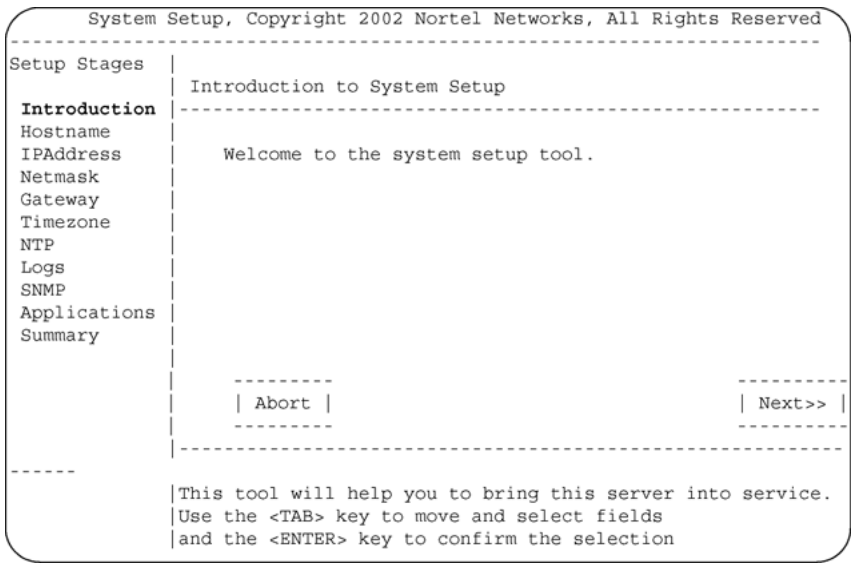
1 Log in to the STORM SAM-XTS unit as the root user by right clicking on the STORM icon and selecting **Launch Command Line** from the context menu.

A console window opens and prompts for a user name. Enter root and press the Return key. Enter the root user password at the next prompt, and press the Return key.

2 Start the commissioning shell:

```
> commish
```

The screen clears and a console menu application starts.



Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If the screen is garbled, press Ctrl+c to exit the application, enter ***export TERM=vt100*** *, press* **Return** *, and start the commish tool again.*

3 Press the **Return** key to accept the existing datafill until the menu advances to the SNMP menu option.

4 On the SNMP menu screen, enter the IP address and port number of IEMS server application and the SNMP user name provisioned at IEMS server application.

SNMP menu option screen

```
      System Setup, Copyright 2002 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------
Setup Stages  |
              | Configure the SNMP Trap destinations (optional)
 Introduction |-----------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter up to 2 SNMP trap destinations
'ipaddr<:port>'
 Netmask      |
 Gateway      |     Trap destination 1
 Timezone     |       []
 NTP          |     Trap destination 2
 Logs         |       []
 SNMP         |     SNMPv3 User Name (eg: v3admin)
 Applications |       []
 Summary      |
              |
              |     ----------                                ----------
              |     | <<Back |                                | Next>> |
              |     ----------                                ----------
              |-------------------------------------------------------------
------
              | Please specify up to 2 destination IP addresses and ports
              | which you want receive SNMP traps. eg: 192.168.5.4:9999
              | Also specify the SNMPv3 user name to use for traps/gets
```

Trap destination should be set to the IEMS virtual IP address. For details on configuring the SNMP traps, see "Configuring traps for SNMP-based devices" (page 368).

5 Press the Return key to accept the SNMP provisioning, and continue pressing the **Return** key to advance to the Summary menu option screen.

6 On the Summary option menu screen, use the tab key to position the cursor on the **Finish** button and then press the **Return** key to commit the provisioning. A reboot is not required.

7 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a UAS NE

Application

IEMS discovers the UAS NE automatically when its corresponding UAS manager is added to the IEMS topology. The UAS network element is added as a map symbol under the grouped UAS map symbol in the Network Elements display panel. It is also added under **Network Elements->UAS** in the IEMS Topologies tree.

The following list provides the operations available for UAS NE in IEMS.

Tasks supported in IEMS for a UAS NE

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

The resynchronization of alarms is supported through the UAS manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Action

Refer to "Adding a Universal Audio Server Manager" (page 77) procedure to add a UAS manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a UMUX NE

Application

Use this procedure to add UMUX NEs.

UNEM manages UMUX 1500, UMUX 1200 and UMUX 900 NEs in the UMUX network. When you add an UNEM, the managed NEs are automatically discovered and added as map symbols under the grouped UMUX-1500, UMUX-1200, and UMUX-900 map symbols respectively in the Network Elements display panel. Also, they are added under **Network Elements->UMUX-1500, UMUX-1200**, and **UMUX-900** respectively in the IEMS Topologies tree.

The following list provides the operations available for UNEM NEs in IEMS.

Tasks supported in IEMS for UNEM NEs

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

Action

Refer to "Adding a UMUX Network Element Manager" (page 74) procedure to add a UNEM.

Copyright © 2006, Nortel Networks

Adding a Universal Signaling Point NE

Application

Use this procedure to add an Universal Signaling Point (USP) NE to the IEMS topology using Java Web Start Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

The following list provides the operations available for USP NE in IEMS.

Task in IEMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	No
Clearing alarms	No	No
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	Yes	No
Report job	Yes	No
Transfer job	Yes	No
Configuring thresholds	Yes	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Others operations		
Launching corresponding applications	Yes	No

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Tools-->Add-->EMS/NE** menu command to invoke the Add EMS/NE wizard.
3	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields.
4	Select **NE** from the Type list box.
5	Select **USP** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the flavour of the USP NE from the Flavour list box. Based on the selected flavour, the corresponding USP Manager is associated to the USP NE map symbol. For launching the USP Manager, refer to "Launching USP Manager for USP NE" section of "Launching applications for USP NE" in *IEMS Overview*, NN10329-111.
8	Enter the client server IP address in the Client Server IP field.
9	Enter the inactive agent IP address in the Unit1 field.
10	Click the **Next** button. When adding a USP NE to the IEMS inventory the SNMP attributes (refer to step 11 to step 15) must align with the configuration of the USP network element. In addition, the manager IP address in the USP must be configured to forward its SNMP traps to the IEMS Server application (the IEMS Virtual IP address). The configuration of the SNMP attributes in the USP are described in *USP Administration and Security*, NN10159-611 and *USP Compact Administration and Security*, NN10160-611.
11	Enter the port value `161` (in which the NE agent communicates with IEMS) in the Port field.
12	Select the SNMP version from the Version list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The SNMP version must align with the version configured in the USP Network Element. The default SNMP version in the USP is V3.

If the SNMP version is	Do
v3	follow step 13 to step 14 and proceed to step 16
v2	proceed to step 15

13 Retain the value "NoAuthNoPriv" for the Security Level list box.

14 Enter the value for the User name field as specified in the *USP Administration and Security guide*, NN10159-61.

The value for the Context name field must be left blank.

15 Enter the community string in the Community field.

16 Click the **Next** button to proceed to the Standby Fault Interface screen in the wizard.

17 Repeat step 11 to step 15.

18 Click the **Next** button.

The Performance Interface panel asking for performance interface details is displayed.

19 Type the user name for FTP PULL in the User ID field.

20 Type the password in the Password field.

21 Click the **Finish** button to add the USP NE.

Once the USP NE is added, a message that reads "Successfully added to database" appears in the status bar.

The USP network element with the specified name is added as a map symbol under the grouped USP map symbol in the Network Elements display panel. It is also added under ***Network Elements->USP*** *in the IEMS Topologies tree*.

Only the active USP unit object provides an interface to determine the fault state of the USP. The inactive USP unit object status is in unknown state (map symbol has gray background color). The IEMS dynamically detects when the USP unit has been swacted. When this occurs, it initiates alarm resync with the newly active USP unit and updates the state of the USP unit objects in the IEMS Client to reflect this change in activity. When this occurs, the previous active unit object map is changed to unknown state, and the new active unit is updated to reflect the highest alarm state of the USP device. For

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

the color mapping of various object status, refer to "Significance of map symbol background color" (page 230) table of "Updating status of objects manually" (page 230).

You have completed this procedure.

—End—

The USP NE can be added using IEMS Web Client. For details, refer to "Adding a USP NE using Web Client" (page 348).

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Editing object properties

The following object properties can be modified after they are added to the topology.

- Display name
- Managed or Unmanaged
- Time zone
- Poll interval
- Fault interface and performance interface details, such as port, user ID, community (only applicable to the element manager and NE objects).

For the following auto-discovered element objects and element managers that have auto-discovered child nodes, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines. To change the IP address of these objects, you must delete and then re-add the appropriate element manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Editing platform object properties

Application

Use this procedure to edit the properties of the following EMS platforms:

- SPFS
- MDM

After adding an EMS platform to IEMS, the added EMS platform object properties can be modified.

For the following auto-discovered element objects and element managers that have auto-discovered child nodes, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines, MG 7480/15000/20000, MSS 15000. To change the IP address of these objects, you must delete and then re-add the appropriate element manager.

Only the Display Name property for the SDM platform can be modified. To edit the display name, double-click the required SDM platform map symbol and change the name and click the **Modify** button.

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 **EMS Platforms** panel under the IEMS Topologies tree in which the required map symbol is shown.
3	Select the required platform map symbol in the EMS Platforms panel and double-click to launch the Object Properties wizard.
4	Select your next step.

If you want to	Do
edit the platform object properties	step 5
up-version the platform objects	step 6

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Edit the following properties if required. For description of the properties, refer to the following table:

Field	Description
Display Name	The name displayed in the topology for the map symbol.
Managed	Indicates whether the object is managed or unmanaged.
IP-Address	The IP address of the platform host. If the IP address is modified and updated, IEMS deletes the existing details of the platform object and adds a new object with details provided in the Object Properties wizard screen.
Time Zone	The time zone associated with the Host Name or IP Address provided.
Device Version	The version of platform.
Poll Interval	The Poll Interval for status updates and the interval to check whether the host is active or not. The poll interval value must be in the range 30 to 3600 or 0. If the value 0 is specified, the polling is disabled, and the status of the object can be updated using "Updating status of objects manually" (page 230).

6 Change the version of the platform to a higher version from the **Version** list box.

7 Click the **Modify** button to modify the platform object properties.

Once the platform object properties is updated in topology, the message "Successfully updated to database" appears in the status bar.

8 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Editing element manager object properties

Application

Use this procedure to edit the element manager managed object properties.

After adding an element manager to IEMS, you can modify the element manager object properties.

For the following auto-discovered element objects and element managers that have auto-discovered child nodes, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines, MG 7480/15000/20000, MSS 15000, MCS Manager, and FPM Manager. To change the IP address of these objects, you must delete and then re-add the appropriate element manager

After adding an MCS Manager, the fault interface and performance details are associated to corresponding physical SM servers which are added in the MCS SM(XXX) node (MCS SM node with the parent MCS Manager display name) under the Element Managers topology. Hence the fault interface and performance details cannot be modified for MCS Manager map symbol in the Element Managers topology. It can be modified only for corresponding physical SM servers in MCS SM(XXX) node. If you try to edit the managed object properties of an MCS Manager, the **Next** button is disabled in Object 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 **Element Managers** topology panel in the IEMS Topologies tree. For FPM or MCS Manager, select the corresponding node (MCS_FPM(<parent MCS display name>:<FPM display name>) or MCS SM(XXX) node, where XXX is the display name) under the Element Managers topology.
3	Right click the required map symbol and select the **View Children** menu item.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

4 Select the required map symbol and double-click to launch the Managed Object Properties window.

5 Select your next step.

If you want to	Do
edit the object properties	step 4
up-version the element manager properties	step 12

6 Edit the following properties if required. The description of the properties is shown in the following table.

Field	Description
Display Name	The name displayed in the topology for the map symbol.
Managed	Indicates whether the object is managed or unmanaged
Platform	Indicates the element manager to which the object belongs.
IP-Address	The IP address of the element manager host. If the IP address is modified and updated, IEMS deletes the existing details of the element manager object and adds a new object with details provided in the Object Properties wizard screen. This is not applicable for MCS Manager objects as only the details are updated for MCS Manager objects.
Time Zone	The time zone associated with the Host Name or IP Address provided.
Device Version	The version of element manager.
Poll Interval	The Poll Interval for status updates, and the interval for checking the connection to determine whether the host is active. If the value 0 is specified, the polling is disabled and the status of the object can be updated using "Updating status of objects manually" (page 230).

7 Click the **Next** button if available.

8 Modify the fault interface details if required.

9 Click the **Next** button if available.

10 Modify the performance interface details if required.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

11 Go to step 13.

12 Change the version of element manager to higher version from the Version list box.

To change the device version for SSLines element manager, you must delete and then re-add SSLines element manager.

13 Click the **Modify** button to modify the manager object properties.

Once the manager object is updated with the provided details in the topology, a "Successfully added to database" message appears in the status bar.

14 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Editing EMS application object properties

Application

Use this procedure to edit EMS application object properties.

After adding EMS applications to IEMS, the added EMS application object properties can be modified.

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 **EMS Applications** topology panel in the IEMS Topologies tree in which the required map symbol is shown.
3	Select the required EMS application map symbol and double-click to launch the Object Properties window.
4	Edit the following properties if required.

Field	Description
Display Name	The name displayed in the topology for the map symbol.
Managed	Indicates whether the object is managed or unmanaged
Platform	The EMS application to which the object belongs.
IP-Address	The IP address of the EMS application host. If the IP address is modified and updated, IEMS deletes the existing details of the element manager object and adds the new object with details provided in the Object Properties wizard screen.
Time Zone	The time zone associated with the Host Name or IP Address provided.
Device Version	The version of EMS application.

For all EMS application type objects, the interval provided in the Poll Interval field is not used.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Click the **Modify** button to modify the EMS application object properties.

Once the EMS application details are updated in the topology, "Done" appears in the status bar.

6 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Editing NE object properties

Application

Use this procedure to edit the network element managed object properties or to up-version the NE objects.

After adding an NE to IEMS, the added NE object properties can be changed.

For the following auto-discovered element objects and element managers that have auto-discovered child nodes, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines. To change the IP address of these objects, you must delete and then re-add the appropriate element manager.

You cannot modify the IP address for the MG 7480/15000/20000 or MSS 15000.

Only the poll interval, managed, and IP address values can be modified for automatically discovered NEs. For a list of automatically discovered NEs, see "Launching applications for IEMS" in *IEMS Overview*, NN10329-111.

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 Elements** topology panel in the IEMS Topologies tree in which the required map symbol is shown.
3	Right click the required map symbol and select the **View Children** menu item.
4	Select the required NE map symbol and double-click to launch the Object Properties window.
5	Select your next step.

If you want to	Do
edit the NE managed object properties	step 6
up-version the NE objects	step 12

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

6 Edit the following properties if required.

Field	Description
Display Name	The name displayed in the topology for the map symbol.
Managed	Indicates whether the object is managed or unmanaged.
Platform	The NE to which the object belongs.
IP-Address	The IP address of the NE host. If the IP address is modified and updated, IEMS deletes the existing details of the NE object and adds the new object with details provided in the Object Properties wizard screen
Time Zone	The time zone associated with the Host Name or IP Address provided.
Device Version	The version of NE.
Poll Interval	The Poll Interval for status updates, and the interval for checking the connection to know whether the host is active or not. If the value 0 is specified, the polling is disabled and the status of the object can be updated using "Updating status of objects manually" (page 230).

7 Click the **Next** button.

8 Modify the fault interface details if required.

9 Click the **Next** button.

10 Modify the performance interface details if required.

11 Go to step 14.

12 Change the version of the NE to a higher version from the **Version** list box.

13 Click the **Modify** button to modify the NE object properties.

Once the NE object properties are updated, a "Successfully updated in database" message appears in the status bar.

14 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring and maintaining MS 2000 devices

The MS2000 Maintenance and Configuration tool is used to configure and perform some configuration and maintenance activities on an MS 2010 or MS 2020 NE. It automatically adjusts the display components, behavior, and configuration options based on the NE type (MS 2010 or MS 2020). This section describes configuration and maintenance operations for MS 2000 NEs:

- To launch the MS 2000 Maintenance and Configuration tool, see Launching applications for an MS 2000 NE in *IEMS Overview*, NN10329-111.
- Configuration
  - "Configuring general parameters for MS 2000 NEs" (page 179)
  - "Configuring SNMP setup for MS 2000 NEs" (page 182)
  - "Configuring the passwords for the MS 2000 NEs" (page 186)
  - "Configuring automated backup of the INI file" (page 189)
  - Configuring IPSec and IKE for IEMS and MS 2000 secure messaging in *Media Server 2000 Series Configuration*, NN10340-511
  - Configuring IPSec and IKE for MS 2000 and GWC secure messaging in *Media Server 2000 Series Configuration*, NN10340-511
  - Editing the Preshared key on the MS 2000, *Media Server 2000 Series Configuration*, NN10340-511
  - Disabling IPSec on the MS 2000 in *Media Server 2000 Series Configuration*, NN10340-511
- Maintenance
  - "Locking or unlocking the MS 2000 node" (page 191)
  - "Backing up the INI file" (page 192)
  - "Uploading the load files to the IEMS Server" (page 195)
  - "Resetting the MS 2000 NE" (page 193)

Copyright © 2006, Nortel Networks

User access privileges for MS 2000 NE

The user authorization required for each function is given in the following table:

Access	Function
mg groups with any access	List of any configuration
mgsprov, mgrw, mgadm	Change configuration
mgmtc, mgrw, mgadm	Lock or unlock of device
mgmtc, mgrw, mgadm	Backup of INI file
mgmtc, mgrw, mgadm	Upload of load files (CMP, INI, DAT, XML)
mgmtc, mgrw, mgadm	Soft reset of NE
mgadm, mgrw	Change SNMP passwords
mgadm, mgrw	Change web interface passwords

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring parameters for MS 2000 NEs

Application

Use this procedure to configure the general parameters to setup the MS 2000 node.

Action

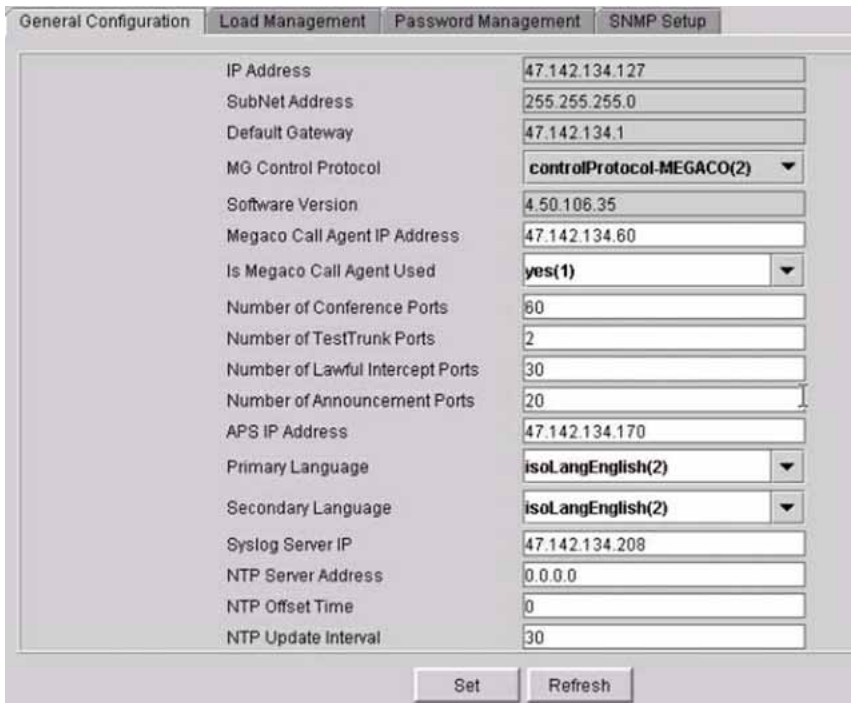
Step	Action

At the IEMS workstation

1 Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111.

The Maintenance and Configuration tool is launched.

2 Click the **General Configuration** tab, as shown in the following figure.



3 Modify the Megaco Call Agent IP address in the Megaco Call Agent IP Address field.

4 To indicate whether Megaco Call Agent is used, select **yes** or **no** from the Is Megaco Call Agent Used field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Enter the number of conference ports in the Number of Conference Ports field.

6 Enter the number of test trunk ports in the Number of TestTrunk Ports field.

7 Enter the number of lawful intercept ports in the Number of Lawful Ports field.

8 Enter the number of announcement ports in the Number of Announcement Ports field.

9 Enter the APS IP address in the APS IP Address field.

10 Select the primary language from the Primary Language list box.

11 Select the secondary language from the Secondary Language list box.

12 Enter the SYSLOG Server IP address in the Syslog Server IP Address field.

13 Select the ATM default application type from the ATM Default Application Type list box.

14 Select the transmission mode from the Transmission mode list box.

15 Click the **Set** button to save the configuration changes.

If valid data is entered in the each of fields, then you are prompted to save the configuration changes made by backing up the INI file.

If invalid data is entered, the following error message is displayed:

"An INI backup should be done in order to save the configuration changes. When backing up configuration changes it is recommended that the INI file be copied to the tftp server so that if a device reboot occurs, it will initialize with the latest configuration settings. Would you like to backup the INI file now?"

16 Click the **Backup to tftp server and IEMS server** button or **Backup to IEMS server only** button. You can back up either to the IEMS server or to the tftp server. If you click the **Backup to tftp server and IEMS server** button, the INI file is saved to the SDM/CBM and IEMS server.

Once the INI backup is done, you are prompted to perform a soft reset on the node to save the configuration changes to flash memory.

17 Click the **Perform Soft Reset** button.

You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks

Configuring SNMP setup for MS 2000 NEs

This subsection describes the following procedures to configure the SNMP setup for the MS 2000 node. Once performed, the procedures allow you to manage the Trusted Managers table and the Trap Destination Table. The MS 2000 node can handle up to five entries in each of these tables. This subsection consists of two procedures:

- "Configuring Trusted Managers table" (page 182)
- "Configuring Trap Destinations table" (page 183)

Configuring Trusted Managers table

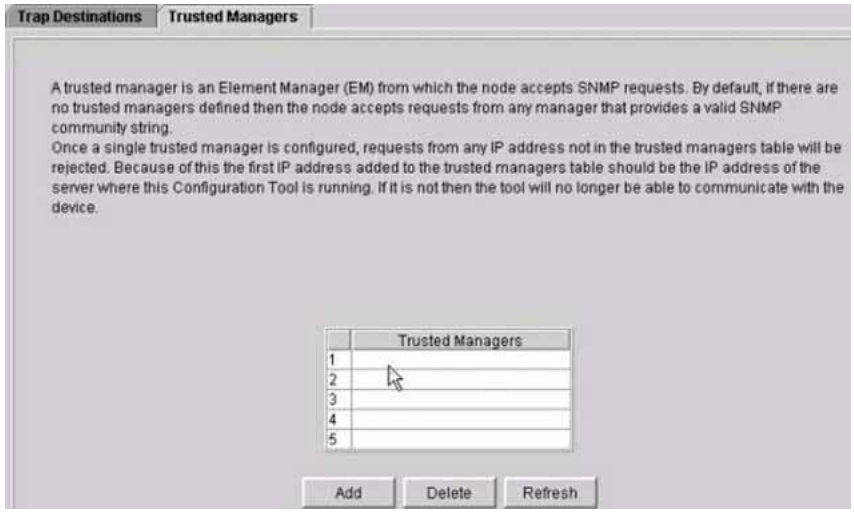
Application

Use this procedure to configure the Trusted Managers table for MS 2000 node.

Action

Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*
2	Click the **SNMP Setup** tab in the right side of the screen.
3	Click the **Trusted Managers** tab. *The Trusted Managers tab is displayed as in the following figure.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



4 Enter the manager IPs in the rows under the Trusted Managers column. Enter the IEMS virtual IP address first, then the platform logical IP address. In an HA configuration, the logical IP address is the cluster IP. In a simplex configuration, the logical IP address is the physical IP.

5 Repeat step 4 to add more trusted managers.

6 Click the **Add** button.

To remove a trusted manager, enter the trusted manager IP and click the **Delete** button.

7 You have completed this procedure.

—End—

Configuring Trap Destinations table

Application

Use this procedure to configure the Trap Destinations table.

Action

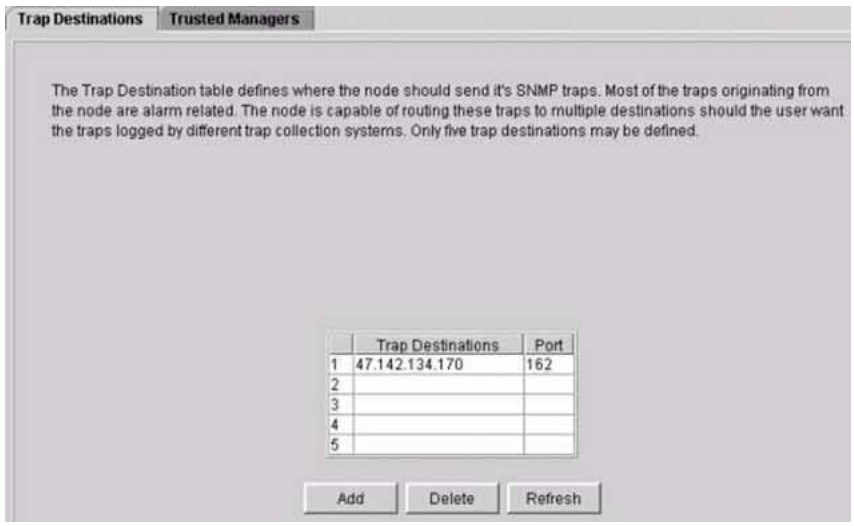
Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2 Click the **SNMP Setup** tab in the right side of the screen.

3 Click the **Trap Destinations** tab.

The Trap Destination tab is displayed as in the following figure.



4 Enter the trap destination IP in the rows under the Trap Destinations column. The trap destination IP is the IEMS virtual IP address.

5 Enter the SNMP trap port for the corresponding trap destination under the **Port** column.

6 Repeat step 4 and step 5 to add more trap destinations.

7 Click the **Add** button.

To delete the trap destination

8 Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111.

The Maintenance and Configuration tool is launched.

9 Click the **SNMP Setup** tab in the right side of the screen.

10 Click the **Trap Destinations** tab.

11 Enter the SNMP trap port for the corresponding trap destination under the Port column.

12 Enter the trap destination IPs in the row under the Trap Destinations column.

13 Repeat step 11 and step 12 to delete more trap destinations.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

14 Click the **Delete** button.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring the passwords for the MS 2000 NEs

This subsection describes the following procedures to configure the SNMP read and write community strings for the MS 2000 node and the Web server user name and password for MS 20000 node:

- "Configuring SNMP community strings" (page 186)
- "Configuring Web server password" (page 187)

Configuring SNMP community strings

Application

Use this procedure to configure the SNMP community strings for MS 2000 node.

Action

Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*
2	Click the **Password Management** tab in the right side of the screen.
3	Click the **SNMP** tab. *The SNMP tab is displayed as shown in the following figure.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

4 Enter the same read community string in the Read String field.

5 Enter the same read community string in the Confirm field in the Read Community String panel.

6 Click the **Change Read String** button.

The read community string is updated.

To configure the write community string

7 Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111.

The Maintenance and Configuration tool is launched.

8 Click the **Password Management** tab in the right-side of the screen.

9 Click the **SNMP** tab.

10 Enter the write community string in the **Write String** field.

11 Enter the same write community string again to confirm in the **Confirm** field in the Read Community String panel.

12 Click the **Change Write String** button.

The write community string is updated.

13 You have completed this procedure.

—End—

Configuring Web server password

Application

Use this procedure to configure the Web server password.

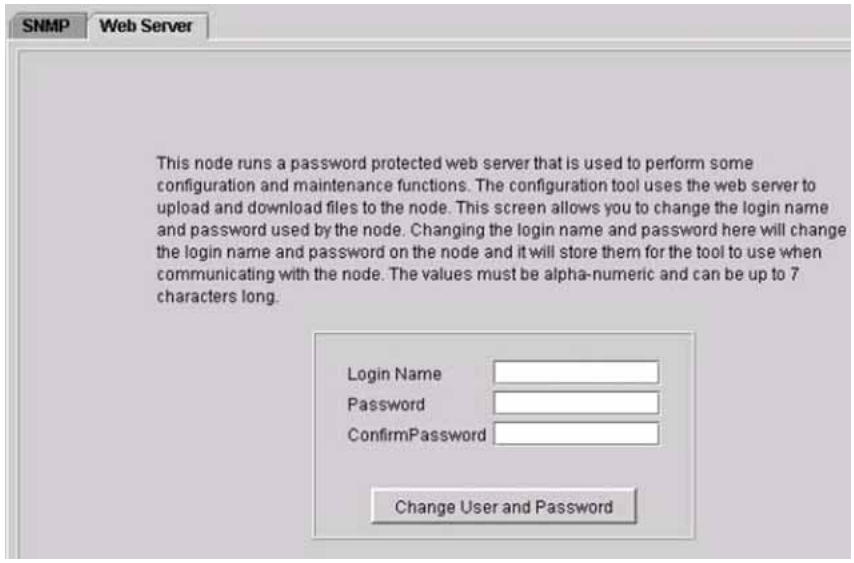
Action

Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*
2	Click the **Password Management** tab in the right side of the screen.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

3 Click the **Web Server** tab.

The Web Server tab is displayed as in the following figure.



4 Enter the login name in the Login Name field.

5 Enter the password in the Password field in the Read Community String panel.

6 Enter the same password in the Confirm field.

7 Click the **Change User and Password** button.

The password is updated.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring automated backup of the INI file

Application

Use this procedure to configure automated backup of the INI file.

The initialization file is a configuration data file used by the MS 2000 system to set up the node in event of a reboot. The automated backup of the INI file can be configured using the Automated INI File Backup Configuration GUI. The INI file backup is configured based on the time and day you specify in the Automated INI File Backup Configuration tool.

If the proper communication is not setup between the IEMS and the tftp server (SDM or CBM), then the backup of the INI file to the tftp server fails. If file backup failures to the tftp server are seen and you suspect this communication has not been setup, refer to "Setting up the BootP file on SPFS" in *Nortel Carrier Voice over IP Upgrade and Patches*, NN10440-450.

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 **MS 2000** topology panel under the Network Elements in the IEMS Topologies tree in which the required map symbol is shown.
3	Right-click a map symbol and select the **Configure MS2000 Automated INI Backup** tool. *The Automated INI File Backup Configuration tool is launched.*
4	Check the **Enable Automated INI file backup:** check box to enable the automated INI file backup.
5	Select the start time for backup from the Automated INI Backup Start Time: list box.
6	Select the **Daily** option under Recurrence for daily backup. OR Select the **Weekly** option and select the days of the week in which the backup must occur.
7	Click the **OK** button.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Locking or unlocking the MS 2000 node

Application

Use this procedure to lock or unlock the MS 2000 node.

The lock function is to prevent any audio resources from being allocated on the node.

Action

Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*
2	Select the **Graceful Lock** option to lock the MS 2000 node with graceful lock. **Graceful lock** A graceful lock signals to the node that a lock has been requested. The node then stops allocating new audio resources and waits for the last resource to be freed before actually locking the node. OR Select the **Forced Lock** option to lock the MS 2000 node with forced lock. **Forced lock** A forced lock causes the node to immediately free up any resources in use and lock the node.
3	Click the **Lock** button to lock the MS 2000 node. To unlock the MS 2000 node, click the **Unlock** button. You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Backing up the INI file

Application

Use this procedure to back up the INI file.

The initialization file is a configuration data file used by the MS 2000 system to set up the node in event of a reboot. The file contains all of the user-defined configuration changes. The Maintenance and Configuration tool allows you to save the initialization file back to the IEMS server or to the tftp server (the SDM or CBM). By saving the INI file in the IEMS server, you have simply saved a backup copy of the configuration changes for later use. The Maintenance and Configuration tool saves up to five initialization files for each node, deleting the oldest file once the maximum number of files have been saved. By saving the file to the tftp server, this updates the initialization file that the MS 2000 node retrieves and a hard reset occurs.

Action

Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*
2	Select the **Backup to IEMS server only** option to save the INI file to the IEMS server only. OR Select the **Backup INI to tftp server and IEMS server** option to save the INI file to the TFTP and IEMS servers. It is recommended that whenever configuration changes are made, back up the latest settings in an INI file to the tftp server.
3	Click the **INI Backup** button. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Resetting the MS 2000 NE

Application

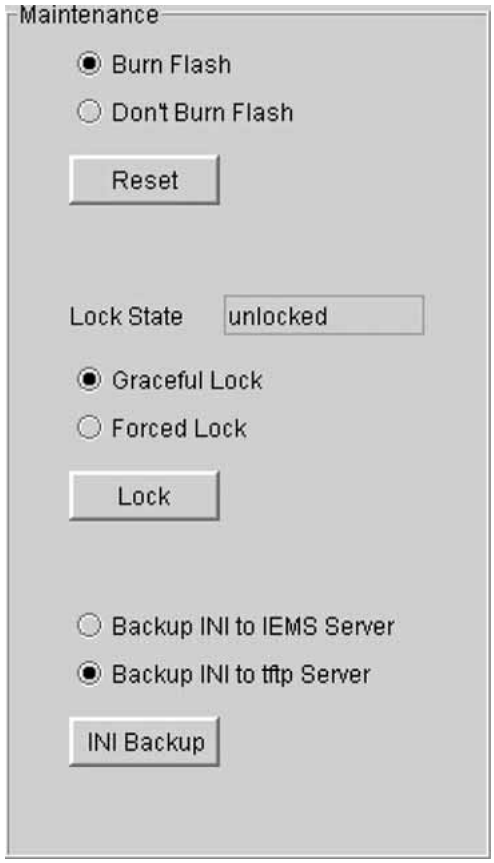
Use this procedure to reset the MS 2000 NE.

A soft reset of the node is reinitialization of the software running on the MS 2000 NE. You can select either to burn configuration settings or to re-initialize with the previous burned settings. When a soft reset is done on the node with the burn option, the existing configuration settings are burned into flash memory and then the NE goes through an initialization cycle. This takes the MS 2000 NE out of service for a short period of time and drops any resources in use.

Action

Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to of "Configuring and maintaining MS 2000 devices" (page 177). *The Maintenance and Configuration tool is launched. The Maintenance panel in the left side of the Maintenance and Configuration appears similar to the following figure:*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



2 Select the **Burn Flash** option to reset the MS 2000 NE with the burn option.

OR

Select the **Don't Burn Flash** option to reset the MS 2000 NE without the burn option.

3 Click the **Reset** button.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Uploading the load files to the IEMS server

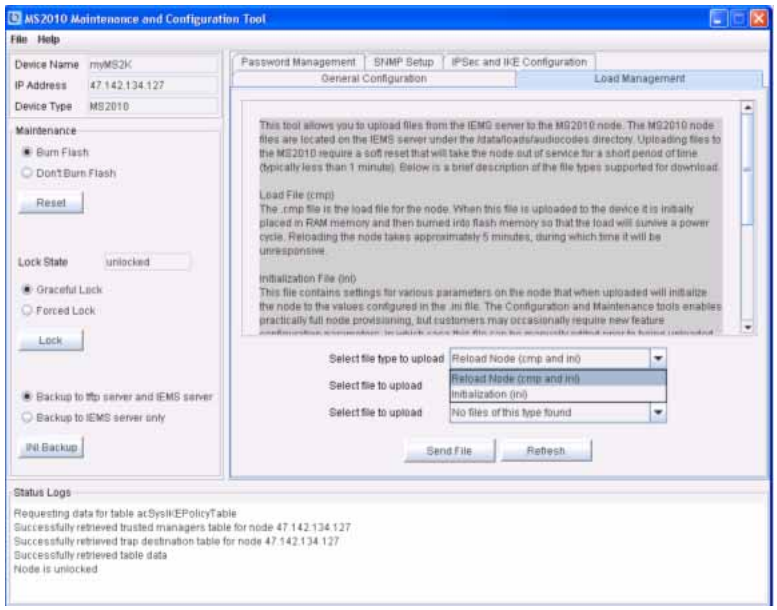
Application

Use this procedure to upload the load files to the IEMS server.

The MS2000 Configuration and Maintenance tool lets the user upload some of the file types used by the MS 2000 node. The files displayed in the tool are uploaded from the /data/loads/audiocodes folder of the IEMS server. The Maintenance and Configuration tool provides an option to remotely reload the device by downloading a CMP load file and an INI initialization file.

Action

To upload the selected files to the IEMS server, follow these steps:

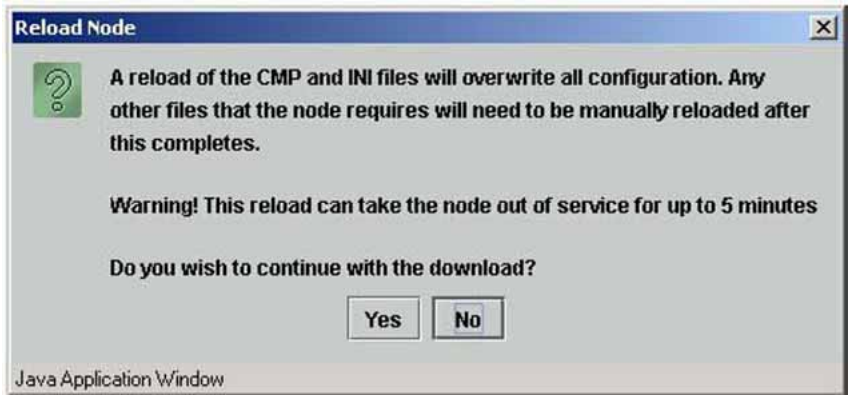
Step	Action
	At the IEMS workstation
1	Launch the Maintenance and Configuration tool. For details, refer to to Launching applications for an MS2000 NE in *IEMS Overview*, NN10329-111. *The Maintenance and Configuration tool is launched.*
2	Click the **Load Management** tab in the right-side of the screen similar to the following figure: 

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

3 Select the CMP file to be reloaded and INI file which has to be uploaded from the first panel.

4 Click the **Send Files** button in the first panel.

The following dialog is displayed when you select this option:



5 Click the **Yes** button to reload the CMP and INI files.

6 In other panels, select the files to be uploaded from the list box and click the **Send Files** button against the list box.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring and maintaining the MG 3200 devices

The MG 3200 Configuration and Maintenance tool is used to configure and perform some configuration activities on MG 3200 NE. This section provides the following configuration and maintenance operations for MG 3200 NEs:

- Configuration operations
  - "Configuring IKE parameters for MG 3200 NEs" (page 199)
  - "Configuring IPSec parameters for MG 3200 NEs" (page 204)
  - "Enabling and disabling the IPSec for MG 3200" (page 209)
  - "Configuring automated backup of the INI file for MG 3200" (page 211)
- Maintenance operations
  - "Resetting the MG 3200 NE" (page 213)

Configure the IKE parameters and then change the IPSec parameters.

Launching the IPSec and IKE Configuration tool

Application

Use this procedure to launch the IPSec and IKE Configuration tool.

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 **MG 3200** topology panel under Network Elements in the IEMS Topologies tree in which the required map symbol is shown.
3	Right-click a map symbol and select the **IPSec and IKE Config Tool**.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The MG 3200 IPSec and IKE Configuration tool is launched.

4 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring IKE parameters for MG 3200 NEs

This subsection describes how to configure the IKE parameters for the MG 3200 NE.

Adding an entry to IKE Configuration table

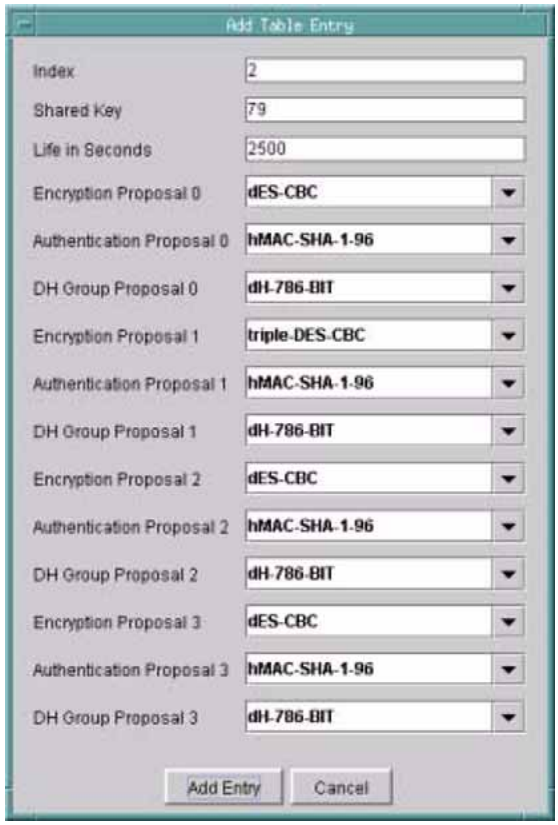
Application

Use the procedure to add an entry to IKE Configuration table.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the **IKE Configuration** tab.
3	Click the **Add Entry** button. *The Add Table Entry window opens.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



4 Enter the index in the Index field. (The value must be an integer in the range 0-19.)

Example
1

5 Enter the shared key in the Shared Key field. (The value must be a string.)

6 Enter the lifetime (in seconds), for security association derived from this policy, in the Life in Seconds field.

Example
600

7 Select the proposal encryption number from the Encryption Proposal 0 list box.

8 Select the proposal authentication number from the Authentication Proposal 0 list box.

9 Select the proposal number from the DHGroup Proposal 0 list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 Select the proposal encryption number from the Encryption Proposal 1 list box.

11 Select the proposal authentication number from the Authentication Proposal 1 list box.

12 Select the proposal number from the DHGroup Proposal 1 list box.

13 Select the proposal encryption number from the Encryption Proposal 2 list box.

14 Select the proposal authentication number from the Authentication Proposal 2 list box.

15 Select the proposal number from the DHGroup Proposal 2 list box.

16 Select the proposal encryption number from the Encryption Proposal 3 list box.

17 Select the proposal authentication number from the Authentication Proposal 3 list box.

18 Select the proposal number from the DHGroup Proposal 3 list box.

19 Click the **Add Entry** button to add a row to the IKE Configuration table.

A row is added with the details provided.

20 You have completed this procedure.

—End—

Editing an entry in the IKE Configuration table

Application

Use this procedure to edit an entry in the IKE Configuration table.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2 Select the row from the IKE Configuration table which has to be edited.

3 Click the **Edit Entry** button.

The Edit Table Entry window is invoked.

4 Follow step 4 to step 17 of "Adding an entry to IKE Configuration table" (page 199) procedure.

5 Click the **Save** button.

6 Click the **Refresh Table** button.

The row is updated in IPSec Configuration table with the details provided.

7 Reset the MG 3200 to enable the new pre-shared key and any other modified values. Refer to "Resetting the MG 3200 NE" (page 213) for the procedure to reset the MG 3200.

8 You have completed this procedure.

—End—

Deleting an entry from the IKE Configuration table

Application

Use this procedure to delete an entry from the IKE Configuration table.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the row in the IKE Configuration table which has to be removed.
3	Click the **Delete Entry** button. *The selected row is deleted from the IPSec Configuration table.*
4	Reset the MG 3200. Refer to "Resetting the MG 3200 NE" (page 213) for the procedure to reset the MG 3200. You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks

Configuring IPSec parameters for MG 3200 NEs

This subsection describes how to configure the IPSec parameters for the MG 3200 NE.

Adding an entry to IPSec Configuration table

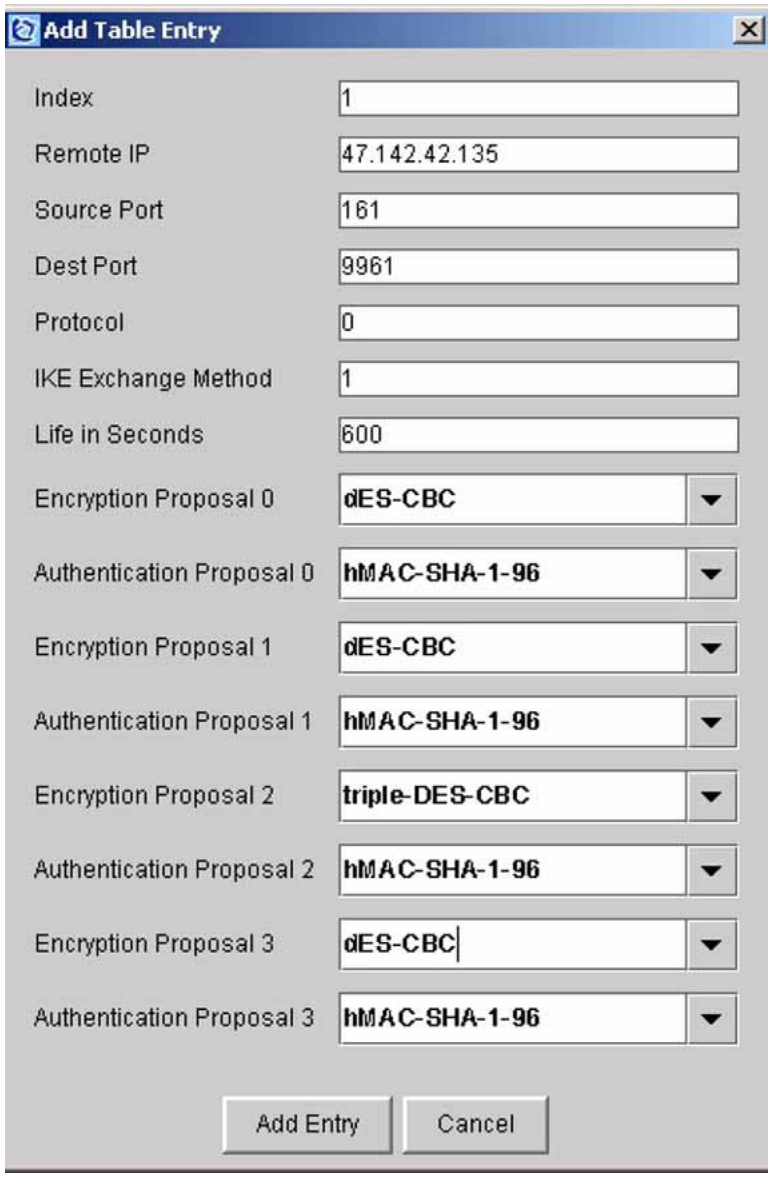
Application

Use this procedure to add an entry to the IPSec Configuration table.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the **IPSec Configuration** tab (if required).
3	Click the **Add Entry** button. *The Add Table Entry window opens*.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



The value for the fields must be provided based on the desired IPSec configuration for the lab. Ensure that the values provided match the selections made during the MG 3200 configuration.

4 Enter the index in the Index field. The value must be an Integer in the range 0-19.

Example
1

5 Enter the destination IP address or DNS name in the Remote IP field.

If the DNS is given for this make sure the DNS server is configured.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Example
47.142.42.135

6 Enter the source port in the Source Port field. Enter the value "0" if all the ports match.

Example
161

7 Enter the destination port in the Dest Port field. Enter the value "0" if all the ports match.

Example
9961

8 Enter the protocol type in the Protocol field.

If the protocol is	Do
UDP	enter the value 17
TCP	enter the value 6
All protocols match	enter the value 0

9 Enter the index for the corresponding IKE entry in the Exchange Method field. The values must be an integer.

Example
1

10 Enter the lifetime (in seconds), for security association derived from this policy, in the Life in Seconds field.

Example
600

11 Select the proposal encryption number from the Encryption Proposal 0 list box.

12 Select the proposal authentication number from the Authentication Proposal 0 list box.

13 Select the proposal encryption number from the Encryption Proposal 1 list box.

14 Select the proposal authentication number from the Authentication Proposal 1 list box.

15 Select the proposal encryption number from the Encryption Proposal 2 list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

16 Select the proposal authentication number from the Authentication Proposal 2 list box.

17 Select the proposal encryption number from the Encryption Proposal 3 list box.

18 Select the proposal authentication number from the Authentication Proposal 3 list box.

19 Click the **Add Entry** button to add a row to the IPSec Configuration table.

A row is added with the details provided.

20 After configuring the parameters for IPSec and IKE Configuration table, Enable the IPSec using the "Enabling and disabling the IPSec for MG 3200" (page 209) procedure.

21 You have completed this procedure.

—End—

Editing an entry in the IPSec Configuration table

Application

Use this procedure to edit an entry in the IPSec Configuration table.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the row from the IPSec Configuration table which has to be edited.
3	Click the **Edit Entry** button. *The Edit Table Entry window is invoked as in the following figure.*
4	Follow step 9 to step 18 of "Adding an entry to IPSec Configuration table" (page 204) procedure.
5	Click the **Save** button.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

6 Click the **Refresh Table** button.

The row is updated in IPSec Configuration table with the details provided.

7 Reset the MG 3200 to enable the new preshared key and any other modified values. Refer to "Resetting the MG 3200 NE" (page 213) for the procedure to reset the MG 3200.

8 You have completed this procedure.

—End—

Deleting an entry from the IPSec Configuration table

Application

Use this procedure to delete an entry from the IPSec Configuration table.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the row from the IPSec Configuration table which has to be removed.
3	Click the **Delete Entry** button. *The selected row is deleted from IPSec Configuration table.*
4	Reset the MG 3200. Refer to "Resetting the MG 3200 NE" (page 213) for the procedure to reset the MG 3200. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Enabling and disabling the IPSec for MG 3200

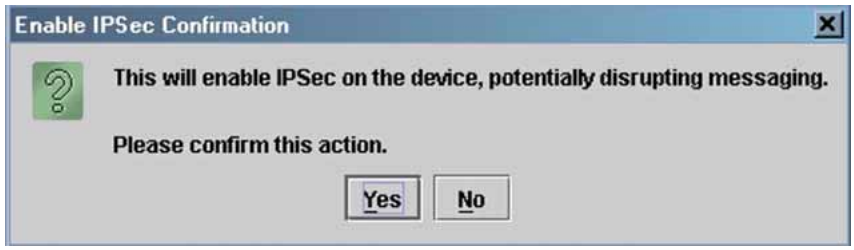
This subsection provides the procedures on how to enable or disable the IPSec for MG 3200.

Enabling IPSec for MG 3200

Application

Use this procedure to enable IPSec for MG 3200.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the **Enable IPSec** field to enable the SSL communication between IEMS Server and MG 3200 NE. *The following dialog is invoked:* 
3	Select the **Yes** button. After receiving the message indicating successful enabling of IPSec, the MG 3200 needs to be reset. Refer to "Resetting the MG 3200 NE" (page 213) for the procedure to reset the MG 3200.
4	You have completed this procedure.

—End—

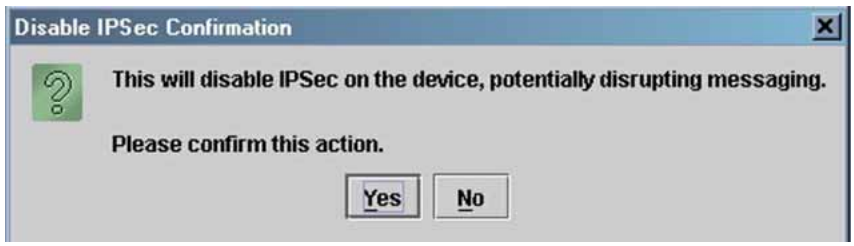
Disabling IPSec for MG 3200

Application

Use this procedure to disable IPSec for MG 3200.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Deselect the **Enable IPSec** field to disable the SSL communication between IEMS Server and MG 3200 NE. *The following dialog is invoked:* 
3	Select the **Yes** button. After receiving the message indicating successful enabling of IPSec, the MG 3200 needs to be reset. Refer to "Resetting the MG 3200 NE" (page 213) for the procedure to reset the MG 3200. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring automated backup of the INI file for MG 3200

Application

Use this procedure to configure automated backup of the INI file for MG 3200.

The initialization file is a configuration data file used by the MG 3200 system to set up the node in event of a reboot. The automated backup of the INI file can be configured using the Automated INI File Backup Configuration GUI. The INI file backup is configured based on the time and day you specify in the Automated INI File Backup Configuration tool.

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 **MG 3200** topology panel under the Network Elements in the IEMS tree.
3	Right-click a map symbol and select the **Configure MG 3200 Automated INI Backup** tool. *The Automated INI File Backup Configuration tool is launched.*
4	Check the **Enable Automated INI file backup:** check box to enable the automated INI file backup.
5	Select the start time for backup from the Automated INI Backup Start Time: list box.
6	Select the **Daily** option under Recurrence for daily backup. OR Select the **Weekly** option and select the days of the week in which the backup must occur.
7	Click the **OK** button. *The INI file is backed up in the /data/loads/audiocodes/<MG 3200 IP>/ <current time>.ini in the host where the IEMS Server is installed.* You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks

Resetting the MG 3200 NE

Application

Use this procedure to reset the MG 3200 NE.

A soft reset of the node refers to the re-initialization of the software running on the MG 3200 NE. You can select either to burn configuration settings or to re-initialize with the previous burned settings. When a soft reset is done on the node with the burn option, the existing configuration settings are burned into flash memory and then the NE goes through an initialization cycle. This takes the MG 3200 NE out of service for a short period of time and drops any resources in use.

Action

Step	Action
	At the IEMS workstation
1	Launch the IPSec and IKE Configuration tool. For details, refer to "Launching the IPSec and IKE Configuration tool" (page 197) of "Configuring and maintaining the MG 3200 devices" (page 197). *The MG 3200 IPSec and IKE Configuration tool is launched.*
2	Select the **Burn Flash** option to reset the MG 3200 NE with the burn option. OR Select the **Don't Burn Flash** option to reset the MG 3200 NE without the burn option.
3	Click the **Reset** button. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Working with CEM managed nodes

This section provides procedures on how to add and delete the CEM managed node.

Copyright © 2006, Nortel Networks

Creating a CEM managed node instance

Application

Use this procedure to set up a managed node instance of CEM in order to manage network elements.

Use the Commissioning Manager CLI to configure CEM managed node instances. After installing the CEM package onto a Sun server, users need to set up managed node instances in order to manage network elements. The Commissioning Manager is used to configure coreEMS managed node instances, such as to create, reconfigure and delete a managed node instance. Users should only use the Commissioning Manager to configure managed node instances. Manually editing configuration files is highly discouraged unless the user is absolutely sure of the effect of their action.

Prerequisites

This procedure has the following prerequisites:

- The DMS needs an SDM/CBM with CEM SAF packages installed and services enabled. For details on configuring CEM packages in SDM/CBM, see the *CBM850 Commissioning for UCBM23*, IM 24-2610 and *SDM/FT Installation and Commissioning SDM15 - SDM17, CS2A0002 - CS2E0009*, IM-24-0193, or contact your Nortel representative for instructions.
- The version of CEM on the SDM/CBM must be the same as the target CEM version on the IEMS server.
- You must know the target SDM/CBM IP address.

Action

Step	Action

At your workstation

1 Launch the CEM Commissioning Manager CLI. See Launching the CEM Commissioning Manager CLI in *IEMS Overview*, NN10329-111.

The Commissioning Manager CLI main menu is displayed.

Example response

```
Nortel Networks coreEMS Commissioning Manager
Main menu
1 - Commission a new node
2 - Reconfigure an existing node
3 - Delete an existing node
```


Copyright © 2006, Nortel Networks Nortel Networks Confidential

```
4 - Add a mated pair monitor
5 - Delete a mated pair monitor
6 - SDM to CBM migration
0 - Exit
Selection :
```

2 Enter the number next to Commission a new node in the menu.

Example response

```
Configure a Node Instance
1 - DMS
2 - HLR200
3 - MDM
4 - NSP
5 - SESM
6 - USP_NES
7 - DS
Select a new device type for the new node:
```

3 Select the DMS device type for the new node instance by entering the number next to DMS in the menu.

DMS is the only supported option in this configuration.

Example response

```
Hint:  Input a string up to 15 characters drawn
from "-a-z0-9".  The 1st character must be an alpha
character; the last one must not be a minus sign.
Element name cannot be "server", "localhost", "loghost"
or the hostname of the local host.
Mandatory input.
Element Name :
```

4 Enter the name for the new node at the Element Name prompt.

The name can be a string of up to 15 alphanumeric characters and the minus sign (-). The first character must be alphanumeric and the last character must not be a minus sign. The element name cannot be server, localhost, loghost, or the hostname of the local host.

Example response

```
Hint:  Enter the region path to the node or select
one from the list.  Valid path characters include
alpha-numeric and the '/' characters.  Mandatory input.
List of existing regions:
Nortel
Region :
```

5 Enter the region name at the Region prompt.

Example response

```
Hint:  Choose a software version.
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

```
Mandatory input.
[1] GEM18
Software Release (1):
```

6 Select GEM18 for the new node by entering 1 at the Software Release prompt.

Example response

```
Hint:  Input a dot-decimal representation of an IP
address or the string "localhost".
Mandatory input.
Target SDM IP Address:
```

7 Enter the target IP address at the Target SDM IP Address prompt.

The target IP address must be in dot-decimal format.

Example response

```
Hint:  Answer Yes if the SDM has Call Trace installed,
otherwise answer No.
Mandatory input.
1 - Yes
2 - No
Enable Call Trace (1) :
```

8 Enter the number next to No at the Enable Call Trace prompt.

No is the only supported option in this configuration.

Example response

```
Hint:  Answer Yes if this DMS has an MSC/TriNode, No if
this DMS is an HLR.
Mandatory input.
1 - Yes
2 - No
Install Billing Manager(1) :
```

9 Enter the number next to No at the Install Billing Manager prompt.

No is the only supported option in this configuration.

Example response

```
Hint:  Answer Yes if this DMS has USP, otherwise answer
No.  Not valid if Billing Manager = Yes
Mandatory input.
1 - Yes
2 - No
Does This DMS Have USP (2) :
```

10 Enter the number next to No at the Does This DMS Have USP prompt.

No is the only supported option in this configuration.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Example response

```
Proceed to create this node?  [y/n] (n):
```

11 Enter y at the proceed to create this node prompt.

Example response

```
Commissioning node, please wait...
Commissioning node completed successfully!
Is sdma2 already in server mode?  [y/n] (n):
```

12 Enter y at the prompt.

Example response

```
Start all applications of node <nodename>?  [y/n] (n):
```

13 Enter y at the prompt to start the node applications.

14 Wait until the following message appears.

Example response

```
Returning to service all applications of node
<nodename>.
This action may take a few minutes.
Please wait...
Busy/Rts action completed!
```

The Nortel Networks core EMS Commissioning Manager Main menu appears.

```
Nortel Networks coreEMS Commissioning Manager
Main menu
1 - Commission a new node
2 - Reconfigure an existing node
3 - Delete an existing node
4 - Add a mated pair monitor
5 - Delete a mated pair monitor
6 - SDM to CBM migration
0 - Exit
Selection -
```

15 Exit the Commissioning Manager CLI by entering the number next to Exit in the Nortel Networks core EMS Commissioning Manager Main menu.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Deleting a CEM managed node instance

Application

Use this procedure to delete a managed node instance of CEM.

Action

Step	Action
	At your workstation

1	Launch the CEM Commissioning Manager. See Launching the CEM Commissioning Manager CLI in *IEMS Overview*, NN10329-111.
	The Commissioning Manager CLI main menu is displayed.
	Example response
	`Nortel Networks coreEMS Commissioning Manager`
	`Main menu`
	`1 - Commission a new node`
	`2 - Reconfigure an existing node`
	`3 - Delete an existing node`
	`4 - Add a mated pair monitor`
	`5 - Delete a mated pair monitor`
	`6 - SDM to CBM migration`
	`0 - Exit`
	`Selection -`

2	Enter the number next to Delete an existing node in the menu.
3	Select the node you want to delete. *Example response* `Proceed to delete this node?  :`

4	Enter y at the prompt to delete this node.
	The Nortel Networks core EMS Commissioning Manager Main menu appears.
	`Nortel Networks coreEMS Commissioning Manager Main menu`
	`1 - Commission a new node`
	`2 - Reconfigure an existing node`
	`3 - Delete an existing node`
	`4 - Add a mated pair monitor`
	`5 - Delete a mated pair monitor`
	`6 - SDM to CBM migration`
	`0 - Exit`
	`Selection -`

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Exit the Commissioning Manager CLI by entering the number next to Exit in the Nortel Networks core EMS Commissioning Manager Main menu.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using topology operations

This section provides the following procedures to use operations in the topology window of IEMS Java Web Start Client.

Copyright © 2006, Nortel Networks

Editing and viewing object properties using Java Web Client

Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

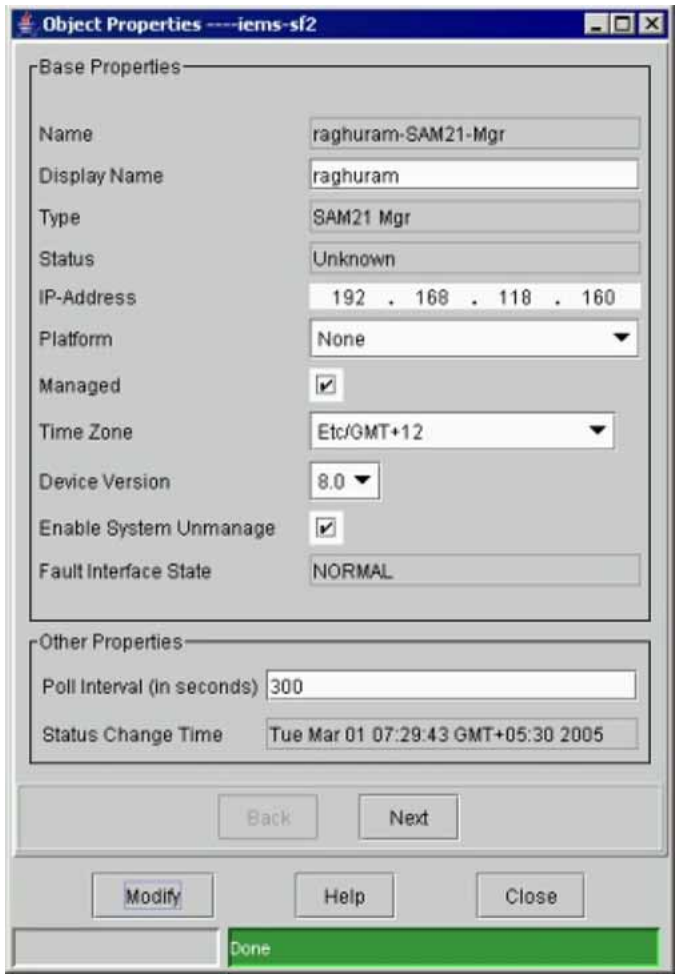
Prerequisites

There are no prerequisites for this procedure.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client. Refer to procedure Launching IEMS Java Web Start Client in *IEMS Overview*, NN10329-111. To launch the IEMS Java Web Start Client using the CDMA Network Manager (CNM), refer to procedure "Starting the Core Element Manager subcomponent GUIs" in Nortel Network *Management Systems (CNM, W-NMS) Administration: CEM Browser*, 411-8111-503.
2	Select the required object in the IEMS Topologies tree under Applications. The properties of an object from the Inventory panel of IEMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree, under Applications to open the Inventory view. Double-click the required row in the Inventory view.
3	Right-click the map symbol and select the Managed Object Properties menu item or double-click the map symbol to open the Object Properties window. *A window similar to the following figure opens. The object properties displayed can differ for each component.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



4 If required, modify the object properties. Use the following table to assist you in understanding the fields.

For the following auto-discovered element objects and element managers that have auto-discovered child nodes, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines. To change the IP address of these objects, you must delete and then re-add the appropriate element manager.

For the following element objects, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Portal, SSLines, MG 7480/15000/20000, MSS 15000

You cannot modify the IP address for the MG 7480/15000/20000 or MSS 15000.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

For the following element objects, only the Display Name and the Managed field can be modified: SDM platform, APS Manager, CS 2000 Core, MG 7480/15000/20000, MSS 15000.

Managed object properties in Java Web Client

Field	Description
Name	Displays a unique name for the object
Display Name	Edit the name displayed in the topology for the object
Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
IP-Address	Edit the IP address of the object
Platform	Select the platform where the object resides from the drop-down list
Managed	Indicates whether the object is managed or unmanaged
Time Zone	Select the time zone of the geographical location where the object exists from the drop-down list
Device Version	Select the device version of the managed object from the drop-down list
Enable System Unmanage	Enable or disable the System_Un managed state. Refer to section "System_Unmanaged state" in "Configuring the Message Overload Controller parameters" in *IEMS Fault Management*, NN10334-911.
Poll Interval	Edit the Poll Interval for status updates
Status Change Time	Displays the last status change time of the object

5 Select your next step.

If	Do
you do not want to modify any other properties	go to step 6
you want to view or modify the fault interface or performance interface properties	go to step 8

6 Click the Modify button to update the changes.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

7 Go to step 16.

8 Click the Next button to proceed to the Fault Interface window.

A window similar to the following figure opens.

9 Edit or view the fault interface properties of the object as required.

The Details panel dynamically changes according to the fault interface of the EMS/NE.

For MS 2000, do the following. Enter v2c as the SNMP version for (I)SN09U. The SNMP read Community and write Community strings by default are public and private. If these values were changed, enter the correct values here.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 Select your next step.

If	Do
you do not want to modify any other properties	step 11
you want to view or modify the performance interface properties	step 13

11 Click the Modify button to update the changes.

12 Go to step 16.

13 Click the Next button to proceed to the Performance Interface window.

A window similar to the following figure opens.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

14 Edit or view the performance interface properties of the object as required.

For MS 2000, do the following. Enter v2c as the SNMP version for (I)SN09U. The SNMP read Community and write Community strings by default are public and private. If these values were changed, enter the correct values here.

15 Click the Modify button to update the changes.

16 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Updating status of objects manually

Application

Use this procedure to manually update the status of managed objects.

IEMS updates the status of managed objects in regular intervals (status polling), but it is possible to update the status of the managed objects manually which interrupts the regular polling. SNMP and CORBA-based devices communicate to IEMS through unreliable streams (without establishing connections). When manually triggering updates for the SNMP or CORBA-based devices is done, IEMS checks whether the communication with the device is active. The color of the map symbols background indicates the severity levels as tabulated below:

Significance of map symbol background color

Background color	Severity level or status
	Critical
	Major
	Minor
	Warning

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Background color	Severity level or status
	Clear
	Unmanaged or unknown object status

For USP NEs, only the active USP unit object provides an interface to determine the fault state of the USP. The inactive USP unit object status is in unknown state (map symbol has gray background color). The IEMS dynamically detects when the USP unit has been swacted. When this occurs, it initiates alarm resync with the newly active USP unit and updates the state of the USP unit objects in the IEMS Client to reflect this change in activity. When this occurs, the previous active unit object map is changed to unknown state, and the new active unit is updated to reflect the highest alarm state of the USP device. For the color mapping of various object status, refer to ""Updating status of objects manually" (page 230)".

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 topology panel in the IEMS tree. *The tree shows the EMSs discovered or added for that type of EMS.*
3	Select the map symbol for which the update status is required.
4	Right-click the selected map symbol and select the **Update Status** menu item. *Progress of update is shown in the status bar. After the status update is complete, a "Status update over" message is displayed in the status bar.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

The above procedure can be used to manually trigger updates for NE, EMS application, or platform objects.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Managing objects

Application

Use this procedure to manage an object using Java Web Start Client.

Using IEMS Client, a provisioned EMS, NE, application, or platform can be managed or unmanaged. When a provisioned (or discovered) object is being managed, the state of the object is actively updated to reflect the current alarm status. When a device is unmanaged, the state of the device is no longer updated.

When an object is unmanaged, IEMS does not status poll the corresponding object. Also, IEMS does not receive the events and alarms from the unmanaged object and does not forward the events to northbound.

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 a topology panel in the IEMS tree in which the required map symbol is displayed.
3	Right-click the required symbol (that needs to be managed) in the topology panel and select the **Manage** menu item. You have completed this procedure.

—End—

Managing an object: example

To manage a Core Element Manager (in unmanaged state), 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.

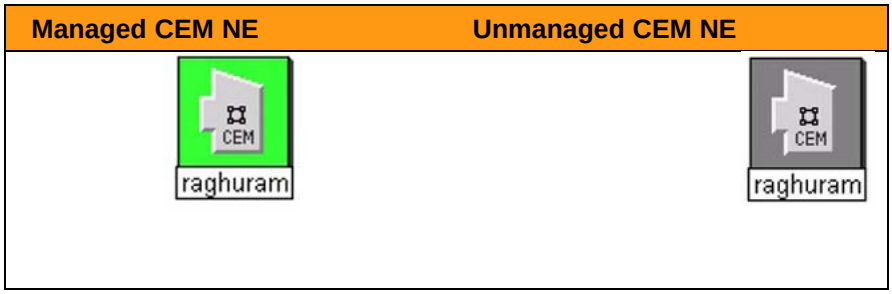
Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2 Select the **Element Manager**s topology panel in the IEMS tree in which the required map symbol is displayed.

3 Right-click the required CEM map symbol (that needs to be managed) in the Element Managers topology panel and select the **Manage** menu item.

Once a selected map symbol is set to be managed, an icon is displayed against the selected map symbol indicating the severity status of the device. The following figure shows the difference between managed and unmanaged objects.

Difference between Managed and Unmanaged NE



The objects in unknown state and unmanaged state have the same map symbol background color.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Unmanaging objects

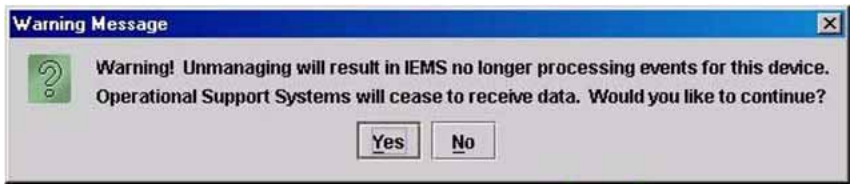
Application

Use this procedure to unmanage an object.

Unmanaging an object stops IEMS from monitoring the object.

When an object is unmanaged, IEMS does not status poll the corresponding object. Also, IEMS does not receive the events and alarms from the unmanaged object and does not forward the events to a northbound interface.

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 a topology panel in the IEMS tree in which the required map symbol is displayed.
3	Right-click the required symbol (that needs to be managed) in the topology panel and select the **UnManage** menu item. The following warning message is displayed: 
4	Click the **Yes** button to unmanage the object. You have completed this procedure.

—End—

Example of unmanaging an object

Step	Action
	At the IEMS workstation

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

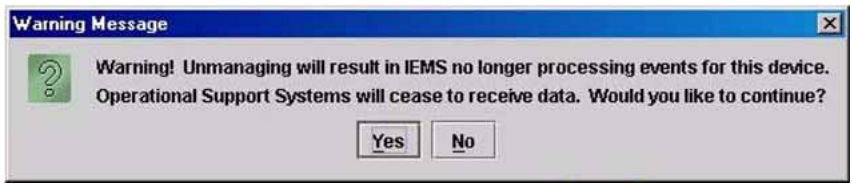
1 Launch the IEMS Java Web Start Client. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.

2 Select the **Element Manager**s topology panel in the IEMS tree in which the required map symbol is displayed.

3 Right-click the required CEM map symbol (that needs to be unmanaged) in the Element Managers topology panel and select the **UnManage** menu item.

4 Right-click the required symbol (that needs to be managed) in the topology panel and select the **UnManage** menu item.

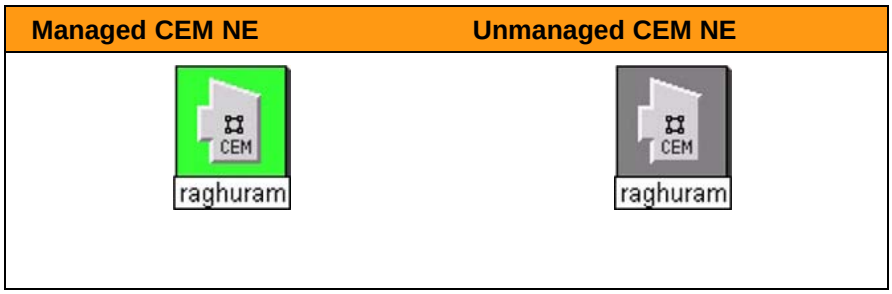
The following warning message is displayed:



5 Click the **Yes** button to unmanage the object.

Once a selected map symbol is unmanaged, the status icon in the map symbol becomes gray. The following figure shows the difference between a managed and an unmanaged object.

Difference between a managed and an unmanaged NE



The objects in an unknown state and unmanaged state have the same map symbol background color.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a custom topology node

Application

Use this procedure to add a topology node in the IEMS tree.

This procedure also describes the custom topology tree node and how it is different from the default topology tree node. Custom topology nodes can be used to filter map symbols based on specified criterion.

Custom topology tree node: Custom tree topology nodes have some specific criteria, which must be met for the map objects or symbols to be displayed.

Default topology tree node: Default topology tree nodes are those provided automatically by the objects. Unlike the custom topology node, where map symbols must satisfy certain criterion, the default topology node does not require the map symbols to satisfy any criterion. Any object can be added to a default topology.

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 a topology node in the IEMS tree in which the required map symbol is shown.

3 Select the **Custom Views-->Add New Map** menu item to launch the Add Map window.

4 In the Add Map window, specify the set of map-related information. The editable fields are listed in the following table.

Field	Description
name	The name of the topology node that is to be added.
label	The display name or label of the topology node. This name is displayed in the tree.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Field	Description
topology	Displays a list of al topologies supported for the map. topology. Comma-separated values are permitted. The first topology listed becomes the default topology for the map unless another topology is entered in the currentTopology field. **Example** grid, star, ring, flow.
imageName	The image file which appears as the background of the topology. The images can be in JPEG or PNG format. The images must be placed under the <IEMS Home>/images directory. **Example** *images/networkmapmain.png*
autoPlacement	True (default) - the map layout is displayed according to the defined current topology. False - Allows you to arrange the map symbols for that map.
menuName	The panel-specific menu file for this topology. The menu files are available under the <IEMS Home>/mapdata/menus directory. Example: mapmenu.xml, nodemenu.xml
groupName	Reserved for future use
WebNMS	Reserved for future use
helpDoc	Displays the URL for the help documentation that is displayed when you click the Help button. Editable.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Field	Description
mapSymbolRenderer	The renderer that paints the map symbols in the topology canvas. By default, there are 3 map symbol renderers bundled with the product. Symbol Renderers: mapSymbolRendererImpl: On selection of a map symbol, four dark squares appear on the edges of the symbol. mapSymbolRendererImpl_2: On selection of a map symbol, a square box is painted over the symbol. mapSymbolRendererImpl_3: Status of the objects is represented in a small box on the top corner of the symbol. On selection of the symbol, a square box is painted over the symbol. This is the default map symbol renderer used in the IEMS client.
mapLinkRenderer	Specifies the map link renderer that renders the links between the map symbols in the topology.
anchored	Specifies whether the anchor property of the topology is editable. True - the topology components that are added to the topology are not editable. False - the topology is editable. The default value is false.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Field	Description
treeIconFileName	The name of the icon file that appears in the client tree against the topology node. The images must be placed under the <IEMS Home>/images directory. **Example** *images/ers8600_tree.png*
currentTopology	Sets the default topology for the map. If you do not enter a topology in this field, then the first topology listed in the topology field is the default.
ParentNode	The parent node in the tree is selected from the list box. If the **Fault Management** node is selected, the topology is added under the **Fault Management** node in the client tree.

For the imageName fields listed in the above table, the images in the /opt/nortel/iems/current/images directory (where IEMS server is installed) can be used. If required, the images can be copied to the above location and used.

5 Select your next step

If	Do
you want certain criteria to be matched for the objects to be displayed	step 6
do not want to customize the map	step 10

6 If you want certain criteria to be matched for the objects to be displayed, click the **More** button to launch the Custom Map Properties dialog box.

7 Enter the search criteria in the Custom Map Properties dialog box.

The search criteria can be any of the properties of the managed object.

8 Click the **OK** button.

9 Click the **Add Map** button to add the topology.

10 You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks

Searching for objects in the topology view

Application

Use this procedure to search for an object map symbol in the 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	Navigate to the **IEMS Topologies** node in the IEMS tree.
3	Click Network Elements, Element Managers, EMS Applications, EMS Platforms, or their subnodes under IEMS Topologies to display the required topology panel.
4	Select the **Search** menu item in the **Edit** menu to launch the Find dialog box. You can also open the Find dialog box by clicking the **Find** button in the toolbar.
5	Enter the label name in the Symbol label field. You can enter the whole of the label name or part of the label name.
6	Click the **Find next** button to search for the map symbol with the specified label name. You can skip to the next topology by clicking the **Next Map** button. The **Up** and **Down** radio buttons are used to specify the direction in which the search is performed. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Viewing the SAM21 cards

Application

Use this procedure to view the SAM21 cards.

After a SAM21 Manager is added, the corresponding SAM21 NEs are automatically discovered. Each discovered SAM21 network element is added as a map symbol under the grouped SAM21 map symbol in the Network Elements display panel. They are also added under **Network Elements->SAM21** in the IEMS Topologies tree.

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	Expand the **Networks Elements** node in the IEMS tree.
3	Select the **SAM21_1** sub node under the SAM21 node. *The SAM21 cards are displayed. The card arrangement in the SAM21 device is also displayed.*
4	You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Partitioning the NEs discovered by MDM

Application

Use this procedure to partition the NEs discovered by MDM.

When an MDM is added to the topology, the corresponding Media Gateway 7480/15000/20000 and MSS 15000 NEs are discovered by IEMS. These NEs can be unmanaged or made invisible to all the users in the various topologies such as network elements, Media Gateways, MSS15K, and MSS-Unknown. This is achieved by partitioning the NEs as managed, unmanaged, or invisible devices in the Partition NEs GUI.

NEs are invisible to all the users in the various topologies, that is, NEs do not appear in the topologies but the details of these NEs are present in the database.

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 **Element Managers** topology in the IEMS tree.
3	Right-click the MDM map symbol for which the NEs must be partitioned and select **Partition NE's** menu item. *The Partition NEs GUI is launched.*
4	Select the NE to be unmanaged from the Managed Devices list and move it to Unmanaged Devices list by clicking the **>>** button (present next to Managed Devices list). To move the NE from Unmanaged Devices list to Managed Devices list, select the NE and click the **<<** button (present next to Managed Devices list). When an object is unmanaged, IEMS does not status poll the corresponding object. Also, IEMS does not receive the events and alarms from the unmanaged objects and does not forward events to northbound.
5	Select the NE to be made invisible in the topologies from the Unmanaged Devices list and add it to Invisible Devices list by clicking

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

the **>>** button (present between Unmanaged Devices and Invisible Devices list).

You must move the NE to Unmanaged Devices list from Managed Devices and then add it to Invisible Devices list.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Zooming the topology view

Application

Use this procedure to zoom the topology view.

The zooming function in the topology of IEMS Client displays an enlarged view of the topology and its components. Map symbols can be zoomed using the Zoom button in the Map toolbar.

The zoom functionality can be achieved by accessing the zoom tool buttons of the topology toolbar as tabulated below.

Zoom tool buttons

Zoom Tool button Name	Zoom Tool button
Zoom Mode	
Zoom In	
Zoom Out	
Zoom Overview	

Zoom mode: The Zoom Mode tool button enables the zooming of one or more map symbols. To have to select one symbol at a time for zooming, use the Selection tool. Otherwise, select more than one symbol over a given area in the topology and click the Zoom Mode tool. Symbols in the topology cannot be selected when the Zoom Mode tool is enabled.

Zoom in mode: To zoom in on the entire displayed topology, access the corresponding button in the Map toolbar. On clicking the button, the Map zooms in at the center.

Zoom out mode: Zoom out to view the entire topology at its default size by accessing the corresponding button of the Map Toolbar. On clicking the button, the topology returns back to its original size.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Zoom overview: To view the exact region, which is currently being zoomed in or zoomed out, access the Zoom Overview tool button of the Map Toolbar. On clicking this button, a separate Map Overview window pops up at the left corner of the window, highlighting the area of the Map (with red bars), which is being zoomed. This is useful for locating the exact positions of the map symbols in a Map. In this window, zooming can be adjusted by varying the size of the zoom overview. When the zoom overview window is changed, the zoom overview also varies proportionately.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Clien. Refer to "Launching IEMS Java Web Start Client" in *IEMS Overview*, NN10329-111.
2	Navigate to the IEMS Topologies node in the IEMS tree.
3	Select a topology panel in the IEMS Topologies node. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using toolbars in the Topology view

When a topology (such as Element Managers, EMS Applications, EMS Platforms or Network Elements) is selected in the IEMS Topologies tree, two toolbars can be found in the IEMS client.

- Main topology toolbar
- Topology configuration toolbar

Using the main topology toolbar

This toolbar is used to add, delete, save, refresh or relayout a topology. For descriptions of these toolbar options, refer to the following table.

Main topology toolbar buttons

Tool button name	Tool button	Menum command	Shortcut key	Description
Undo		Edit-->Undo Add/Delete	Ctrl+Shift+Z	Used to undo the last action.
Add Map		Custom Views-->AddMap	Ctrl+N	Adds a topology.
Delete Map		Custom Views-->DeleteMap	Ctrl+D	Deletes the selected topology. ***Note:*** Only custom maps can be deleted.
Save Map		Custom Views-->Save Map	Ctrl+S	Saves the topology properties and map symbol properties (if symbols are present) to the respective database tables.
Refresh Map		View-->Refresh	F5	Reloads the topology with the most recently saved information.
Relayout Topology		Custom Views -->Relayout Map	Ctrl+R	Click this button to relayout the entire set of objects.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using the topology configuration toolbar

Each topology has a toolbar available at the top of the view. This toolbar is used to configure the appearance of the topology that is being viewed.

The topology toolbar icons and their descriptions are listed in the following table.

Description of tool buttons in the topology configuration toolbar

Toolbar button name	Toolbar button	Description
Select		Selects a map symbol in the topology, (indicated by being enclosed within four blocks). Only one map symbol can be selected at a time.
Zoom Window		Displays the Zoom window. First select a map symbol and then click this Zoom Window button. The Zoom window displays the exact location of the selected map symbol in the topology. You can use this to find the exact location of the map symbol within the topology.
Zoom Mode		Enables selection of one or more map symbols for zooming.
Zoom In		Obtains an enlarged view of the selected topology. The topology is zoomed from the center of the selection. This button can be selected multiple times to perform multiple zooms.
Zoom Out		Zooms out of the topology view. This button can be selected multiple times to zoom out further.
Cut		Cut any map symbol in the topology view.
Copy		Copies a map symbol from a topology view ready for pasting to an existing or to a newly created topology view.
Paste		Pastes any map symbol previously cut or copied from a view to an existing topology or to a newly created topology.
Undo		Performs an undo of the most recent action.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Toolbar button name	Toolbar button	Description
		Displays the topology in its default state with map symbols, container, and groups.
Group View		***Note:*** Disabled for Network Elements, EMS Platforms and EMS Applications topology node under the IEMS topology node.
		Expands an existing group, displaying all the map symbols within the group.
Expand Selected Groups		***Note:*** Disabled for Network Elements, EMS Platforms and EMS Applications topology node under the IEMS topology node.
		Groups the selected map symbols.
Group Selected Symbols		***Note:*** Disabled for Network Elements, EMS Platforms and EMS Applications topology node under the IEMS topology node.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Grouping and ordering map symbols

Map symbols are icons displayed for different object types. The objects can be grouped or ordered. The following procedures describe how to group or order map symbols.

Grouping map symbols

Application

Use this procedure to group map symbols. In addition, groups can also be ungrouped, disable groups, open groups, and save changes on server option.

Grouping map symbols helps to view map symbols representing managed objects connected within a local vicinity or managed objects which share a logical connection.

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.
	To group based on preference
2	Select the required topology panel in the IEMS tree.
3	Select a set of map symbols with combination of Ctrl key and mouse click.
4	Group them using the **Group Selected symbols** tool button in the topology toolbar. A group symbol is displayed in place of the selected symbols. The remaining map symbols remain unaffected.
	To group based on number of map symbols per group
5	Open a topology and select the **Edit-->No Of Symbols Per Group** menu command, to group map symbols as per the specified number. After creating a group, save the map using the **Custom Views-->Save Map** menu command to maintain the state of group.
	To ungroup the groups to view map symbols
6	Select the required topology panel in the IEMS tree.
7	Select one or more group symbols.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

8 Select the **Expand Selected (or all) Groups** tool button in the topology toolbar to view the symbols in the selected groups in one view (or) double-click on a group symbol to view the map symbols in that group.

The map with group symbols can be saved for future use.

To disable groups

9 Select the **Edit-->Disable Grouping** menu command.

To open a group

10 Select the required topology panel in the IEMS tree.

11 Select one of the grouped map symbol.

12 Select the menu **Group-->Open Group** from the menu bar [or] right-click the group symbol and select the context-sensitive menu option **OpenGroup**. Double-clicking the group symbol can also open the group.

To Save Changes On Server option

13 To retain the symbols inside the group, the symbols' groupName property must be updated with the respective group name. This can be performed by either:

- saving the map using the **Custom Views-->Save Map** menu command

  OR

- using the **Save Changes on Server** option for every map symbol present inside the group.

The Save Changes On Server option in the group symbol property form saves only the group properties in the server. Consequently, the server is not aware of the symbols present inside the group. After saving the group, and performing a refresh (or when the client is next started), the group is present but none of the symbols are shown.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Ordering map symbols

The map symbols can be sorted in an orderly manner by using the **Edit-->Order By** menu option. The map symbols can be sorted based on the criteria shown in the following table.

Criteria Attributes for Ordering Map Symbol

Criteria Attribute	Description
name	Sorts the map symbols based on their names. Order of sorting is A-Z.
label	Sorts the map symbols based on the symbols' label values. Order of sorting is A-Z.
objName	Sorts the map symbols based on the name of the managed object that is represented by the symbol.
status	Sorts the map symbols based on the status of the managed objects represented by the symbols. Order of sorting is from critical to clear.
groupName	Sorts the map symbols based on the name of the group to which they belong.
objType	Sorts the map symbols based on the type of the managed object represented by the symbols.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Deleting object and traces

Application

Use this procedure to delete an object and traces from the topology.

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 topology panel.
3	Right-click the required object or map symbol in the topology and select the **Delete Object and Traces** menu item. *A confirmation dialog is displayed with the message "This operation will delete sub-elements of the selected object(s). Do you want to proceed ?"*. Deleting an object and traces from the topology does not remove the events associated with the object. Deleting an object only removes it from the topology and its associated alarms.
4	Click the **Yes** button. *"The node has been deleted successfully" message is displayed.* When you delete an MG 3200 NE, the following message is displayed. *The node has been deleted successfully. The node should also be removed from the HTTPS proxy using the SPFS CLI tool.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Changing the topology layout

Application

Use this procedure to change the topology layout.

The topology layout can be changed to grid, star, ring, or flow layout.

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 topology. For example, the **Network Elements** topology panel.
3	Double-click on the background of the topology. *The Map Properties dialog is displayed.*
4	Select the required layout in the CurrentTopology list box.
5	Click the **Modify** button to save the selection.
6	Click the **Close** button to close the Map Properties dialog. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks

Changing topology background

Application

Use this procedure to change the topology background.

The background displayed for each of the topology can be changed. The backgrounds are images in either PNG or JPEG format.

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 topology panel. For example, **Network Elements** topology panel.
3	Double-click on the background of the topology. *The Map Properties dialog box is displayed.*
4	Using the file chooser button next to the ImageName field, select the required image.
5	Click the **Modify** button to save the selection.
6	Click **Close** button to close the Map Properties dialog. For the ImageName field specified above, the images in the /opt/nortel/iems/current/images directory is used. If required, the user-defined image files can be copied here and subsequently used. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Working with the inventory panel

The Inventory panel maintains the properties of all managed objects of a network. These managed objects and their object properties are listed in the Inventory panel. The Inventory panel can be selected from IEMS tree. You can navigate through the displayed Inventory panel by objects. The property details of these managed objects can be accessed through the menu specific for the selected object.

Copyright © 2006, Nortel Networks

Navigating inventory panel

Application

Use this procedure to locate the Navigation toolbar in Inventory, as well as to find out how to navigate the inventory.

The inventory can be navigated with the help of navigation tools such as view range, navigator buttons and column reordering. You can navigate the inventory for an easy and understandable view or sort out the database based on your requirements. The various ways in which the Inventory can be navigated are listed below:

View Range: The range of rows that are displayed in the table. It is placed on top of the Inventory window. You can also use the default page lengths available in the list box.

In the Inventory panel, the objects being viewed take precedence over the updates received (for example, when new managed objects are added into the database). This is unlike objects displayed in the Events or Alarms browser. In Events or Alarms browser, the latest objects added are displayed in the beginning of the browser followed by the already added objects (for example, updates get precedence over the objects being viewed). In the Inventory panel, the latest objects added are displayed at the end, wherein you need to scroll through to view the latest managed objects that were added.

Navigator Buttons: The Inventory panel contains four navigator buttons on the right top. They are First, Previous, Next, and Last. The descriptions of the buttons (according to the order they are displayed) are as follows.

- **First button**: This button is used to view the first page of the internal frame, which displays data retrieved from the database.
- **Previous button**: This button is used to view the previously viewed page of the internal frame, which displays data retrieved from the database.
- **Next button**: This button is used to view the next page of the internal frame, which displays data retrieved from the database.
- **Last button**: This button is used to view the last page of the internal frame, which displays data retrieved from the database.

Sort: You can sort the data based on the column type and the details can be viewed either in ascending order or descending order. For details, refer to "Understanding sorting of data" in *IEMS Overview*, NN10329-111.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Both server-side and client-side sorting can be done for one column as required. These sorting are also indicated by the combination of the above indicators.

Column reordering: For an easy view of the data, you can reorder the columns by just dragging the column header and moving it to the required place in the table.

Search: One can find the required device of a particular criteria or on a general condition. The Search dialog can be launched from the Edit menu or through the Find option in the toolbar or by pressing Ctrl+F. For more details refer to searching devices.

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	Navigate to the Inventory panel in the IEMS tree. You can find the Navigation toolbar in the top part of the Inventory panel in the right-hand side of IEMS Client. You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Searching EMS/NE from inventory panel

Application

Use this procedure to invoke the Search dialog, and to find out how to search EMS/NE from the inventory panel.

This function enables you to search one or more related events from the inventory. The search operation is performed on the entire database. You can find the required network using a particular criteria or a general condition.

The search is made on the server side, which means that the search is done on the entire database and is not restricted to the displayed page alone. More flexibility has been provided in the search feature so that you can search on a particular property or on a general condition.

You have an option to select whether all the criteria or any of the criteria given has to be satisfied. This option can be set by selecting the **Match any of the following** option or **Match all of the following** option.

The search can be on one or more criteria using the **More** and **Fewer** buttons. You can add any criterion on which you have to go for search. The first option in the screen pop up is a list box, which lists the existing column headers in the Inventory table of the Inventory panel. The second option has two different sets of search criteria: a normal set of criteria, and a date/time criteria:

The normal set of criteria consists of:

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

The third option is a data field or Date/Time component for entering your specific argument. By default, the Date/Time component shows the current date and time in the order of month, date, year, hour, minute, second, and AM/PM, which can be chosen by using the up and down arrows.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Inventory** panel in the IEMS tree.
3	Launch the Search dialog using the **Edit-->Search** menu command. The Search dialog can be launched using the **Edit-->Search** menu command or using the **Find** button in the toolbar, or by pressing Ctrl+F keys. You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Resynchronizing inventory for element managers

Application

Use this procedure to resynchronize the element manager details through the topology view or the inventory view in Java Web Start Client.

Managed objects (MOs) are added to the IEMS topology either by adding them through the Add EMS/NE wizards or they can be auto-discovered. For example, when provisioning an element manager in IEMS, the associated element manager is added to the Element Managers node in the topology tree and IEMS discovers the sub-tending devices managed by that element manager. The discovered devices are also added to the Network Elements branch in the topology tree. Auto discovery is performed when provisioning the following element managers to the IEMS topology.

- APS Manager
- GWC Manager
- MG 9000 Manager
- Multiservice Data Manager
- SAM21 Manager
- UAS Manager

After the IEMS server is started, some of the managed element managers support the dynamic change of their properties to IEMS in order to update the Inventory. The above element managers do not support the dynamic change of properties; such element managers need to manually resynchronize to update the IEMS Inventory.

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	Navigate to the Element Managers topology panel under the **IEMS Topologies node** in the IEMS tree.
3	Select the required Element Manager map symbol in the selected topology node for which you want to resynchronize the inventory details.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

4 Select **Re-Synchronize Inventory** from the **<Object-specific>** menu where the **<Object-specific>** menu indicates the selected EMS/NE.

Element manager objects that have inventory details in IEMS database in synchronization with the corresponding element manager properties cannot be resynchronized. Those element manager map symbols do not have the **Re-Synchronize Inventory** menu item in the **<Object-specific menu>**.

When the re-synchronization is complete, a message is displayed that says "Resynchronize inventory request for <device> succeeded".

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Identifying problems of objects in the inventory panel

In the domain of Network Management Systems, it is imperative that the Manager (IEMS) is informed about the state of every network element (NE). The Manager receives network notifications about the state of every managed NE. These notifications are unsolicited messages sent by either the agent in the NE or through status polling techniques adopted by the Manager. These malfunctions or faults are acknowledged by IEMS as generated events and alarms. You can view the generated events and alarms for a device selected from the displayed list of the Inventory panel. This can be accomplished by accessing the panel-specific menu View. On clicking the required menu item, that is, events or alarms of the panel-specific menu, the corresponding panel gets displayed in the Client with the display of the generated events or alarms of the selected device.

Navigating to the inventory node

Application

Use this procedure to navigate to the Inventory node.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Java Web Start Client (refer to "Launching IEMS Java Web Start Client" of *IEMS Overview*, NN10329-111).
2	Navigate to the **Inventory** panel in the IEMS tree. You have completed this procedure. You can only access alarms or events for the following types of objects: • element managers • NEs • EMS platforms

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Accessing Alarms for selected EMS/NE

You can view the alarms generated for the EMS/NE selected in the list view of the Inventory panel by accessing the panel-specific menu option **View-->Alarms**. On choosing this menu option, the Alarms panel (under the **Fault Management** node) of IEMS Tree is selected, displaying the last generated alarm and its severity status for the selected device.

The alarms associated with the managed object can be viewed from the topology node by selecting the managed object in the topology and then selecting the **View-->Alarms** menu command.

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

Accessing Events

You can view the events generated for the device (selected in the list view of the Inventory panel) by accessing the panel-specific menu option **View-->Events**. On choosing this menu option, the Network Events panel (under the **Fault Management** node) of IEMS Tree is selected, displaying the list of generated events over a period of time for the selected device.

The events associated with the managed object can be viewed from the topology node by selecting the managed object in the topology and then selecting **View-->Events** menu command.

Updating the Status

Whenever the status of a selected object is to be updated, the Object-specific menu **Update Status** menu item can be used from the corresponding map symbol. This menu item enables the user to view the latest status of the selected device, instantaneously. This means, irrespective of the configured polling period, the IEMS fetches for the current status of the selected device. For example, if you have to retrieve the status of a particular selected node of the displayed list of the Inventory panel, select the menu command **Node-->Update Status**.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Dumping inventory details of IEMS

Application

Use this procedure to write inventory details to a text file from the IEMS object, the Inventory GUI, or the Topology GUI. For more details on the inventory details, see "Understanding dumped inventory details" (page 267).

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 your next step.

If you want to dump the inventory details from	Do
the IEMS object	step 3
the Inventory GUI	step 6
the Topology GUI	step 7

3	Select the IEMS map symbol in the Element Managers topology panel in the IEMS tree.
4	Select the **IEMS Mgr-->Dump Inventory Details** menu command. *A dialog opens and displays the message that inventory information is written to the file inventoryData.txt under /opt/nortel/iems/current/logs.*
5	Go to step 8.
6	Select the Inventory panel in the IEMS tree. Go to step 8.
7	Select the Topology panel in the IEMS tree.
8	Select the **Tools-->Dump Inventory Details** menu command. *A dialog opens and displays the message that inventory information is written to the file inventoryData.txt under /opt/nortel/iems/current/logs.*
9	You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Understanding dumped inventory details

The inventory details are dumped in a text file as mentioned in the table below. This section describes how the information is stored in this file and provides details of the properties. These details can be used to parse the information stored in the text file.

File details

The details of the file in which the inventory details are dumped are listed in the table below.

Field	Value
File name	inventoryDetails.txt
File location	/opt/nortel/iems/current/logs
Field delimiters	Comma (separated by ",")
Record separator	Next line (Enter)
End of file marker	-1 (when read byte-by-byte as in Sun Java terminology)
Maximum file size	No limit

Details of properties

The details of properties are displayed in the table below.

Field	Data type in database	Column size	Description	Possible values
Name	Varchar2	100	A unique name for the map symbol.	Not Applicable
ParentName	Varchar2	100	The host name of the parent if present. This field is filled only for sub-units, NEs or EMS applications objects which are discovered automatically with corresponding platforms or element managers.	null or parent name

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Field	Data type in database	Column size	Description	Possible values
			Example succession-sol1-SSPFS-Unit-0 is sub-unit of succession-sol1-SSPFS platform object.	
IPAddress	Varchar2	100	The IP address of the object.	Not Applicable
Type	Varchar2	100	The type of object.	Name of the EMS application, element manager, platform, or NE.
Version	Varchar2	25	The version of the object.	
Status	Number	22	The status of the object.	Unknown, Clear, Critical, Major, Minor, or Warning
Managed	Varchar2	10	Indicates whether the object is managed or unmanaged.	true or false
InterfaceDetails	Varchar2	200	Displays the location of files with file names in which the interface details are stored. The interface name and each file location are separated by ":"(colon)	null or location of interface details
			Example SYSLOG:/var/log/customerlog:/var/log/securitylog:/var/log/auditlog	

The data type for the property Status is "Number" since the status of object is stored in numeric format. For example, an object with status "Critical" is stored with the value "1" in the Status column.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

A sample text from the inventoryDetails.txt file is given below. The commas together(,,) indicates the null value in the corresponding field.

```
Name,ParentName,IPAddress,Type,Version,Status,Manag
ed,InterfaceDetails
umanand-USP,,192.168.9.97,USP,6.2,Unknown,true,SNMP
:public:v1:161
succession-sol1-SSPFS,,192.168.4.176,SSPFS,6.2,Clea
r,true,SYSLOG:/var/log/customerlog:/var/log/securit
ylog:/var/log/auditlog
succession-sol1-SSPFS-Unit-0,succession-sol1-SSPFS,192.168
.4.176,SSPFS,6.2,Clea
r,true,SYSLOG:/var/log/customerlog:/var/log/securit
ylog:/var/log/auditlog
succession-sol1-SSPFS-Unit-0,succession-sol1-SSPFS,192.168
.4.176,SSPFS,6.2,Clea
r,true,SYSLOG:/var/log/customerlog:/var/log/securit
ylog:/var/log/auditlog
raghuram-LMM,,192.168.9.105,LMM,6.2,Clear,true,,
kashok-ERS8600,,192.168.1.98,ERS8600,7.0,Clear,true
,SNMP:public:v1:161
mvivekanandan-STORM,,192.168.9.97,STORM,6.2,Clear,t
rue,SNMP:public:v2c:161
saranganj-NPM,,192.168.9.243,NPM,6.2,Clear,true,SYS
LOG:/var/log/customerlog:/var/log/securitylog:/var/
log/auditlog
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Creating a custom view for the inventory panel

By creating custom views, you can find or filter out the required output in the screen by sorting through large amount of data from the IEMS. A custom view is a set of objects or data, which are subsets of a complete set of data or objects, satisfying a given criteria.

Using features in the custom view

The various features in the custom view are listed below

- The inventory of a specific criteria can be viewed.
- The updates of data are dynamic.
- Same custom view name can be used at different levels.
- The column (properties to view) is customizable.
- You can change the column order, sort the data, and save the states of custom view.
- Custom view can be modified.
- Custom view can be renamed.

Performing custom view operations for the inventory node

Application

Use this procedure to perform custom view operations for the inventory node.

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.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

2 Select the Inventory node in the IEMS tree and proceed with the menu bar options in the following table to utilize the features listed above.

Features in custom views for Inventory

Menu bar option	Tool button in Toolbar	Shortcut	Description
Custom Views--> Add Custom View		Ctrl+N	To add a new custom view with specific criteria.
Custom Views--> Remove Custom View		Ctrl+R	To remove a custom view. The parent custom view (Inventory) cannot be removed.
Custom Views--> Modify Custom View		Ctrl+M	To modify any custom view.
Custom Views--> Save Custom View		Ctrl+S	To save the current state of the custom view, such as column order, sort order, and others.
Custom Views--> Rename Custom View		Alt+F2	To rename any custom view

Add or modify a custom view. This option adds a new custom view with the given criteria. When this option of adding a new custom view is chosen, a custom view property window is displayed. After the form is filled with the necessary criteria and submitted, the new custom view is created and you can see the difference in the tree on the left.

Remove a custom view. This option removes the currently selected custom view. If a custom view has one or more custom views (as child view), the complete set (parent and child) are removed. The main parent custom view (default - Inventory) cannot be removed. Selecting the Remove Custom View option asks for a confirmation.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Save a custom view. This option saves the current state of the custom view such as order of the column, the sort order, and the displayed data.

Rename a custom view. This option helps you rename the current custom view as required. While renaming the custom view name, if you wish to have the same old name, then the user must press Esc key before completing it.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Setting custom views for inventory: matching criteria

Application

Use this procedure to set the match criteria as well as specify other properties.

By creating custom views, you can find out the required output on the screen from a large collection of data of IEMS. You can set the match criteria by using the Object Properties form, which is retrieved by accessing the Custom Views (panel-specific menu) -->Add Custom Views menu command. The properties form can contain details such as filter view name, parent name, class name, IP address, and other properties.

Besides the object properties, you can specify other properties such as Tree Node properties. This is achieved in the Tree Node Properties tab of the GUI. The Tree Node properties can include properties such as Frame Title, Menu File Name, Icon File, and others.

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 to the Inventory node in the IEMS tree.

3 Launch the Object Properties window by selecting the **Custom Views-->Add Custom Views** menu command.

The Properties fields are displayed.

4 Fill in the fields as required. (Refer to the following table for the properties in the property sheet, for filling in the fields, and for other information.)

Field	Description
Filter View Name	Specify name for the particular custom view.
ParentName	In the drop-down list, select the object in the tree list box under which this custom view is to be added. The default is Inventory node.
Name	Specify the unique name of the EMS/NE.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Field	Description
ipAddress	Specify the unique address assigned to each device. ***Note:*** 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 an invalid IP address.
Managed	Specify whether the devices are managed. True: Includes all managed devices. False: Excludes all managed devices. All: Includes all devices.
Type	Specify the type of EMS/NE, such as network, map symbol, or an interface.
isSNMP	This field must not be used.
Classname	Specify the class name of the managed device. For example, the class name for a node object (map symbol) is the value "Node".
Netmask	Specify the net mask assigned to the managed device.
PollInterval	Specify the poll interval (the time gap between two successive status polling of a managed device).
Status	Specify the status (severity) of the device in the inventory that indicates the criticality. The severity of the device to be filtered can be assigned here.
StatusChangeTime	Specify the time at which the status of the device changed. The time is represented as the number of milliseconds.
Tester	Specify the class used for the status polling of the selected managed devices.
Uclass	Specify the class to be launched for status polling. Use this field only if the value in the Tested field is "usertest".

If all the parameters (except filter view name) are left blank, then the default value "all" is assigned.

5 Select the **Tree Node Properties** tab.

The Tree Node Properties fields are displayed.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

6 Fill in the fields as required. (Refer to the following table for a description of the fields.)

Description of fields in Tree Node Properties tab of Custom View GUI for Inventory

Field	Description
Frame Title	Specify the name to be displayed on the title bar of the custom view's internal frame.
Menu File Name	The panel-specific menu file name for the Inventory panel. Do not modify this field.
Icon File	Indicate which icon you want 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/* folder or any sub folder under the */opt/nortel/iems/current/* folder. The */opt/nortel/iems/current/* folder is the folder under which the IEMS Server is installed.
Table Popup Menu	The file name of the menu used to display a contextual menu for the objects displayed in the table of the **Inventory** table. Do not modify this field.
Tree Popup Menu	The file name of the menu used to display a contextual menu for the Inventory node in the IEMS tree. Do not modify this field.
Node	Specify 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.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Example for creating a custom view for inventory

Application

Use this procedure as an example of how to create a custom view for the inventory details for the given criteria.

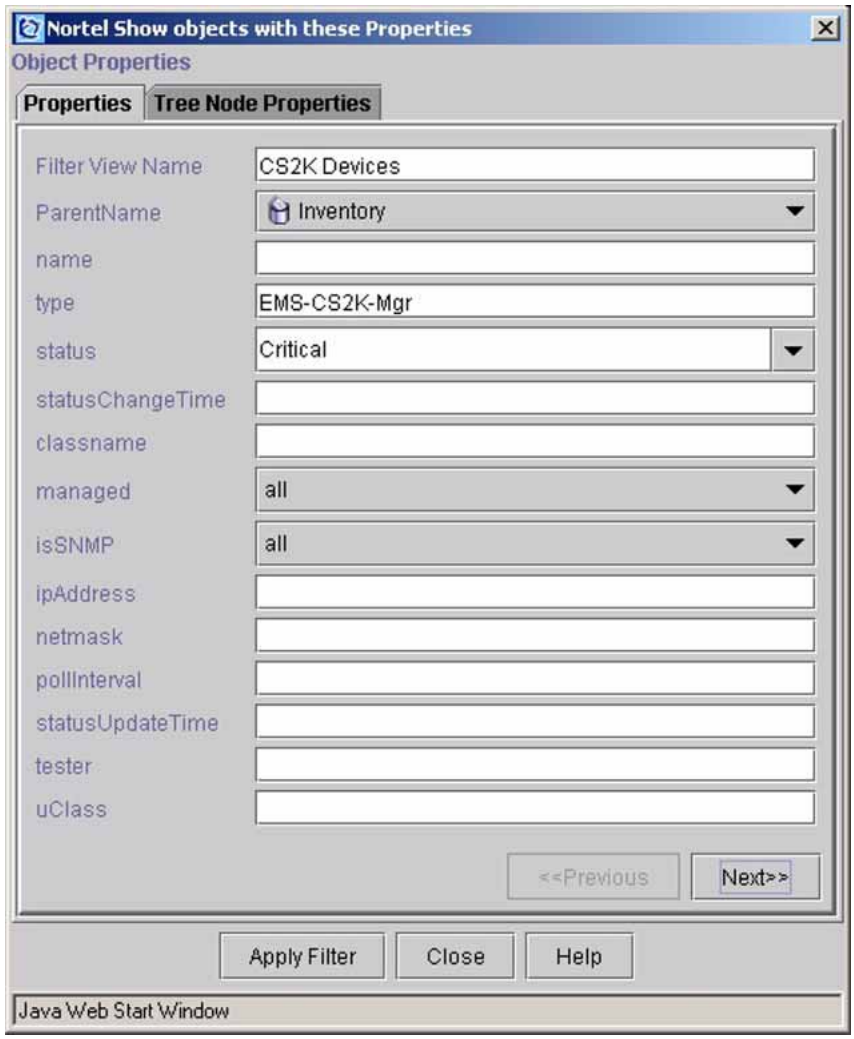
In the Matching Criteria section, you can find the properties with which you can filter events.

In this example, a custom view is created for the inventory details of all the CS 2000 Manager with ’Critical’ status.

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 **Inventory** node in the IEMS tree.
3	Right-click the Inventory node and select **Custom Views-->Add Custom Views** menu item. *The Object Properties form is displayed.*
4	Enter the value "CS2K Devices" in the Filter Value Name field.
5	Enter the value "EMS-CS2K-Mgr" in the Type field, since the device with type "CS2K" is filtered and displayed in custom view.
6	Select the **Critical** value from the Status editable list box. *A GUI similar to the following screen shot is displayed.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



7 Click the **Next** button to proceed to the next screen of the wizard.

8 Click the **Select Props To View** button.

The Select Table Columns window is displayed.

9 Select the following text boxes with the text

- Name
- Type
- Last Changed Time
- Managed

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

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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

You have completed this procedure.

The match criteria for a custom view can be modified after they are created. This is achieved by right-clicking the custom view and select the Custom Views-->Modify Custom View. This invokes the Object Properties form. You can also remove a custom view by right-clicking the custom view and selecting the Custom Views-->Remove Custom View.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks

Working with topologies in Web Client

The topology user interface displays a set of related objects, symbols, and sub-nodes that provide a graphical and hierarchical representation of element managers, network elements, EMS applications, and platforms. The topology nodes of the Web Client provides a view of the networks and systems using Web Client. The topology is displayed on the frame on the right. The frame on the left contains a tree view to navigate between different topology views.

This section describes how to add objects such as element managers, network elements, EMS applications, and platforms. In addition, this section provides procedures on how to view the map details, manage or unmanage, and perform other operations.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding objects to the topology in Web Client

This section describes the procedures on how to add the objects to the IEMS topology using Web Client. A map symbol is associated with a managed object representing its status. When you add an object to the IEMS topology, the corresponding map symbol is added to the associated topology. The procedures on how to add these various objects are provided in the following subsections:

- "Adding platforms using Web Client" (page 285)
- "Adding element managers in Web Client" (page 289)
- "Adding EMS applications in Web Client" (page 319)
- "Adding network elements in Web Client" (page 329)

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 an invalid IP address.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding platforms using Web Client

This section provides the procedures on how to add the SPFS and MDM platforms to the IEMS topology using Web Client.

SDM platforms are automatically discovered by the IEMS and added to the topology. The discovered SDM platform map symbols can be viewed under the **EMS Platforms** topology node in the Module tree of the Web Client.

Copyright © 2006, Nortel Networks

Adding an MDM platform using Web Client

Application

Use this procedure to add the MDM platform version to the topology in the Web Client.

The MDM platform is the runtime environment for various Nortel EMSs and applications. The IEMS adds the MDM platform automatically when adding the MDM to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Select the **Add Platform** node under the Network Admin tree to invoke the Add Platform page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **MDM** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Click the **Add Platform** button to add the MDM platform. *Once the MDM platform is added, the "Successfully added to the database" message is displayed. The MDM platform with the specified name is added as a map symbol under the grouped MDM map symbol in the EMS Platforms display panel. It is also added to the MDM topology under the* ***EMS Platforms*** *topology node in the Module tree of Web Client.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an SPFS platform using Web Client

Application

Use this procedure to add the SPFS platform to the topology using Web Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

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 **Admin** tab in the Web Client.
3	Select the **Add Platform** node under the Network Admin tree. *The Add Platform page in the right-side frame appears.*
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **SPFS** from the Device Type list box.
6	Select the mode from the Mode list box. If **Simplex** is selected from the Mode list box, follow a and proceed to step 7. If **Duplex** is selected from the Mode list box, follow these steps: a. Enter the IP address of the active unit in the Unit-0 IP Address field. b. Enter the IP address of the inactive unit in the Unit-1 IP Address field.
7	Select the version of the device from the Device Version list box.
8	Check the **Radius Secret** check box to enable the RADIUS secret password and enter the RADIUS secret password in the Radius Secret field. If the **Radius Secret** check box is checked and the password is not entered, the wizard displays "Enter the radius secret" error.
9	Select the **Fault Interface** from the vertical button.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 Enter the port value "2222" (in which the SPFS communicates with IEMS) in the Port field.

11 Enter the community in the Community field.

12 Select the SNMP version **v2c** from the Version list box.

13 Click the **Performance Interface** from the vertical tab.

14 Enter the port value "1161" in the Port field.

15 Enter the community in the Community field.

16 Select the SNMP version **v1** from the Version list box.

17 Click the **Add Platform** button to add the SPFS platform.

*Once the SPFS platform is added, the "Successfully added to the database" message is displayed. The SPFS platform with the specified name is added as a map symbol under the grouped SPFS map symbol in the **EMS Platforms** topology panel. It is also added to the SPFS topology under **EMS Platforms** in the topology tree.*

The IEMS only correlates events received from the SPFS SNMP interface. The non-SNMP interfaces such as SYSLOG must be disabled using the "disable local logging" option from CLI. For details, refer to the "Disabling local logging of SPFS platform faults" section in *ATM/IP Solution-level Fault Management*, NN10408-900.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding element managers in Web Client

IEMS provides an integration point for the various element managers. It allows a centralized point to launch the various element managers and the ability to view the faults from these systems in a common graphical interface. This section describes the procedure on how to add an element manager to the IEMS topology using Web Client.

When element manager systems are added to the IEMS topology, the network elements managed by the element managers are discovered automatically and added to the IEMS topology.

IEMS supports dynamic updates for some of the element managers. IEMS topology is updated based on the objects managed by the corresponding element managers. IEMS supports dynamic topology updates for the following element managers:

- Audio Provisioning Server Manager
- Universal Audio Server Manager
- GWC Manager

Copyright © 2006, Nortel Networks

Adding an APS Manager using Web Client

Application

Use this procedure to add the Audio Provisioning Server Manager to the IEMS topology 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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields in the Add EMS/NE page. For details on these fields, refer to the following table:

Description of fields in Add EMS/NE page

Field	Description
Host Name/IP Address	The field for the host name or IP address of the element manager.
Time Zone	A list box to select the time zone associated with the object.

5	Select **EMS** from the Type list box.
6	Select **APS Mgr** from the Device Type list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Select the version of the device from the Device Version list box.
9	Click the **Add EMS/NE** button to add the APS Manager. *Once the APS Manager is added, "Successfully added to the database" message is displayed. The APS Manager with the specified name is added as a map symbol to the Element Managers*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

topology. In addition, a topology node named APS Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a CEM using Web Client

Application

Use this procedure to add a Core Element Manager (CEM) to the IEMS topology using Web Client.

The Core Element Manager is available with selected versions of Carrier VoIP platforms. Hence, Core Element Manager is available in selected sites of Carrier VoIP platforms.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
5	Select **EMS** from the Type list box.
6	Select **CEM Mgr** from the Device Type list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Add EMS/NE** button to add the Core Element Manager. *Once the Core Element Manager is added, "Successfully added to the database" message is displayed. The Core Element Manager with the specified name is added as a map symbol to the Element Managers topology.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a CICM Manager using Web Client

Application

Use this procedure to add a CICM Manager to the IEMS topology using Web Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

For IEMS to receive CICM fault and performance data

CICM Manager must be configured to send fault data to IEMS. The CICM has a script called **preboot** which is used to configure the CICM with the IEMS server virtual IP address and port for sending the fault data to IEMS. Without this configuration, IEMS receives no faults from CICM.

For launching CICM Manager

CICM Manager has to be configured using the SPFS CLI tool for launching CICM Manager from IEMS Client. For details, refer to *CICM Configuration*, NN10240-511.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard.
5	Select **EMS** from the Type list box.
6	Select **CICM Mgr** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

9 Select the manager unit mode from the Mode list box. If **Duplex** mode is selected, enter the inactive unit IP in the Inactive Unit IP field.

10 Enter the card location in the Card Location field.

11 Select the **Fault Interface** from the vertical tab.

12 Enter the port (in which the EMS communicates with IEMS) in the Port field or retain the default value as "161".

13 Enter the community in the Community field.

14 Select the SNMP version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

15 Select the **Performance Interface** from the vertical tab.

16 Repeat step 12 to step 14.

17 Click the **Add EMS/NE** button to add the CICM Manager.

Once the CICM Manager is added, the "Successfully added to the database" message is displayed. The CICM Manager with the specified name is added as a map symbol to the Element Managers topology.

You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks

Adding a CS 2000 Core Manager using Web Client

Application

Use this procedure to add a CS 2000 Manager in IEMS topology using Web Client. The CS 2000 Core Manager residing on an SPFS platform is known as Core Billing Manager (CBM).

ATTENTION

While configuring the CS 2000 Core Manager logroute, ensure the following:

- Logroute on the associated SDM must be configured for TCPIN.
- Logroute on the associated SDM must be configured with ECORE set to OFF.
- Logroute on a CS 2000 Core Manager with a pre SDM20 software load version: the associated SDM log format must be set to STD or SCC2.
- Logroute on a CS 2000 Core Manager with a SDM20 or greater software load version: the associated SDM log format must be set to STD_OLD or SCC2_OLD.
- Logroute on a CS 2000 Core Manager residing on SSPFS platform or CBM, the associated log format must be set to SCC2 (not NTSTD).
- Logroute on a CS 2000 Core Manager residing on a SDM/CBM must be set to SCC2 (not NTSTD) as the associated log format.

The end of log format for the NTSTD and SCC2 feeds can be configured in IEMS by modifying the MLDefaultParams.xml file under the /opt/nortel/iems/current/conf folder. The SCC2 end of log format is specified in "SCC2_MESSAGE ENDOFLOG" parameter, and the NTSTD end of log format is specified in "NTSTD_MESSAGE ENDOFLOG" parameter. The end of log format must use the X character format and be separated with a colon (":"). The default end of log format values in MLDefaultParams.xml file are:

- SCC2_MESSAGE ENDOFLOG="0A:0D:20:0A:0D"
- NTSTD_MESSAGE ENDOFLOG="0A:19:0A:0D"

If the end of log format is changed in the MLDefaultParams.conf, the IEMS server requires a restart to reflect the changes.

IEMS polls periodically to check the CS 2000 platform object status. If the data is not received between two status polls, IEMS disconnects and reconnects the CS 2000 Core Manager. If the reconnect attempt throws an

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

error, the CS 2000 Core Manager and its corresponding components turn to an unknown object status in IEMS. The map symbols of these objects turns to a gray background.

It is suggested that the polling interval for the CS 2000 Core Manager object in IEMS retain (or be left near) the default value (300 seconds). Reducing this significantly can result in frequent and unnecessary attempts to reconnect to the CS 2000 Core Manager fault feed.

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

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Change the values to include name, time zone, and display name.
5	Select **EMS** from the Type list box.
6	Select **CS2K Core Mgr** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "SDM" if it belongs to SDM platform or SPFS. If SDM check the **Radius Secret** checkbox to enable the RADIUS secret password and enter RADIUS secret password in the Radius Secret field. If the Radius Secret field is checked and the password is not entered, the wizard displays "Enter the radius secret" error. To configure Radius Secret refer to: • *IEMS Administration and Security*, NN10336-611 • *ATM/IP Solution-Level Administration and Security*, NN10402-600.
9	Select the NE type **CS 2000 Core** or **Call Agent Core** from the Managing NE Type list box. By default, "CS 2000 Core" is selected

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

in the list box. If you select CS 2000 Core from the Managing NE Type list box, enter the CS 2000 Core device IP address in the CS 2000 Core IP Address field. If you select Call Agent Core from the Managing NE Type list box, follow these steps:

a. Select the mode from the Mode list box. If "Duplex" item is selected, perform sub-step and proceed to .

b. Type the valid IP address of the active unit in the Active Unit IP field.

c. Type the valid IP address of the inactive unit in the Inactive Unit IP field.

10 Select the Fault Interface from the vertical tab.

11 Refer to the Attention box and select the log format SCC2 or NTSTD from the Log Format list box.

12 Enter the port in the Port field.

The CS 2000 Core Manager sends log messages either through the NTSTD interface or through the SCC2 interface. Select the applicable interface fields and enter the port (if different from default value).

13 Click the **Add EMS** button to add the CS 2000 Core Manager.

Once the CS 2000 Core Manager is added, "Successfully added to the database" message is displayed. The CS 2000 Core Manager with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named CS 2000 Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Fault and Performance Manager using Web Client

Application

Use this procedure to add a Fault and Performance Manager (FPM) to the IEMS topology using Web Client.

Prerequisites

To add an FPM, the corresponding MCS must be added to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Enter the values for the Host Name/IP Address and Time Zone fields.
4	Select the **Add EMS/NE** node under the Network Admin tree.
5	Select **EMS** from the Type list box.
6	Select **FPM Mgr** from the Device Type list box.
7	Select the version in the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "None" if it does not belongs to any platform.
9	Select the mode in the Mode list box. If **Duplex** mode is selected, enter the primary IP address and secondary IP address in the Instance 0 and Instance 1 fields respectively.
10	Select the MCS Manager to which the FPM corresponds from the MCS Managers list box.
11	Enter the user name of the device in the User Name field.
12	Select the **Fault Interface** from the vertical tab.
13	Enter the port value through which the EMS communicates with IEMS in the Port field. The port value is <FPM device base port

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

number>+17. For example, if the FPM device port is 65400, then the port number is 65417.

14 Enter the community in the Community field.

15 Select the SNMP version **v2c** from the Version list box.

The port value and SNMP version are dependent on the MCS Manager configuration which is added.

16 Select the **Performance Interface** from the vertical tab.

17 Enter the directory name of the CSV file (present in the device) in the Directory field.

18 Enter the file mask of the CSV file (present in the device) in the File Mask field.

Wildcard support is available for this field.

Example

If the file names starts with "CSVOM" string, user can enter the value "CSVOM*.closed".

19 Enter the user name for SFTP-PULL in the User ID field.

20 Enter the password in the Password field.

21 Click the **Add EMS/NE** button to add the FPM.

Once the FPM is added, the "Successfully added to the database" message is displayed in the status bar. The details on how the map symbol and FPM node is added under Element Managers node, refer to "Adding a Fault and Performance Manager" (page 37).

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a GWC Manager using Web Client

Application

Use this procedure to add a Gateway Controller (GWC) Manager to the IEMS topology using Web Client.

Gateway Controller Manager manages Gateway Controller NEs.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **EMS** from the Type list box.
6	Select **GWC Mgr** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
9	Click the **Add EMS/NE** button to add the GWC Manager. *Once the GWC Manager is added, "Successfully added to the database" message is displayed. The GWC Manager with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named GWC Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MCS Manager for MCS/CSE and Media Portal using Web Client

Application

Use this procedure to add the MCS Manager for MCS/CSE and Media Portal to the IEMS topology using Web Client. The MCS Manager is also known as the MCS system manager (MCS SM) or MCS 5200.

When adding an MCS Manager to an SPFS HA configuration in IEMS, both the active and inactive MCS Manager must be added as separate objects in IEMS topology. The physical IP address of active or inactive MCS Manager host must be entered in the Name field of the Add EMS/NE wizard. If the events are received from MCS Manager with a virtual IP address, the events received from corresponding MCS Manager are correlated as events from unknown device.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

The following sections list the MCS Manager configuration references required to integrate with the IEMS.

Fault interface

Refer to "SNMP information" and "Configuring an SNMP Manager" in *System Manager*, NN10030-111. The MCS SNMP trap destination must be configured in the device for the IEMS to manage its fault interface.

Configuration interface

No additional configuration is required.

Performance management

No additional configuration is required.

Security configuration

No additional configuration is required.

MCS Client launch

MCS client launch is available only on a PC that has MCS software installed. For details of how to install the software, refer to *MCS System Management Console User Guide*, NN10247-111. MCS Client software can be launched only in Microsoft Windows platforms.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Name, Time Zone, and Display Name fields.
5	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
6	Select **EMS** from the Type list box.
7	Select **MCS Mgr** from the Device Type list box.
8	Select the version of the device from the Device Version list box.
9	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
10	Select the NE type from the Managing NE Type list box. By default, MCS/CSE MX is selected in the list box.
11	Select the mode of the device from the Mode list box. If **Duplex** mode is selected, enter the primary IP address and secondary IP address in the Instance 0 and Instance 1 fields respectively.
12	Enter the user name of the device in the User Name field.
13	Select the **Fault Interface** from the vertical tab.
14	In the Port field, enter the port value (in which the EMS communicates with IEMS).
15	Enter the community in the Community field.
16	Select the SNMP version **v2c** from the Version list box. The port value and SNMP version are dependent on the MCS Manager configuration that is added.
17	Select the **Performance Interface** from the vertical tab.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Performance metrics will be collected from both servers during a SWACT.

18 Enter the directory name where the CSV file (is present in the device) in the Directory Name field.

19 Enter the file mask of the CSV file (present in the device) in the File Name field.

Wildcard support is available for this field.

Example

If the file names starts with "CSVOM" string, the user can enter the value "CSVOM*.closed".

20 Enter the user name for SFTP-PULL in the User ID field.

21 Enter the password in the Password field.

22 Click the **Add EMS/NE** button to add the MCS Manager.

Once the MCS Manager is added, the "Successfully added to the database" message is displayed in the status bar. The MCS Manager with the specified name is added as a map symbol to the Element Managers topology.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MCS Manager for SSLines using Web Client

Application

Use this procedure to add the MCS Manager for SSLines to the IEMS topology using Web Client.

The MCS system manager (MCS SM) is also known as MCS Manager.

When adding an MCS Manager for SSLines for an SPFS HA configuration in IEMS, both the active and inactive MCS Manager must be added as separate objects in IEMS topology. The logical IP address of active or inactive MCS Manager host must be entered in the Name field of the Add EMS/NE wizard.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS logical IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

The following sections list the MCS Manager configuration references required to integrate with the IEMS.

Fault interface

Refer to "SNMP information" and "Configuring an SNMP Manager" in *System Manager Overview*, NN10030-111. The MCS SNMP trap destination must be configured in the device for the IEMS to manage its fault interface.

Configuration interface

To configure the Apache Web Server on an SPFS-based server for HTTPS proxy, see Configuring the Apache Web Server for HTTPS proxy in *ATM/IP Solution-level Configuration*, NN10409-500.

To configure the HTTPS proxy for SSLines, see *Session Server Lines - SIP Voice Basics*, NN10437-111.

Performance management

No additional configuration is required.

Security configuration

No additional configuration is required.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

MCS Client launch

MCS client launch is available only on a PC that has MCS software installed. For details of how to install the software, refer to *MCS System Management Console User Guide*, NN10247-111. MCS Client software can be launched only in Microsoft Windows platforms.

To launch the MCP Provisioning Client from the Element Manager for SSLines, you must configure the IEMS with the IP addresses for the provisioning servers. Refer to "Configuring provisioning clients" (page 58).

To launch the Session and System Manager Command Line from the Element Manager for SSLines, you must configure the IEMS with the IP addresses for the Session Manager and System Manager servers. Refer to "Configuring Session Managers for SSH launch" (page 56).

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Name, Time Zone, and Display Name fields.
5	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
6	Select **EMS** from the Type list box.
7	Select **SSLines Mgr** from the Device Type list box.
8	Select the version of the device from the Device Version list box.
9	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
10	Select the mode of the device from the Mode list box. If **Duplex** mode is selected, enter the primary IP address and secondary IP address in the Instance 0 and Instance 1 fields respectively.
11	Enter the user name of the device in the User Name field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

12 Select the **Fault Interface** from the vertical tab.

13 In the Port field, enter the port value (through which the EMS communicates with IEMS).

14 Enter the community in the Community field.

15 Select the SNMP version **v2c** from the SNMP Version list box.

The port value and SNMP version are dependent on the MCS Manager for SSLines configuration that is added.

16 Select the **Performance Interface** from the vertical tab.

Performance metrics will be collected from both servers during a SWACT.

17 Enter the directory name where the CSV file (is present in the device) in the Directory Name field.

18 Enter the file mask of the CSV file (present in the device) in the File Mask field.

Wildcard support is available for this field.

Example

If the file names starts with "CSVOM" string, the user can enter the value "CSVOM*.closed".

19 Enter the user name for SFTP-PULL in the User ID field.

20 Enter the password in the Password field.

21 Click the **Add EMS/NE** button to add the MCS Manager for SSLines.

Once the MCS Manager for SSLines is added, a "Successfully added to the database" message is displayed in the status bar. The MCS Manager for SSLines with the specified name is added as a map symbol to the Element Managers topology.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MDM using Web Client

Application

Use this procedure to add the Multiservice Data Manager to the IEMS topology using Web Client. Multiservice Data Manager manages Media Gateway7480/15000/20000 and Multiservice Switch 15000 NEs.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to open the Add EMS/NE page.
4	Enter the values for the Name, Time Zone, and Display Name fields.
5	Select **EMS** from the Type list box.
6	Select **MDM** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
9	Select the manager unit mode from the Mode list box. There are two modes to be selected based on whether the MDM application is to run in a simplex or duplex mode. In the simplex mode, the MDM application is configured in one machine, while in the duplex mode the application is configured to run in two machines. In the duplex mode configuration, the IEMS switches over to the alternate (or secondary) machine in which the MDM application is executing, when the current (or primary) machine is down.

If the mode is	Do
simplex	follow step 11 to step 14 and proceed to step 17
duplex	follow step 10 to step 20

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 Enter the secondary machine IP address in which the MDM application is to run, for the Inactive Unit IP field.

Do not specify the IP address 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 an invalid IP address.

11 Configure the user name and password under the **MDM Account Details** section for centralized account common to all MDM devices.Changing the user name or password for any MDM device is reflected for all MDM devices.

The **MDM Account Details** section is displayed when an MDM device is added to the IEMS for the first time.

12 Select the **Fault Interface** from the vertical tab.

13 In the Port field of the Primary panel, enter the port in which log messages are sent by the MDM element manager.

14 Enter the user identification in the User ID field of the Primary panel.

15 In the Port field of the Secondary panel, enter the port in which log messages are sent by MDM element manager.

16 Enter the user identification in the User ID field of the Secondary panel.

17 Select the **Performance Interface** from the vertical tab.

A Performance Measurement Stream Processor (PMSP) server must already be configured on the MDM workstation. For more information, refer to "Start-up command" in section "Performance Measurement Stream Processor (PMSP)" of *Nortel Networks Multiservice Data Manager Server Reference*, 241-6001-310.

18 Enter the port in the Five Min Collection Port field.

The port configured in this field is scheduled to collect data every five minutes from the NEs managed by the MDM application. The port number must match the 5-minute TCP port number configured for the MDM's PMSP server. The default port is 1646.

19 Enter the port in the Thirty Min Collection Port field.

The port configured in this field is scheduled to collect data every thirty minutes from the NEs managed by the MDM application. The port number must match the 30-minute TCP port number configured for the MDM's PMSP server. The default port is 1647.

20 Click the **Add EMS** button to add the Multiservice Data Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

After the Multiservice Data Manager is added, provision the client-server IP address with the procedure explained in "Launching Multiservice Data Manager" in *IEMS Overview*, NN10329-111.

Once the MDM is added, a "Successfully added to the database" message is displayed. The MDM with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named MDM with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MG 9000 Manager using Web Client

Application

Use this procedure to add the MG 9000 Manager to the topology using Web Client.

MG 9000 Manager manages MG 9000 NEs.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **EMS** from the Type list box.
6	Select **MG9K Mgr** from the Device Type list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Select the version of the device from the Device Version list box.
9	Enter the valid IP address in MG9K Mid Tier IP field. The IP address of the Mid Tier existing between IEMS and MG 9000 Manager must be provided here.
10	Select the **Fault Interface** from the vertical tab.
11	Enter the subnet value with version in the Subnet (with version) field.
12	Select the **Performance Interface** from the vertical tab.
13	Enter the user name for SFTP-PULL in the User ID field.
14	Enter the password in the Password field.
15	Click the **Add EMS/NE** button to add the MG 9000 Manager.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Once the MG 9000 Manager is added, "Successfully added to the database" message is displayed. The MG 9000 Manager with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named MG 9000 Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a SAM21 Manager using Web Client

Application

Use this procedure to add a Services Application Module (SAM21) Manager to the IEMS topology using Web Client.

SAM 21 Manager manages SAM21 NEs.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **EMS** from the Type list box.
6	Select **SAM21 Mgr** from the Device Type list box. *The various fields display the location of various log files such as Customer Log File, Audit Log File, and Security Log File.*
7	Select the version of the device from the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
9	Click the **Add EMS/NE** button to add the SAM21 Manager. *Once the SAM21 Manager is added, "Successfully added to the database" message is displayed. The SAM21 Manager with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named SAM21 Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a UAS Manager using Web Client

Application

Use this procedure to add a Universal Audio Server (UAS) Manager to the topology using Web Client.

Universal Audio Server Manager manages Universal Audio Server NEs.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **EMS** from the Type list box.
6	Select the **UAS Mgr** value from the Device Type list box. *The channel name and the administrator name are displayed in various fields.*
7	Select the version of the device from the Device Version list box.
8	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
9	Click the **Add EMS/NE** button to add the Universal Audio Server Manager. *Once the Universal Audio Server Manager is added, "Successfully added to the database" message is displayed. The UAS Manager with the specified name is added as a map symbol to the Element Managers topology. In addition, a topology node named UAS Manager with the specified display name in brackets is added under the Element Managers topology node in the IEMS tree.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a UNEM using Web Client

Application

Use this procedure to add a UNEM to the IEMS topology using Web Client. UNEM manages UMUX 1500, UMUX 1200, and UMUX 900 NEs in the UMUX network.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the **Network Admin** tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Name, Time Zone, and Display Name fields.
5	Select the **Add EMS/NE** node under the **Network Admin** tree to invoke the Add EMS/NE page in the right-side frame.
6	Select "EMS" from the **Type** list box.
7	Select "UNEM" from the **Device Type** list box.
8	Select the **SSH enabled** field if the SSH is enabled in the UNEM device. If the SSH enabled field is selected and the UNEM server does not have SSH installed, the launching of the UNEM browser from UNEM and UMUX NEs and the launching of UMUX Shelf Configuration fails. For the procedure to launch the UNEM browser for UNEM, refer to "Launching the UNEM browser for UNEM" in *IEMS Overview*, NN10329-111. For the procedure to launch the application for UMUX NEs, refer to "Launching applications for UMUX NEs" in *IEMS Overview*, NN10329-111.
9	Select the **Fault Interface** from the vertical tab.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

10 In the **Port** field, enter the port value (in which the EMS communicates with IEMS).

11 Enter the community in the **Community** field.

12 Click the **Add EMS/NE** button to add the UNEM.

*Once the UNEM is added, the "Successfully added to the database" message is displayed in the status bar. The UNEM with the specified name is added as a map symbol to the **Element Managers** topology*.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding EMS applications in Web Client

EMS applications manage elements in a network. This section describes how to add EMS applications to the IEMS topology using Web Client.

Copyright © 2006, Nortel Networks

Adding an LMM application using Web Client

Application

Use this procedure to add the LMM application to the IEMS topology using Web Client.

IEMS manages the Line Maintenance Manager (LMM) application after it is added to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to invoke the Add Application page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **LMM** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Add Application** button to add the LMM application. *Once the LMM application is added, "Successfully added to the database" message is displayed. The LMM application with the specified name is added as a map symbol under the grouped LMM map symbol in the EMS Applications topology panel. It is also added to the LMM topology under the EMS Applications topology node in the IEMS tree.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an NPM application using Web Client

Application

Use this procedure to add Network Patch Manager (NPM) application to the IEMS topology using Web Client.

IEMS manages the Network Patch Manager application after it is added to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to invoke the Add Application page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields in the wizard.
5	Select **NPM** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Add Application** button to add the NPM application. *Once the NPM application is added, the "Successfully added to the database" message is displayed. The NPM application with the specified name is added as a map symbol under the grouped NPM map symbol in the EMS Applications topology. It is also added to the NPM topology under the EMS Applications topology node in the IEMS tree.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an OSSGate application using Web Client

Application

Use this procedure to add the OSSGate to the topology using Web Client.

IEMS manages OSSGate application after it is added to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to invoke the Add Application page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **OSSGate** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Add Application** button to add the OSSGate application. *Once the OSSGate application is added, "Successfully added to the database" message is displayed. The OSSGate application with the specified name is added as a map symbol under the grouped OSSGate map symbol in the EMS Applications topology panel. It is also added to the OSSGate topology under the EMS Applications topology node in the IEMS tree.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a QCA using Web Client

Application

Use this procedure to add the QoS Collector application to the IEMS topology using Web Client.

IEMS manages the QoS Collector application after it is added to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to invoke the Add Application page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields in the wizard.
5	Select **QoS Collector** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Add Application** button to add the QoS Collector application. *Once the QoS Collector application is added, the "Successfully added to the database" message is displayed. The QoS Collector application with the specified name is added as a map symbol under the grouped QoS Collector map symbol in the EMS Applications topology panel. It is also added to the **QoS Collector** topology under the EMS Applications topology node in the IEMS tree.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an SBRM application using Web Client

Application

Use this procedure to add the SBRM application to the IEMS topology using Web Client.

IEMS manages the SBRM application after it is added to the IEMS topology.

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	Click the **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to invoke the Add Application page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields in the wizard.
5	Select **SBRM** from the Device Type list box.
6	Click the **Add Application** button to add the SBRM application. *Once the SBRM application is added, the "Successfully added to the database" message is displayed. The SBRM application with the specified name is added as a map symbol under the grouped SBRM map symbol in the EMS Applications topology panel. It is also added to the SBRM topology under the EMS Applications topology node in the IEMS tree.* You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a TMM application using Web Client

Application

Use this procedure to add the Trunk Maintenance Manager (TMM) application to the IEMS topology using Web Client.

IEMS manages the Trunk Maintenance Manager application after it is added to the IEMS topology.

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 **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to invoke the Add Application page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **TMM** from the Device Type list box.
6	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
7	Click the **Add Application** button to add the TMM application. *Once the TMM application is added, the "Successfully added to the database" message is displayed. The TMM application with the specified name is added as a map symbol under the grouped TMM map symbol in the EMS Applications topology panel. It is also added to the TMM topology under the EMS Applications topology node in the IEMS tree.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a Certificate Manager application using Web Client

Application

Use this procedure to add a Certificate Manager application to the IEMS topology using Web Client.

Prerequisites

This procedure has the following prerequisites:

- you must belong to the emsadm group to add the Certificate Manager application.

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 **Admin** tab in the Web Client.
3	Select the **Add Application** node under the Network Admin tree to open the Add Application page.
4	Enter the values in the Name, Time Zone, and Display Name fields.
5	Select **CertMgr** from the Device Type list box.
6	Select the version of the device from the Device Version list box.
7	Select the associated platform from the Platform list box or retain the default value "None" if it does not belong to any platform.
8	Click the **Add Application** button to add the Certificate Manager application. *Once the Certificate Manager application is added, a message appears in the status bar that reads "Successfully added to the database" . The Certificate Manager application is added as a map symbol under the grouped CertMgr map symbol in the EMS Applications topology panel. It is also added under **EMS Applications** in the IEMS tree.*
9	You have completed this procedure.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding network elements in Web Client

IEMS manages the fault domain and provides a centralized location to access the management interfaces. This section describes how to add these NEs using Web Client.

Copyright © 2006, Nortel Networks

Adding a CICM NE using Web Client

Application

Use this procedure to add a CICM NE to the topology using Web Client.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

For IEMS to receive CICM fault and performance data

CICM Manager must be configured to send fault data to IEMS. The CICM has a script called **preboot** which is used to configure the CICM with the IEMS server virtual IP address and port for sending the fault data to IEMS. Without this configuration, IEMS receives no faults from CICM.

For launching CICM Manager

CICM Manager has to be configured using the SPFS CLI tool for launching CICM Manager from the IEMS client. For details, refer to *CICM Configuration*, NN10240-511.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **NE** from the Type list box.
6	Select **CICM** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Select the NE unit mode from the Mode list box. If **Duplex** mode is selected, follow these steps: a. Enter the inactive unit IP in the Inactive-Unit IP field,

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

b. Enter the Card B IP address in the Card B IP Address field.

c. Enter the Card B display name in the Card B Display Name field.

9 Enter the card location in the Card Location field.

10 Enter the Card A IP address in the Card A IP Address field.

11 Select the **Fault Interface** from the vertical tab.

12 Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".

13 Enter the community in the Community field.

14 Select the SNMP version from the Version list box. If you select **v3** from the Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

15 Select the **Performance Interface** from the vertical tab.

16 Repeat step 12 to step 14.

17 Click the **Add EMS/NE** button to add the CICM.

Once the CICM NE is added, a "Successfully added to database" message is displayed in the status bar. The CICM NE with the specified name is added as a map symbol under the grouped CICM

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

map symbol in the Network Elements topology panel. It is also added to the CICM topology under the Network Elements topology node in the Module tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks

Adding an Ethernet Routing Switch 8600 NE using Web Client

Application

Use this procedure to add the Ethernet Routing Switch (ERS) 8600 NE to the topology using Web Client.

ERS 8600 NEs can be managed using IEMS by adding them to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

For IEMS to receive ERS 8600 fault and performance data

ERS 8600 NEs must be configured to send fault and performance data to IEMS; without this configuration, IEMS receives no fault and performance data from ERS 8600 NEs.

For launching ERS 8600 Device Manager

ERS 8600 Device Manager must be installed on the client machine in order to launch the GUI. For details of how to install the Device Manager, refer to *Installing ERS 8600 Switch Modules*-312749F.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Name, Time Zone, and Display Name fields.
5	Select **NE** from the Type list box.
6	Select **ERS 8600** from the Device Type list box.
7	Select the version of the device from the Device Version list box.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

8 Select the **Fault Interface** from the vertical tab.

9 Enter the Port in the **Port** field or retain the default value as "161".

10 Enter the Community in the **Community** field.

11 Select the SNMP Version from the **Version** list box. If you select "v3" from Version list box, select the security level from the Security Level list box. If you select the value "NoAuthNoPriv" from the Security Level list box, enter the following details:

- User Name
- Context Name

If you select the value "AuthNoPriv" from the Security Level list box, enter the following details:

- User Name
- Context Name
- Authentication Protocol

If you select the value "AuthPriv" from the Security Level list box, enter the following details:

- User Name
- Context Name
- Authentication Protocol
- Privacy Protocol

12 Select the **Performance Interface** from the vertical tab.

13 Repeat step 9 to step 11.

14 Click the **Add EMS/NE** button.

Once the ERS 8600 is added, the "Successfully added to database" message is displayed in the status bar. The ERS 8600 NE with the specified name is added as a map symbol under the grouped ERS 8600 map symbol in the Network Elements topology panel. It is also added to the ERS 8600 topology under the Network Elements topology node in the Module tree..

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MAS NE using Web Client

Application

Use this procedure to add the MAS NE to the topology using Web Client.

MAS NEs can be managed using IEMS by adding them to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

For further details on configuring the MAS, refer to *Nortel Media Application Server Configuration*, NN10455-511.

Prerequisites

MAS must be configured to send fault data to IEMS; without this configuration, IEMS receives no fault and performance data from MAS NEs.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **NE** from the Type list box.
6	Select **MAS** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Select the **Fault Interface** from the vertical tab.
9	Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".
10	Enter the community in the Community field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

11 Select the SNMP version from the Version list box. If you select **v3** from the Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

12 Select the **Performance Interface** from the vertical tab.

13 Enter the directory name where the CSV file is getting pushed in IEMS Server from the device in the Directory Name field.

14 Enter the file mask of the CSV file getting pushed in the File Name field.

Wildcard support is available for this field.

Example
If the file names starts with the "SystemOMs" string, user can enter the value "SystemOMs*.csv".

While configuring each MAS device, ensure that the operational measurement (OM) file names are unique. This is useful to differentiate data transmitted from each of the devices.

15 Retain the **PUSH** mode of file transfer selected in the Mode list box.

In the Mode list box, the **PUSH** mode of file transfer must be selected.

16 Click the **Add EMS/NE** button to add the MAS NE.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Once the MAS NE is added, the "Successfully added to database" message is displayed in the status bar. The MAS NE with the specified name is added as a map symbol under the grouped MAS map symbol in the Network Elements topology panel. It is also added to the MAS topology under the Network Elements topology node in the Module tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MG 3200 NE using Web Client

Application

Use this procedure to add the Media Server 3200 (MG 3200) NE to the topology using Web Client. The Media Server 3200 NE can be managed using IEMS by adding it to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

For IEMS to receive MG3200 fault and performance data, MG 3200 must be configured to send fault data to IEMS. For details, refer to *MG 3200 H.248 User's Manual*, LTRT72704

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the **Network Admin** tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Name, Time Zone, and Display Name fields.
5	Select "NE" from the **Type** list box.
6	Select "MG 3200" from the **Device Type** list box.
7	Select the version of the device from the **Device Version** list box.
8	Enter the Web server user name in the **User Name** field.
9	Enter the Web server password in the **Web Password** field.
10	Select the **Fault Interface** from the vertical tab.
11	Enter the Port in the **Port** field or retain the default value as "161".
12	Enter the Community in the **Community** field.
13	Enter the Write Community in the **Write Community** field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

14 Select the SNMP Version from the **Version** list box. The version must be **v2c**.

15 Select the **Performance Interface** from the vertical tab.

16 Repeat step 11 to step 14 excluding step 13.

17 Click the **Add EMS/NE** button to add the MG 3200 NE.

*Once the MG 3200 NE is added, the "Successfully added to database" message is displayed in the status bar. The MG 3200 NE with the specified name is added as a map symbol under the grouped MG 3200 map symbol in the **Network Elements** topology panel. It is also added to the **MG 3200** topology under the **Network Elements** topology node in the Module tree.*

In order to launch the node's client interface, the HTTPS proxy must be configured using the SSPFS CLI tool" message is displayed.

For configuring the HTTPS proxy in the MG 3200, refer to Configuring MG 3200 HTTPS proxy in the *Nortel Media Gateway 3200 H.248 Configuration Guide*, LTRT72904.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding an MS 2000 NE using Web Client

Application

Use this procedure to add the Media Server 2000 (MS 2000) NE to the topology using Web Client.

Media Server 2000 NE can be managed using IEMS by adding them to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **NE** from the Type list box.
6	Select **MS2000** from the Device Type list box.
7	Select the version of the device from the Device Version list box.
8	Enter the Web server user name in the User Name field.
9	Enter the Web server password in the Web Password field.
10	Enter the SESM Server IP address in the SESM Server IP field.
11	Select the **Fault Interface** from the vertical tab.
12	Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".
13	Enter the community in the Community field.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

14 Select the SNMP version from the Version list box. If you select **v3** from the Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

15 Select the **Fault Interface** from the vertical tab.

16 Repeat step 10 to step 12.

17 Click the **Add EMS/NE** button to add the MS 2000 NE.

Once the MS 2000 NE is added, the "Successfully added to database" message is displayed in the status bar. The MS 2000 NE with the specified name is added as a map symbol under the grouped MS 2000 map symbol in the Network Elements topology panel. It is also added to the MS2000 topology under the Network Elements topology node in the Module tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a STORM NE using Web Client

Application

Use this procedure to add the STORM NE to the topology using Web Client.

STORM NEs can be managed using IEMS by adding them to the IEMS topology.

STORM-IEMS integration is not supported with the STORM dotHill configuration. The dotHill version of the STORM device does not have an SNMP agent to forward or read the faults from the STORM device. IEMS integration is only supported with the new STORM-XTS configuration.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

For IEMS to receive STORM fault and performance data

STORM must be configured to send fault data to IEMS. The STORM has a tool called *commish* which is used to configure the STORM with IEMS server virtual IP address and port for sending the fault data to IEMS; without this configuration, IEMS receives no fault data from STORM. For details, refer to "Configuring STORM for IEMS" (page 157) section.

For launching STORM Manager

STORM has to be configured using the SSPFS CLI tool for launching STORM manager from IEMS Client. For details, refer to *ATM/IP Solution-level Configuration*, NN10409-500.

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields in the wizard.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

5 Select **NE** from the Type list box.

6 Select **STORM** from the Device Type list box.

7 Select the version of the device from the Device Version list box.

8 Select the **Fault Interface** from the vertical tab.

9 Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".

10 Enter the community in the Community field.

11 Select the **SNMP** version from the Version list box. If you select **v3** from Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name

If you select the value **AuthNoPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol

If you select the value **AuthPriv** from the SecurityLevel list box, enter the following details:

- User name
- Context name
- Authentication Protocol
- Privacy Password

12 Select the **Performance Interface** from the vertical tab.

13 Repeat step 9 to step 11.

14 Click the **Add EMS/NE** button to add the STORM.

Once the STORM is added, the "Successfully added to the database" message is displayed. The STORM NE with the specified name is added as a map symbol under the grouped STORM map symbol in the Network Elements topology panel. It is also added to the STORM topology under the Network Elements topology node in the Module tree.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks

Adding an SSTrunks NE using Web Client

Application

Use this procedure to add the SSTrunks NE to the topology using Web Client.

SSTrunks NEs can be managed using IEMS by adding them to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

Prerequisites

The following sections list the SSTrunks NE configuration references required to integrate with the IEMS.

Fault interface

Refer to "Reprovision the NCGL platform software" in *Session Server - Trunks Configuration*, NN10338-511. The SSTrunks SNMP trap destination must be configured in the device for the IEMS to manage its fault interface.

Configuration interface

To configure the Apache Web Server on an SPFS-based server for HTTPS proxy, see *Session Server - Trunks Configuration*, NN10338-511.

Performance management

No additional configuration is required.

Security configuration

The security configuration is not integrated into the IEMS Centralized Security Server.

Launching SSTrunks client interface

Refer to "Add a Session Server - Trunks node to the SPFS server web proxy" of the *Session Server - Trunks Configuration Management*, NN10338-511. To launch the SSTrunks client interface from the IEMS, you must configure the SPFS HTTPS proxy on the IEMS server.

Action

Step	Action
	At the IEMS workstation

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

1. Launch the IEMS Web Client. Refer to Launching IEMS Web Client in *IEMS Overview*, NN10329-111.
2. Select the **Admin** tab in the Web Client.
3. Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4. Enter the values for the Host Name/IP Address and Time Zone fields.
5. Select **NE** from the Type list box.
6. Select **SSTrunks** from the Device Type list box.
7. Select the version of the device from the Device Version list box.
8. Select the device mode from the Mode list box.
9. Select the **Fault Interface** from the vertical tab.
10. Enter the port (in which the NE agent communicates with IEMS) in the Port field or retain the default value as "161".
11. Enter the community in the Community field.
12. Select the SNMP version from the Version list box. If you select **v3** from the Version list box, select the security level from the SecurityLevel list box. If you select the value **NoAuthNoPriv** from the SecurityLevel list box, enter the following details:
    - User name
    - Context name

    If you select the value AuthNoPriv from the SecurityLevel list box, enter the following details:
    - User name
    - Context name
    - Authentication Protocol

    If you select the value AuthPriv from the SecurityLevel list box, enter the following details:
    - User name
    - Context name
    - Authentication Protocol
    - Privacy Password
13. Select the **Performance Interface** from the vertical tab.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

14 Repeat step 10 to step 12.

15 Click the **Add EMS/NE** button to add the SSTrunks NE.

Once the SSTrunks is added, the "Successfully added to the database" message is displayed. The SSTrunks NE with the specified name is added as a map symbol under the grouped SSTrunks map symbol in the Network Elements topology panel. It is also added to the SSTrunks topology under the Network Elements topology node in the Module tree.

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding a USP NE using Web Client

Application

Use this procedure to add the USP NE to the IEMS topology using Web Client.

Universal Signaling Points can be managed using IEMS by adding them to the IEMS topology.

For details to configure SNMP-based devices that are managed by IEMS to send SNMP traps to the IEMS virtual IP address, see "Configuring traps for SNMP-based devices" (page 368).

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 **Admin** tab in the Web Client.
3	Select the **Add EMS/NE** node under the Network Admin tree to invoke the Add EMS/NE page in the right-side frame.
4	Enter the values for the Host Name/IP Address and Time Zone fields.
5	Select **NE** from the Type list box.
6	Select the mode of USP NE from the Mode list box (**Simplex** or **Duplex**). If you select **Duplex** from the Mode list box, you have to enter the inactive agent IP address in the In-Active Agent field.
7	Select **USP** from the Device Type list box.
8	Select the version of the device from the Device Version list box.
9	Enter the client server IP in the Client Server IP field.
10	Enter the inactive agent IP address in the Unit1 IP Address field.
11	Select the **Fault Interface** from the vertical tab. When adding a USP NE to the IEMS inventory the SNMP attributes (refer to step 12 to step 16) must align with the configuration of the USP network element. In addition, the manager IP address in the USP must be configured to forward its SNMP traps to the IEMS

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Server application (the IEMS Virtual IP address). The configuration of the SNMP attributes in the USP are described in the *USP Administration and Security guide*, NN10159-611 and the *USP Compact Administration and Security guide*, NN10160-611.

12 Enter the port value "161" (in which the NE agent communicates with IEMS) in the Port field.

13 Select the **SNMP** version from the Version list box.

The SNMP version must align with the version configured in the USP Network Element. The default SNMP version in the USP is V3.

If the SNMP version is	Do
v3	follow step 14 to step 15 and proceed to step 17
v2	proceed to step 16

14 Retain the value **NoAuthNoPriv** for the Security Level list box.

15 Enter the value for the User name field as specified in *USP Administration and Security guide*, NN10159-61.

The value for the Context name field must be left blank.

16 Enter the community string in the Community field.

17 Select the **Standby Fault Interface** from the vertical tab.

18 Repeat step 12 to step 16.

19 Select the **Performance Interface** from the vertical tab.

20 Type the user name for FTP PULL in the User ID field.

21 Type the password in the Password field.

22 Click the **Add EMS/NE** button to add the USP NE.

*Once the USP NE is added, the "Successfully added to the database" message is displayed. The USP NE with the specified name is added as a map symbol under the grouped USP map symbol in the Network Elements topology panel. It is also added to the **USP** topology under the Network Elements topology node in the IEMS tree.*

Only the active USP unit object provides an interface to determine the fault state of the USP. The inactive USP unit object status is in unknown state (map symbol has gray background color). The IEMS dynamically detects when the USP unit has been swacted. When this occurs, it initiates alarm resync with the newly active USP unit

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

and updates the state of the USP unit objects in the IEMS Client to reflect this change in activity. When this occurs the previous active unit object map is changed to unknown state, and the new active unit is updated to reflect the highest alarm state of the USP device. For the color mapping of various object status, refer to the "Significance of map symbol background color" (page 230) table of ""Updating status of objects manually" (page 230)".

You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using topology operations in Web Client

This section includes procedures that describe how to use operations in the topology GUIs of IEMS Web Client.

Copyright © 2006, Nortel Networks

Editing and viewing object properties using Web Client

Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

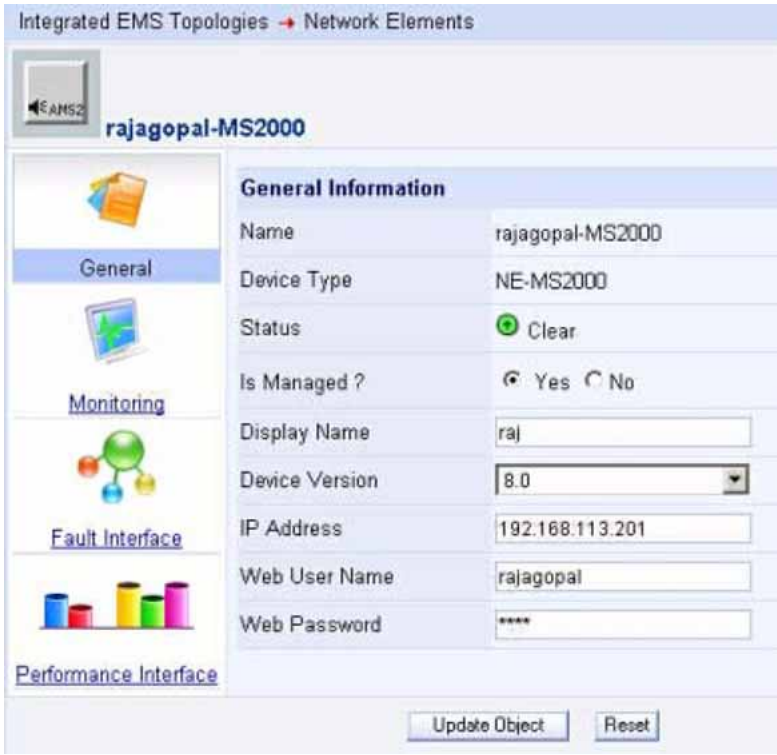
Prerequisites

There are no prerequisites for this procedure.

Action

Step	Action
	At the IEMS workstation
1	Launch the IEMS Web Client. Refer to procedure "Launching the IEMS Web Client" in *IEMS Overview*, NN10329-111.
2	Select the Integrated EMS Topologies tab.
3	Navigate to the required topology node in the IEMS Topologies tree.
4	Click the map symbol label to open the General Information window. *A window similar to the following figure opens. The object properties displayed can differ for each component.*

Copyright © 2006, Nortel Networks
Nortel Networks Confidential



5 If necessary, select each vertical tab and modify the object properties listed in the following table.

Managed object properties in Web Client

Field	Description
General	
Name	Displays the unique object name of the managed object
Device Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
Is Managed?	Indicates whether the object is managed or unmanaged
Display Name	Displays the name or label displayed in map symbol
Device Version	Select the version of the device from the drop-down list
IP Address	Modify the IP address of the object
Web User name	Enter your web user name
Web Password	Enter your web password

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Field	Description
Monitoring	
Last Status Update Time	Displays the time when the status of the managed object last changed
Last Status Change Time	Displays the time when the status of the managed object last changed
Status Polling Interval (secs)	Modify the Poll Interval for status updates
Fault Interface	
If the details are present for the selected object, the details can be modified.	
Performance Interface	
If the details are present for the selected object, the details can be modified.	

6 Click the Update Object button to update the changes.

7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using other operations in the Web Client topology

Operations such as managing or unmanaging an object, deleting an object, and viewing related events or alarms can be done using Web Client. These operations are triggered through the menus launched from map symbol.

Managing or Unmanaging

Application

Use this procedure to unmanage or manage an object in the topology.

You can make IEMS server stop managing a particular object, by selecting the Unmanage menu item. This menu item can be found in the popup menu that appears when you click the arrow symbol in the map symbol.

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 required topology node in the Module tree (IEMS Topologies tree) in which the required map symbol is shown.
3	Click the arrow of the required map symbol in the topology to invoke the popup menu.
4	Select the **Object -->Unmanage** menu command. You have completed this procedure.

—End—

To manage an object which is in unmanaged state, follow step 1 to step 3 and select the **Object-->Manage** menu command.

Deleting object and traces

Application

Use this procedure to delete an object and traces from topology using the Web Client.

An object in the topology can be deleted to remove it from topology.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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 required topology node in the Module tree in which the required map symbol is shown.
3	Click the arrow of the map symbol (that needs to be removed) in the topology to invoke the popup menu and select **<Object type name>-->Delete Object and Traces** menu item. You have completed this procedure.
	—End—

Viewing related events

Application

Use this procedure to view events associated with an object in topology.

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 required topology node in the Module tree in which the required map symbol is shown.
3	Click the arrow in the map symbol of the topology to invoke the popup menu.
4	Select **Object-->View Events** menu command. *The related events of the object in the Events page are listed.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Viewing related alarms

Application

Use this procedure to view the alarms associated with an object in topology

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 required topology node in the Module tree in which the required map symbol is shown.
3	Click the arrow of the map symbol in the topology to invoke the popup menu and select *Object-->Alarms* menu command. *The related alarms of the object in the Alarms page are listed.* You have completed this procedure.
	—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Working with the inventory in Web Client

The inventory maintains the properties of all the managed objects managed in a network. These managed objects and their associated properties are listed in the Inventory view. The information is available in a table format which is called List View.

Copyright © 2006, Nortel Networks

Viewing managed object details

Application

Use this procedure to view the managed object details in IEMS Inventory.

The details of a managed object (such as type, status, managed or unmanaged, and display name) can be viewed and some of the properties can be modified.

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 **Inventory** tab in Web Client.
3	Select the required node in the Module tree (Inventory tree).
4	Click the required managed object name link under the Name column. *The details page of the corresponding managed object is launched.*
5	Modify the properties in the corresponding horizontal tabs if required. For details, see "Editing and viewing object properties using Web Client" (page 352).
6	Click the **Update** button to update the changes. You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Navigating the inventory view

Application

Use this procedure to do the following:

- sort the inventory view
- customize the number managed objects displayed on each page
- browse the inventory view
- show or hide the columns

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 **Inventory** tab in the Web Client.
3	Select the required node in the Module tree (Inventory tree). The Module tree contains the following nodes: • Complete View • EMS • Platform • Application • NE Clicking each node in the Module tree displays its corresponding Managed Object details.
4	Select your next step.

If you want to	Do
browse the inventory view	Use the First, Previous, Next and Last navigator buttons that are located below the module menus

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If you want to	Do
customize managed objects for each page	Select the required page count from the list box to select the entries per page (below the module menus). The default is 50 managed objects per page.
show or hide the columns	See Customizing the Columns in "Navigating Events" in *IEMS Fault Management*, NN10334-911
sort events	Click the column order to sort the column. If the arrow in the column header is pointing upwards, the column is sorted in ascending order; if the arrow is pointing downwards, the column is sorted in descending order. By default, the network elements are displayed in the order of their discovery and in descending order.

5 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Searching for objects in the inventory view

Application

Use this procedure to search for objects in the inventory view.

The Search option in Web Client facilitates searching for managed objects. The search operation is performed on the entire database and is not restricted to the displayed page. You can search for a required managed object based on a general condition or a unique criterion.

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 **Inventory** tab in Web Client.
3	Select the required node in the Module tree (Inventory tree).
4	Click the **Search** menu item in Module Menu below the Module tab. You have completed this procedure.
	—End—

The procedure to search for events in Inventory is found in "Searching Events" in *IEMS Fault Management*, NN10334-911.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Adding, modifying, or removing an inventory view

Application

Use this procedure to add, modify, and remove inventory views for objects listed in the inventory. The views can be used to search for a subset of data that satisfies a given criteria and to filter and display the required data.

By default, the Inventory module has default types of views such as Complete View, EMS, Platform, Application, and NE. You can create new views under these default views.

Example

You can create a new view named MajorEMS under **EMS** inventory node, which shows only managed objects that are in Major status. Within this MajorEMS view, you can create more views such as M1 or M2. M1 can have a different set of criteria, such as only NTSTD enabled managed objects in that particular network. Deleting MajorEMS deletes its child views (M1, M2) as well.

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 **Inventory** tab in Web Client.
3	Select the required node in the Module tree (Inventory tree).
4	Select your next step.

If you want to	Do
add a view	step 5
modify a view	step 15
remove a view	step 19

5	Click **Add Child View** menu item in the Module Menus area. *The Add Child View page is launched.*
6	Enter the child view name in the Child view name field (mandatory).
7	Select the **Match any of the Following** option if you want to perform a search operation that satisfies any of the matching criteria that you

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

specify. If you need all the matching criteria to be satisfied, select **Match all the Following**.

8 Select the property based on the view you need to create. For description of the properties, refer to "Custom View for Events: Matching Criteria" in *IEMS Fault Management*, NN10334-911.

If you have selected property related to date or time, click the **Date Input Helper** button to open the Date Input Helper popup. The current month, year, date, and time is displayed. Select the required date and time on which you need the view criteria to be based and click the **Apply** button.

9 Select the condition that you need to restrict your view.

10 Enter the exact information in the Value field for which you need to create the view.

11 Click the **More** button and repeat step 8 to step 10 to add more criteria. The Fewer option can be used to remove any criteria.

12 Use the **Preview Results** button for a preview of the required view.

13 Click the **Add Child View** button to add the child view with the criterion specified.

14 Go to step 21.

15 Click **Edit View Criteria** menu item in the Module Menus area.

The Edit Inventory View Criteria page is launched.

16 Modify the child view name in the Child view name field (mandatory).

17 Follow step 7 to step 13 to modify the criteria.

18 Go to step 21.

19 Click **Remove View** menu item in the Module Menus area.

A dialog is launched confirming the removal of inventory view.

20 Click the **Yes** button to remove the selected inventory view.

21 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Using other operations in the inventory view

Application

Use this procedure to do the following in the inventory view of Web Client:

- manage or unmanage individual or multiple objects
- view related events or alarms for selected or multiple objects
- delete objects
- print the inventory view

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 **Inventory** tab in Web Client.

3 Select the required node in the Module tree (Inventory tree).

4 Select your next step.

If you want to	Do
print the inventory view	step 8
perform other operations	step 5

5 Click the >> icon next to the Name of the object in the Inventory table to display a popup menu.

6 Select your next step.

If you want to	Do
manage an object separately	Select the Object-->Manage menu item
manage multiple objects	Select the check boxes for the objects in the Inventory table that you want to be managed. Select the Manage item from Operations list box.
unmanage an object separately	Select the Object-->Unmanage menu item

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

If you want to	Do
Delete an object	Select the <object specific menu>-->Delete Object and Traces menu item
Delete multiple objects	Select the check boxes for the objects in the Inventory table that you want to remove. Select the Delete Objects item from the Operations list box.
view events associated with an object	Select the Objects-->View Events menu item
view events associated to multiple objects	Select the check boxes for the objects in the Inventory table for which associated events are listed. Select the View Events item from Events & Alarms list box.
view alarms related to an object	Select the Objects-->View Alarms menu item
view alarms associated to multiple objects	Select the check boxes for the objects in the Inventory table for which associated alarms are listed. Select the View Alarms item from Events & Alarms list box.

7 Go to step 10.

8 To print the inventory table, click the **Print Version** menu item.

9 Click the **Print** button.

10 You have completed this procedure.

—End—

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Configuring traps for SNMP-based devices

SNMP-based devices that are managed by IEMS need to be configured to send their SNMP traps to the IEMS virtual IP address. By default, the IEMS server is listening for these incoming SNMP traps on port 162.

The default IEMS trap listen port is defined in the opt/nortel/iems/current/conf/trapport.conf file on the IEMS server.

The IEMS virtual IP address can be queried by entering the following command on the IEMS server:

```
getpip.ksh IEMS
```


Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Description of SNMP attributes

This section gives the description of SNMP related attributes or terms used in this guide. This section also indicates whether the attributes are mandatory (require user input).

Port
The port in which the managed object (Element Manager, platform, EMS application, or NE) agent is running. This field is mandatory while providing the details for an SNMP v1, v2c, or v3 enabled managed object in the Fault Interface screen of the Add Object wizard (where Object can be EMS/NE, EMS Platform, or NE).

Community
The community to be used while processing the SNMP GET request. The default read community is "public". This field is mandatory while providing the details for an SNMP v1 or v2c enabled managed object in the Fault Interface screen of the Add Object wizard (where Object can be EMS/NE, EMS Platform, or NE).

Version
The version of the SNMP agent. The values can be v1, v2c, or v3. For SNMP version v1, the following fields are mandatory:

- Port
- Community

For SNMP version v2c, the following fields are mandatory:

- Port
- Community
- Write Community (if any)

For SNMP version v3, the following fields are mandatory:

- Port
- Security level
- User Name

Write Community
The community to be used while processing the SNMP SET request. The default write community is "public". This field is mandatory while providing the details for an SNMP v1 or v2c enabled managed object in the Fault Interface screen of the Add Object wizard.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Security level
The SNMPv3 Agent supports the following set of security levels:

- **NoAuthNoPriv:** Communication without authentication and privacy. The following fields require input for this security level:
  - User Name
  - Context Name (if any)
- **AuthNoPriv:** Communication with authentication and without privacy. The protocols used for authentication are MD5 and SHA (Secure Hash Algorithm). The following fields require input for this security level:
  - User Name
  - Context Name
  - Authentication Protocol
- **AuthPriv:** Communication with authentication and privacy. The following fields require input for this security level:
  - User Name
  - Context Name
  - Authentication Protocol
  - Privacy Password

User Name
The security name of the user on whose behalf the operations are to be carried out in the SNMP v3 agent.

Context Name
The name of the SNMP context.

Authentication Protocol
The authentication protocol to be used for authenticating the user. Either MD5 or SHA protocol is used.

Privacy Protocol
The type of privacy protocol to be used for encryption. The DES protocol is used in IEMS.

Privacy Password
The private key used for encryption. This is not required if NO_PRIV protocol is used.

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

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.

Copyright © 2006, Nortel Networks

Copyright © 2006, Nortel Networks
Nortel Networks Confidential

Carrier VoIP

IEMS Configuration

Copyright © 2006, Nortel Networks
All Rights Reserved.

Publication: NN10330-511
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.

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.