Version 03.01
NN10370-111
March 2005

Carrier Voice over IP System Management Console User Guide

NORTEL

Copyright © 2005 Nortel

Trademarks

Contents

About this guide

Overview

This guide provides administrators with instructions on using the System Management Console. The System Management Console is the interface used to configure, monitor, and manage the MCP component hardware and software.

Audience

This guide is intended for administrators using the System Management Console to manage the MCP system component hardware and software.

Text conventions

This guide uses the following text conventions:

bold text	Indicates a menu option, link, or command key you need to click. Examples: Click **Apply**
italic text	Indicates a variable name or document title Example: *CVoIP System Manager Basics*
<**ElementName**>	Indicates a configured element name in the config view. Example: <SESM_x>
separator >	Indicates a menu path Example: **Network Elements** > **Session Managers**

Acronyms

This guide uses the following acronyms:

GUI	Graphical User Interface
IP	Internet Protocol
IPCM	IP Client Manager
MB	megabyte
MCS	Multimedia Communications Server
MCP	Multimedia Communications Portfolio
OAM	Operations, Administration, Maintenance
OM	Operational Measurement
PC	Personal Computer
PRI	Primary Rate Interface
RAM	Random Access Memory
RTP	Real-Time Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
UFTP	UNIStim File Transfer Protocol
URL	Universal Resource Locator (internet address)
XML	EXtensible Markup Language

Related publications

The System Management Console interacts with the MCS system hardware and software components via the System Manager. The tasks described in this guide are generic and do not include specific information for any one component.

Administrators should refer to the following guides for specific details on the management of the related hardware and software components.

Table 1 Related publications

Document	Part No.
CVoIP RTP Media Portal Basics	NN10367-111
CVoIP Database Manager Basics	NN10368-111
CVoIP System Manager Basics	NN10369-111

How to get help

For service issues, please contact your local support or Information Services team.

System Management Console - getting started

Topics in this chapter

System Management Console overview

The System Management Console is a Java-based GUI used by administrators to interact with the System Manager. The System Manager acts as an element manager for the network elements of the MCS software and hardware. The System Management Console runs on a PC using supported Windows operating systems and is used for the following:

- administering system, database, and network elements
- deploying and configuring system sites, servers, network elements, and network element services
- monitoring system using alarms, logs, and performance measurements
- managing collection of operations, administration, and maintenance information

The System Managment Console uses Java Web Start technology and is launched from a web browser.

System Management Console installation

The System Management Console is installed by directing the web browser to the IP address of the System Manager and a port number of 12120, such as http://47.47.47.47:12120. The System Manager needs to be deployed and operational before administrators can install or use the System Management Console.

See the following topics for more information:

- System requirements
- Installing the System Management Console for the first time
- Uninstalling the System Management Console
- Updating the System Management Console

System requirements

Nortel recommends that the workstation meet the following hardware requirements:

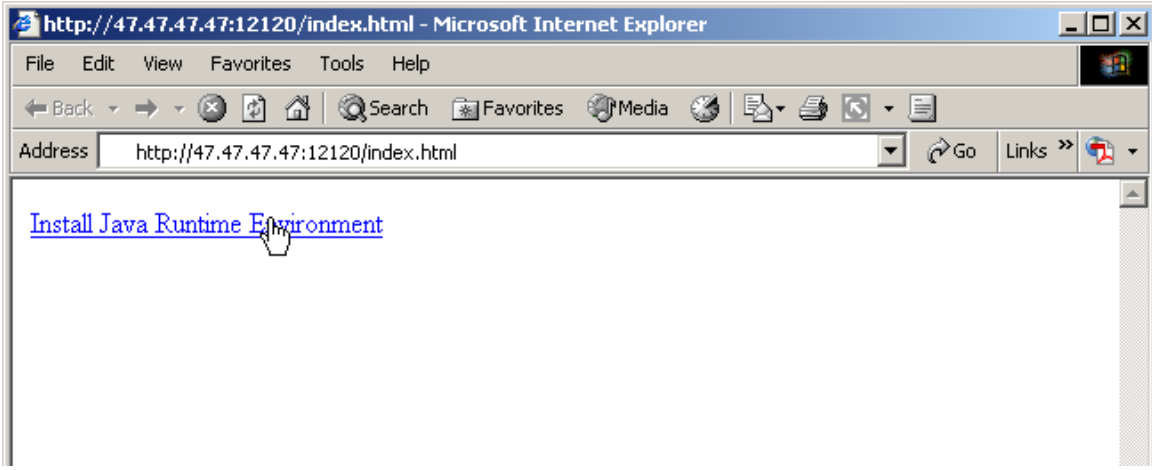
Category	Minimum requirements	Recommended requirements
Processor	600 MHz Pentium-class or equivalent processor	1.0 GHz (or higher) Pentium-class or equivalent processor
Free RAM	64 MB of RAM (This requirement is in addition to the memory requirements of the operating system and other concurrent applications.)	64 MB of RAM (This requirement is in addition to the memory requirements of the operating system and other concurrent applications.)
Free hard disk drive space	50 MB for the Java Runtime Environment and 15 MB for each MCS system that is managed.	50 MB for the Java Runtime Environment and 15 MB for each MCS system that is managed.
Mouse	Required	Required
Video graphics card	640x480 @8bpp [256 colors] VGA	800x600 @16bpp [65,536 colors] VGA or better
Sound card	not applicable	not applicable
Operating systems	Microsoft* Windows* 98(SE)/ME/2000/XP/ Microsoft Windows NT* 4.x with Service Pack 5 (SP5)	Microsoft Windows 2000/XP/98(SE) Microsoft Windows NT 4.x with Service Pack 5 (SP5)
Network connectivity	56 Kbps modem	10Base-T or other fast network connection (DSL, Cable, LAN, etc.)

Category	Minimum requirements	Recommended requirements
Internet browsers	Netscape* Communicator 7.0 Microsoft Internet Explorer* 6.0	Netscape Communicator 7.1 or greater Microsoft Internet Explorer 6.0 or greater
Cookies	Enabled	Enabled
Javascript	Enabled	Enabled

Installing the System Management Console for the first time

The System Management Console is installed with Java Web Start technology. A web browser with connectivity to the System Manager is needed.

1 On the administrator's workstation, open a web browser, enter the IP address of the active System Manager and specify port 12120. For example, enter http://47.47.47.47:12120:

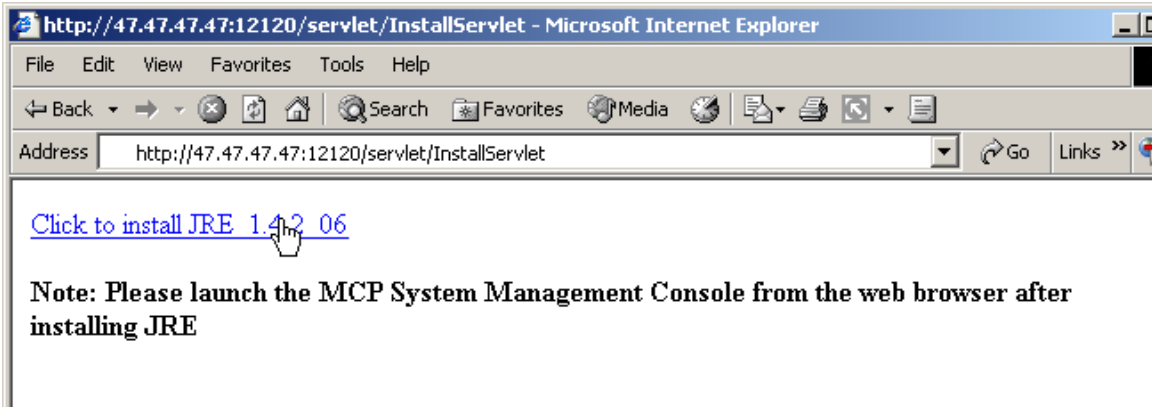


If Java Web Start is not installed on the local workstation, the Install Java Runtime Environment link is active.

2 Click the Install Java Runtime Environment URL to install the JRE needed for the System Management Console.

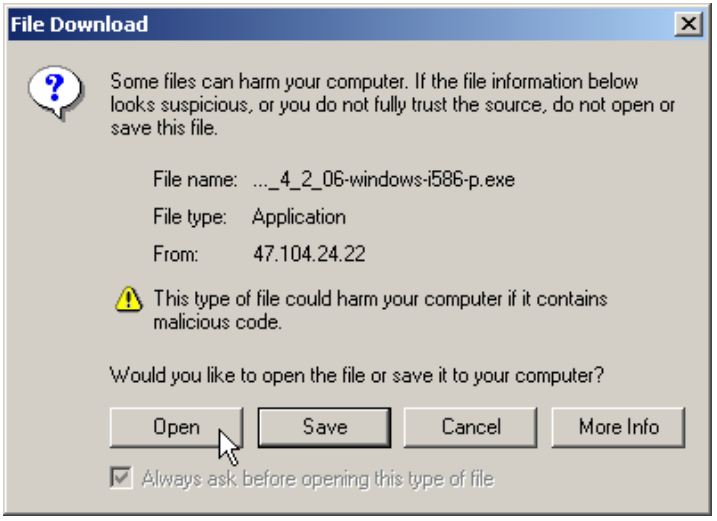
The page refreshes and the web server on the System Manager provides a URL to the correct JRE.

3 Click the URL:



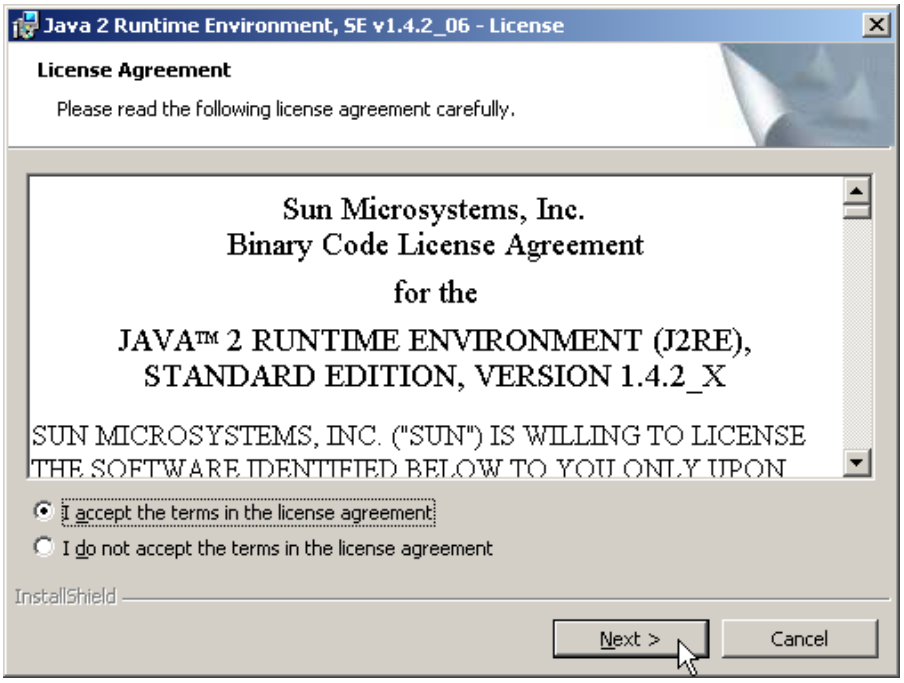
A File Download dialog window opens.

4 Click **Open** on the File Download dialog window:



The correct JRE for the System Management Console is downloaded from the System Manager and the installation starts. The license agreement window opens.

5 Select the radio button for "I accept the terms in the license agreement" and then click **Next**:



The Setup type dialog box opens.

6 Select the **Typical** radio button and click **Next**.

The Progress dialog box opens and files are copied to the local workstation. After the files are copied, the InstallShield Wizard Completed window opens.

7 Cick **Finish** on the InstallShield Wizard Completed window.

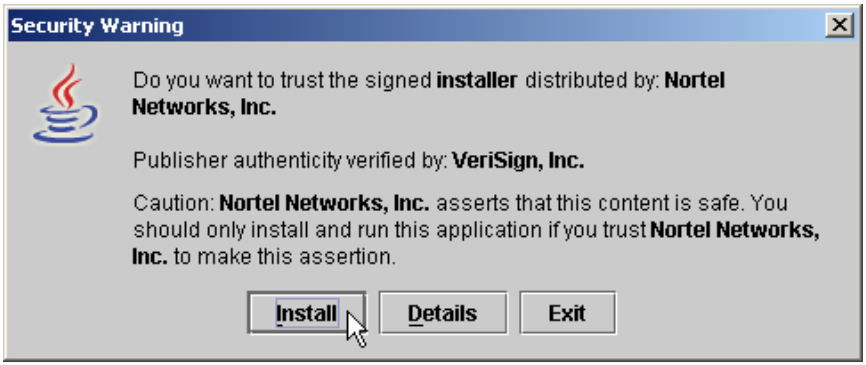
8 At the web browser, go back to the address specified in step 1.

Since the JRE is installed, the link changes to "Launch MCP System Management Console."

9 Click the Launch MCP System Management Console URL.

Java starts, and the files for the System Management Console are transferred from the System Manager to the local worstation. A Security Warning dialog window opens.

10 Click **Install** on the Security Warning dialog window:

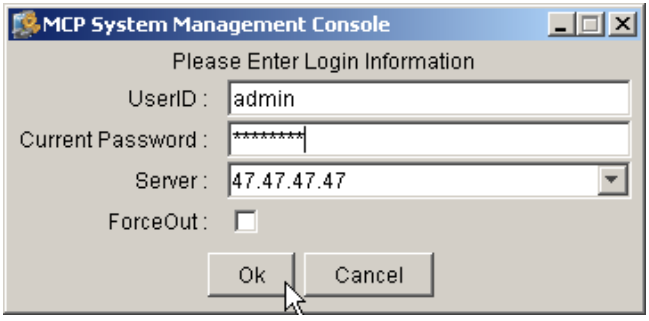


Another Security Warning dialog window opens and requests confirmation to trust the signed application.

11 Click **Start** to trust and install the System Management Console application.

The MCP System Managment Console login window opens.

12 Enter a UserID and Current Password, then click **Ok** to start the System Management Console.



If a message of the day text file (motd.txt) file has been set on the System Manager, then the message of the day is displayed. Click Ok.

The MCS System Management Console splash screen appears, closes, and the System Management Console application opens.

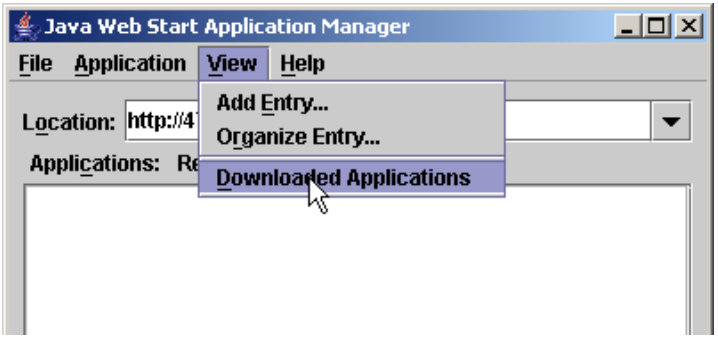
Uninstalling the System Management Console

It is not necessary to uninstall the System Managment Console to update it. When an updated software load is deployed and started on the System Manager, the updated System Management Console is automatically transferred and started at the next log in. However, if preferred, use the following procedure to uninstall the System Management Console:

1 Select **Start** > **Programs** > **Java Web Start** > **Java Web Start** on the workstation.

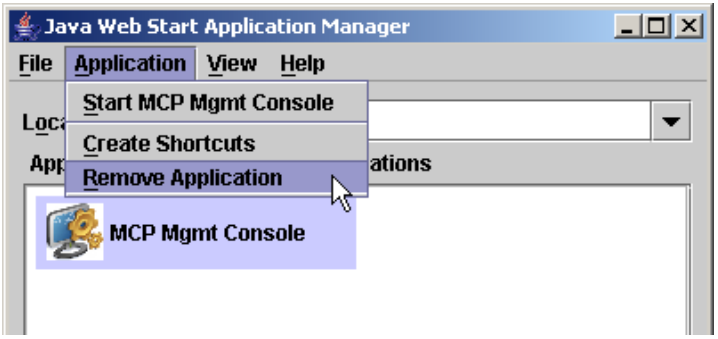
The Java Web Start Application Manager window opens.

2 Select **View** > **Downloaded Applications** from the menu bar:



The MCP Mgmt Console icon appears in the Applications area.

3 Select the MCP Mgmt Console application to remove and then select **Application** > **Remove Application**:



The MCP Mgmt Console is removed.

Updating the System Management Console

After deploying software upgrades on the System Manager and launching the existing version of the System Management Console, the web server on the System Manager and Java Web Start installed on the local workstation automatically download the updated files for the System Management Console and start it. If the System Management Console requires a version of the Java Runtime Environment that is not installed, the correct Java Runtime Environment is automatically downloaded the next time the System Management Console is started.

Java Web Start always starts the version of the System Management Console that is associated with a particular System Manager. If the workstation is used to manage more than one MCS system, then the correct version of the System Management Console software is installed for each MCS system.

A software update to the System Management Console is indicated by a delayed start of the application as the updated software is transferred from the System Manager to the local workstation. The version of the System Management Console is also available by selecting **Help** > **About** from the menu bar

Usernames and passwords required for System Management Console are assigned by an administrator using the System Managment Console. SecurityService privileges are required to add and configure other administrators.

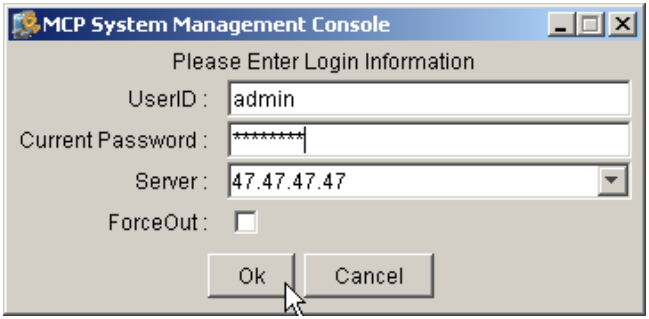
Logging in to the System Management Console

The System Management Console allows only one login for each administrator account at a time. For example, two logins for an account "dbadmin" are not allowed. In this case, a second account such as "dbadmin1" would need to be created for the adminstrator who wants two simultaneous logins.

1. Open a web browser, enter the IP address of the System Manager, and specify port 12120. For example, http:/47.47.47.47:12120.

   A web page opens with a "Launch MCP System Management Console" URL.

2 Click the URL and the MCP System Management Console window opens.



Note: Enable the ForceOut checkbox if the log in window reappears and indicates "Login failed -- User session exists already." This situation can occur if connectivity between the System Manager and the local workstaton is lost while an open System Managment Console session is active.

The ForceOut option is also useful when an administrator doesn't log out of the System Management Console at one location and wants to log in from another location.

3 Click **Ok**.

The System Management Console opens with a successful connection.

4 To terminate a session, select **File** > **Logout** from the System Management Console menu bar.

The System Management Console closes and the session ends.

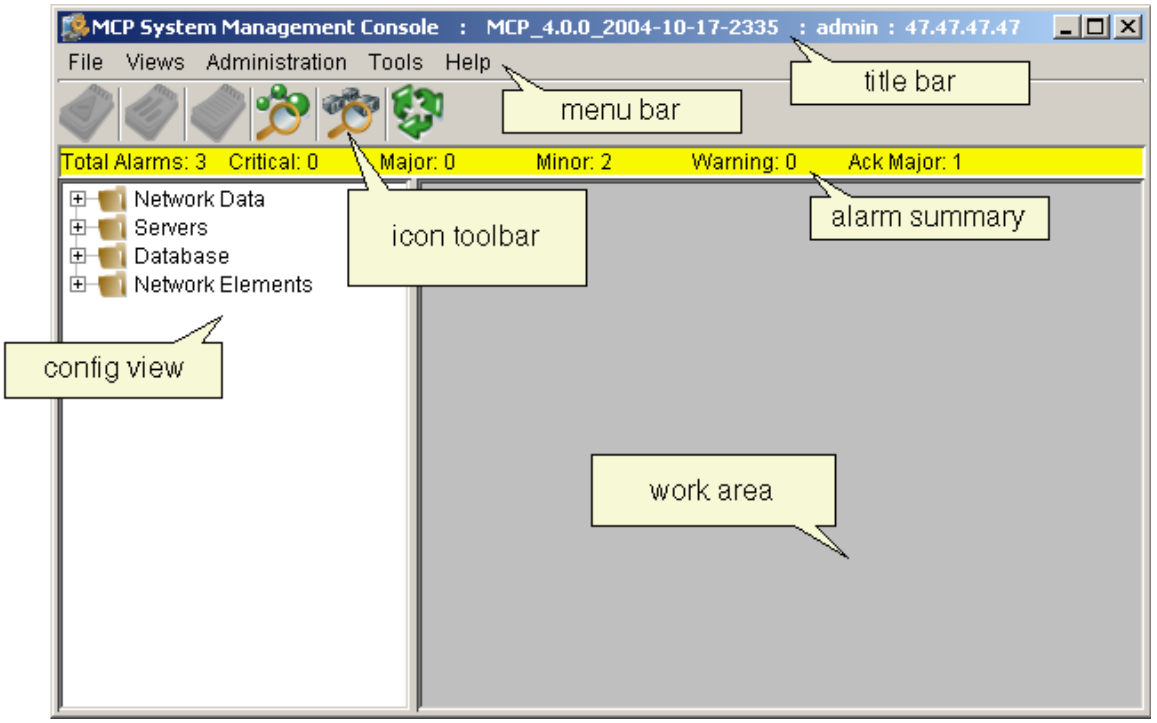
Navigating the System Management Console

Topics in this chapter

System Management Console layout

The System Management Console uses the familiar and easy to use Windows layout. Like other Windows applications, it consists of the title bar on the top, the menu bar, and an icon-based toolbar. Under those, an alarm summary indicates the status of the network elements in the MCS system. Below the alarm summary are the config view in the left panel, and the work area in the right panel.

Figure 1 System Management Console



Title bar

The title bar indicates the following items:

- the application — MCP System Management Console
- the software version on the System Manager
- log in username
- IP address of the System Manager

Menu bar

The menu bar provides access to the physical and logical view windows, user administration, and database import and export. Menu options are discussed in this guide with the related procedures.

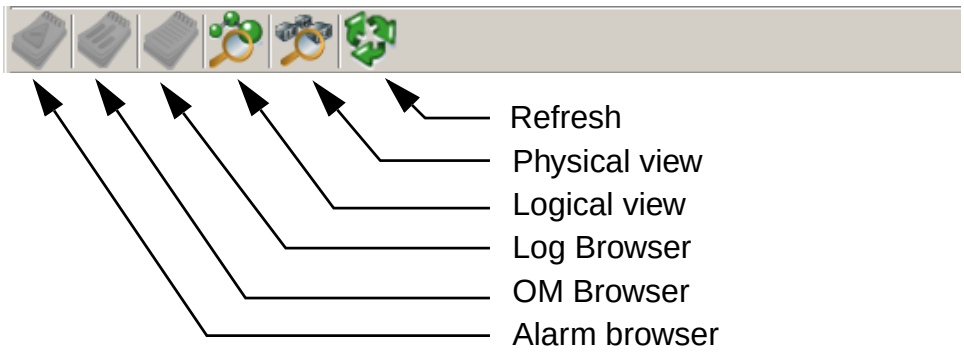
Figure 2 System Management Console menu bar

Icon toolbar

The icons on the toolbar represent menu options frequently used by administrators. Not all toolbar options are available for every component or server. Grayed out icons are unavailable for the element selected in the config view.

The tasks associated with the toolbar options are described in the relevant sections of this guide.

Figure 3 System Management Console icon toolbar



Alarm summary

The color of the alarm summary bar indicates the alarm status of managed and monitored MCS network elements.

The color shown is that of the most severe alarm generated by an MCS network element. The alarm color codes are:

- Green - no alarm or warning
- Yellow - minor alarm
- Orange - major alarm
- Red - critical alarm

In addition, the alarm summary indicates the total number of alarms, the number of critical, major, minor, and warning alarms. If any alarms have been acknowledged by administrators for investigation, then acknowledgement for that severity of alarm is also displayed.

For information on alarms, refer to *Fault Management: Alarm and Log reference*.

Config view

The config view is located on the left side of the System Managment Console.

Information is organized into four sections:

- Network Data — Information such as IP addresses, log report formats, OSS servers, and other data that doesn't change often but does get reused during other configuration tasks is defined here. Entering the data here avoids retyping, and typing errors, during other configuration tasks. License keys for activating features are also managed here.
- Servers — All the managed network elements in the MCS network are deployed on servers that are configured in this area. This area also provides access to server monitors that report hardware and operating system health.
- Databases — This folder contains software load and configuration so the System Manager can connect to the database as well as distibute database connection information to network elements that need database access.
- Network Elements — MCS network elements, managed and monitored, are configured here. Each network element type has a folder, and each configured network element has a subtending folder. Once a network element folder is selected, the Alarm Browser, OM Browser, and Log Browser icons become active for that network element. OAM&P such as load deployment; configuration parameters; om, log, and accounting record configuration; and network element maintenance such as start and stop are located here.

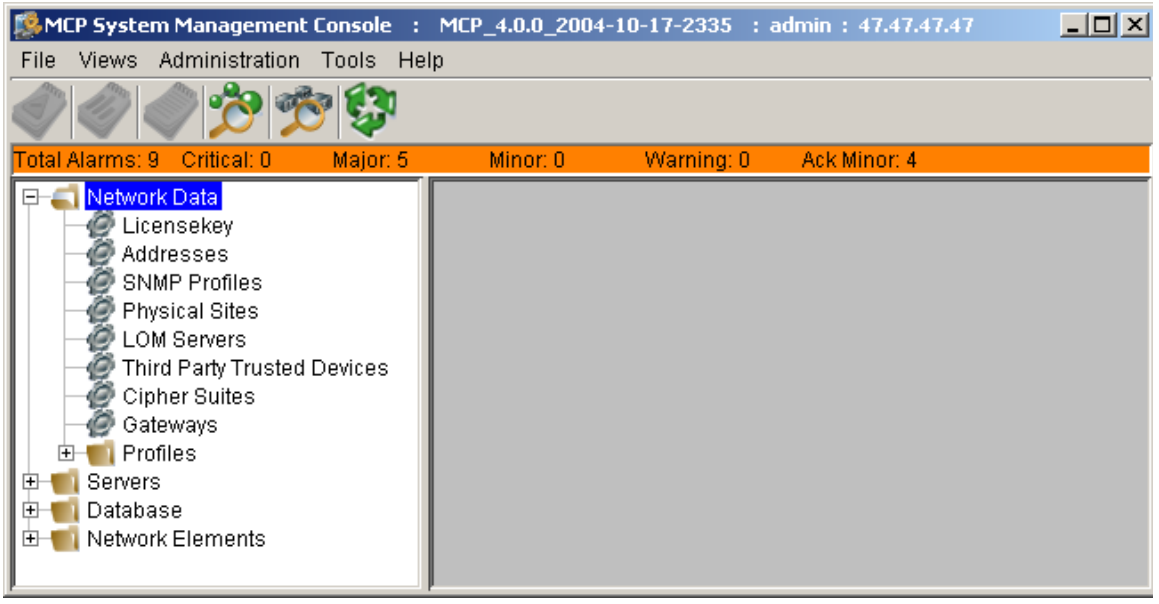
Work area

The work area is located to the right of the config view. It acts as a desktop for panels opened by navigating the config view. Panels can be moved, resized, or closed. Some config view nodes (**Network Data** and **Network Elements**) have no associated displays.

A description of the information displayed in the work area is discussed with the respective config view level in the subsequent chapters.

Network Data configuration and management

Topics are addressed in the order they appear on the System Management Console.



License key management

Updating and querying license keys requires an administrative role with LicenseKeyService privilege.

The following list provides a brief description of each tab displayed on the LicenseKey window.

- **Features** — This tab shows licenseable units which can be enabled or disabled and that also have a limit restricting their use.

- **Feature States** — This tab shows licenseable units which can only be enabled or disabled. They do not have limits associated with their use.
- **Version info** — This tab shows the version of the license key (this may differ from the software version during upgrade). It shows the date and time that the licensekey was generated as well as the id of the generator and the licensekey comments.
- **Licenseable Units** — This tab shows licenseable units which are always enabled and have a limit restricting their use.
- **Network Elements** — This tab shows the network elements that do not have ports or endpoints associated with them in the licensekey. The tab shows the number of these network elements that can be configured in the system as well as the type and number of configured network elements.
- **Network Elements with Ports** — This tab shows the network elements that have ports but not endpoints associated with them in the licensekey. The tab shows the number of these network elements that can be configured in the system and the number of ports that can be used. It also shows the current number of configured network elements of each type.
- **Network Elements with Ports & EndPoints** — This tab shows the network elements that have ports and endpoints associated with them in the licensekey. The tab shows the number of these network elements that can be configured in the system and the number of ports and endpoints that can be used. It also shows the current number of configured network elements of each type.

Updating a license key

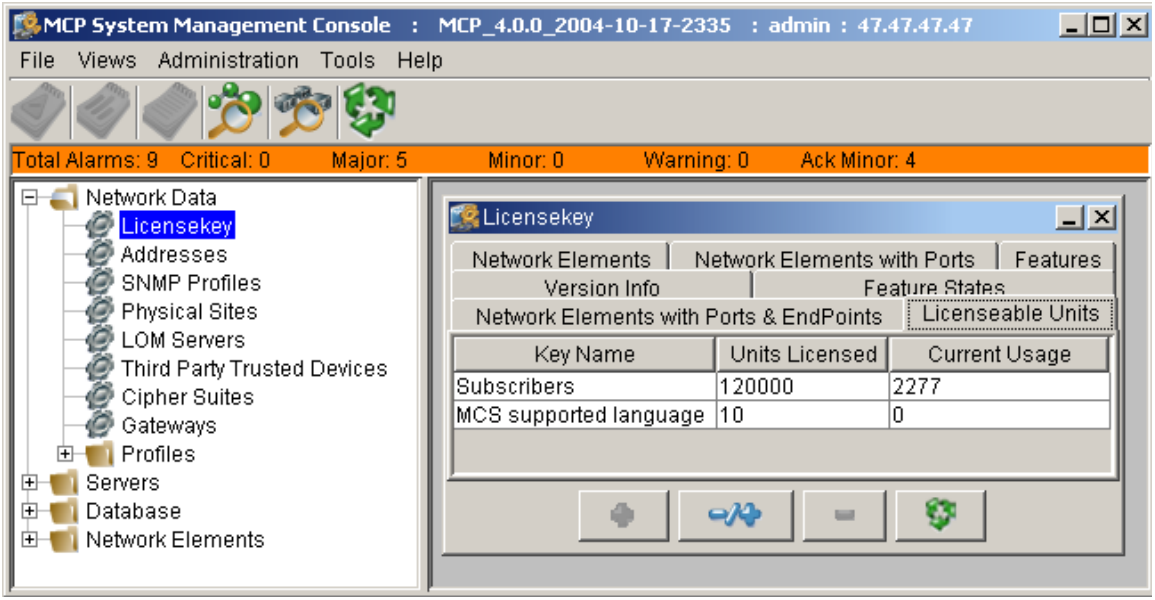
Updates can be performed for a current release and any subsequent maintenance releases only. New releases require a new license key.

Updates to a license key can only increase system capabilities. For example, licenses can be updated to allow capabilities for more subscribers, not fewer.

Administrators update license keys by selecting **Network Data** > **Licensekey** in the config view of the System Management Console. The License Key can be updated dynamically without any disruption of service. The update is rolled back if the License Key update procedure fails.

1 Select **Network Data** > **Licensekey** from the config view.

The Licensekey window opens in the work area.



2 Click the **Edit** button the Licensekey window.

The Select License key File dialog box opens.

3 Navigate to the license key file on the local workstation, select it, and click **Open**.

A confirmation message is displayed once the license key has been successfully saved into the database. If the update fails, the License Key update is rolled back.

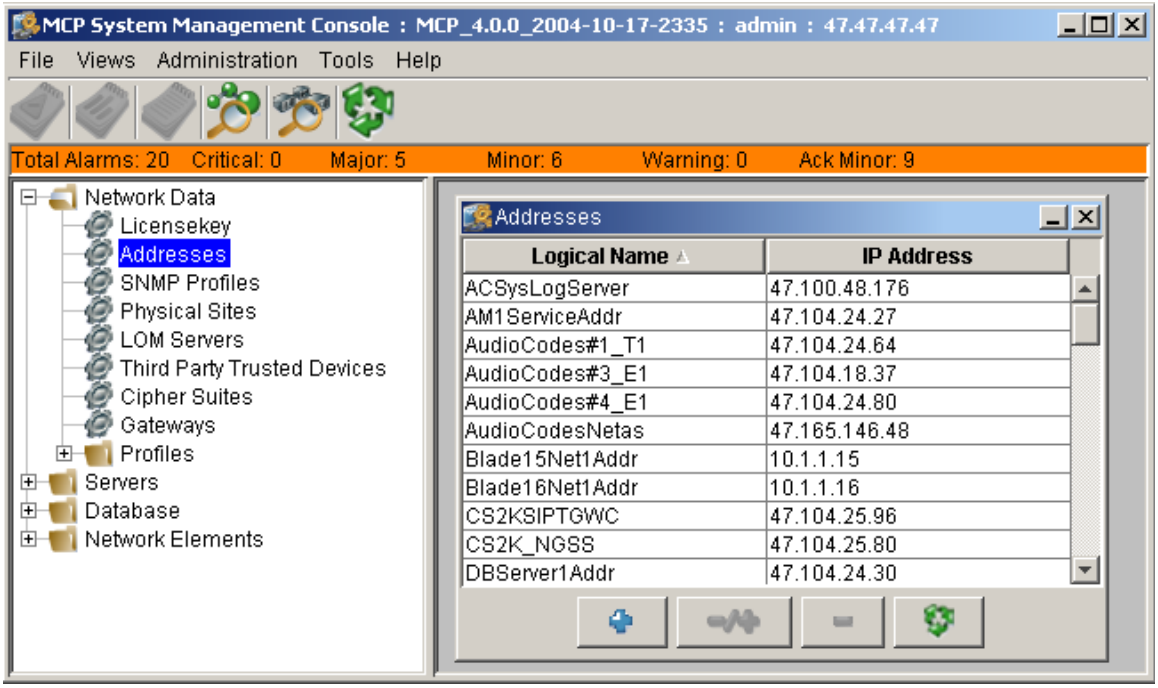
Querying a license key

Administrators query license keys by navigating the tabs on the Licensekey window. The licensed limits and current usage is displayed.

Addresses

To avoid configuration errors related to entering IP addresses inaccurately, all the IP addresses for all managed and monitored network elements are entered once, at the Addresses window.

To open the Addresses window, select **Network Data** > **Addresses** from the config view. All operations performed at the Addresses window require an administrative role with IPAddressService privileges.



Before a server can be added to the MCS network, the IP address the server will use must be added at the Addresses window and have a Logical Name associated with that IP Address. Addresses cannot be deleted if an LOM Server, Third Party Trusted Device, Gateway, OSS Server, or server that hosts an MCS network element is configured against the Logical Name. Addresses can be edited to another IP address, but services are interrupted.

Configuring an IP address

Addresses for servers and network elements are enterred once by following this procedure. Editing an entry and changing the IP Address will disrupt service for the network element and all services for the network elements deployed on the server.

1. Select **Network Data** > **Addresses** from the config view.

   The Addresses window opens the work area.

2. Click **Add** or select an entry and click **Edit**.

   The Address dialog box opens.

3. Enter the configuration data. Both fields, Logical Name and IP Address must be unique values. Click **Apply**.

   The Address dialog box closes and the Addresses window is updated.

Deleting an address

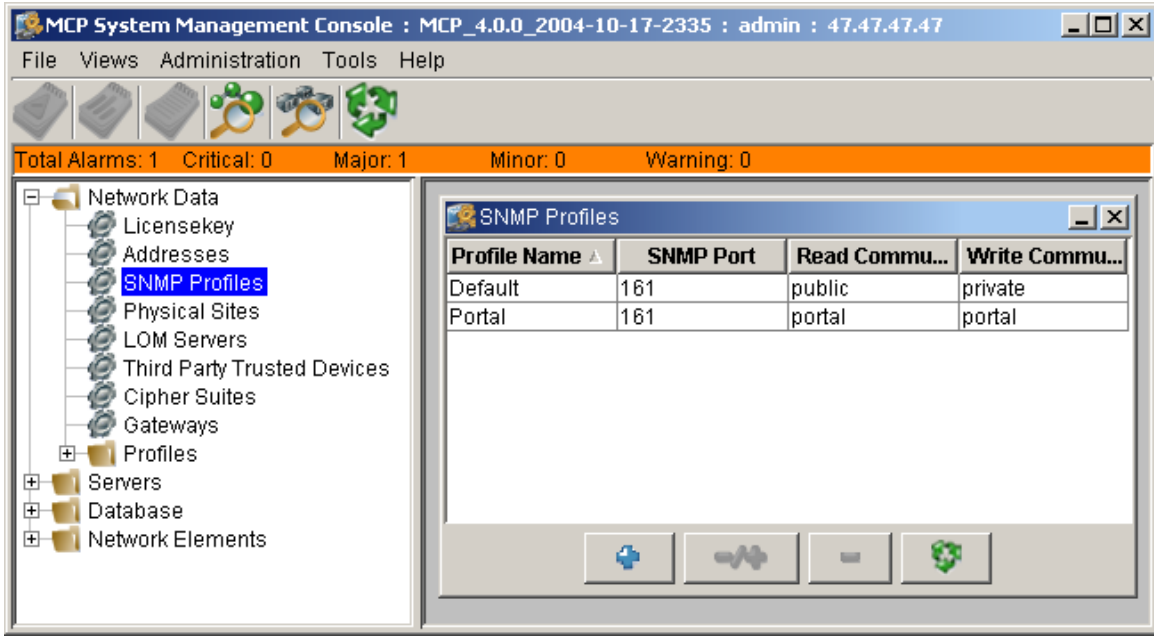
Before deleting an address, the network element or server that uses the IP Address must be deleted

1. Select an entry from the Addresses window and click **Delete**.

   A confirmation prompt opens. Click Yes to confirm the delete. The Addresses window is updated

SNMP Profiles

SNMP profiles are utilized by the System Manager to access (e.g. query) SNMP agents on network elements. SNMP Profiles are accessed and created by selecting **Network Data** > **SNMP Profiles** from the config view. All operations on SNMP profile configuration require an administrative role with SnmpProfileService privileges.



SNMP profiles are created to configure consistent SNMP parameters that can be used by the System Manager for monitoring operating system and server hardware health of the managed and monitored MCS network elements.

A profile is created with a port number and read and write community strings to match SNMP deamon settings on a network element; 161, public, and private match the default settings for most operating systems. Once this profile is created and server configuration begins, this profile is associated with a server so that the server can be monitored by the System Manager.

Once an SNMP Profile is created, it cannot be editted. If administrators want to change the SNMP community string, or any other parameter, to increase security, perform the following steps:

- Configure a new SNMP profile as described in “Configuring an SNMP profile” on page 35.
- Assign the new SNMP profile to each server as described in “Configuring a server” on page 54.

To increase SNMP security, administrators can be assigned an administrative role that does not have SnmpProfileServices privilege.

Configuring an SNMP profile

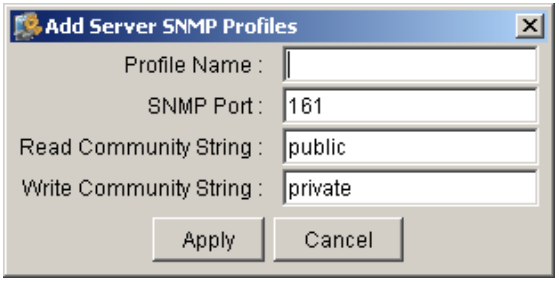
Use this procedure to create a new SNMP profile. Afterward, use the System Management Console to associate the new SNMP profile with the servers to use the profile.

1 Select **Network Data** > **SNMP Profiles** from the config view.

The SNMP Profiles window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The Server SNMP Profiles dialog box opens.



3 Enter the configuration data on the Server SNMP Profiles dialog box and click **Apply**.

The SNMP Profiles window is updated.

Deleting an SNMP profile

Before deleting an SNMP Profile, edit any servers that use the profile and configure the servers to use a different SNMP Profile.

1 Select an entry from the SNMP Profiles window and click **Delete**.

A confirmation prompt opens. Click OK to confirm the delete. The SNMP Profiles window is updated.

Physical Sites

Managing site information requires an administrative role with PhysicalSiteService privileges. When an administrator selects **Network Data** > **Physical Sites** in the config view, the work area displays a panel with the following site level information:

- Site Name — a name configured for this site by the administrator
- Zone — the Universal Transverse Mercator (UTM) zone for the site
- Easting — the UTM Easting coordinate for the site
- Northing — the UTM Northing coordinate for the site

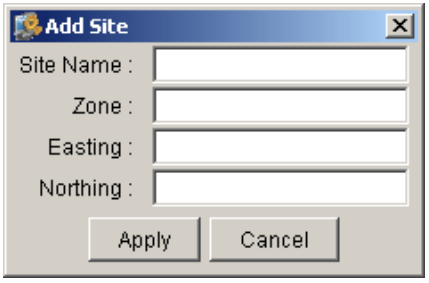
Configuring a site

1. Select **Network Data** > **Physical Sites** from the config view.

   The Physical Sites window opens in the work area.

2. Click **Add** or select an entry and click **Edit**.

   The Site dialog box appears.



3. Enter the configuration data and click **Apply**.

Field	Value	Description
Site Name	alphanumeric (1-20 characters)	A unique name identifying the site
Zone	alphanumeric (1-3 characters)	UTM zone location of this site

Easting	integer, 1 to 1 000 000	Easting of the site
Northing	integer, 1-7 digits	Northing of the site

The Physical Sites window in the work area is updated.

Deleting a site

Administrators must delete all the servers and network elements of the site before deleting the site itself.

1 Select the site from the Physical Sites window and click **Delete**.

A confirmation prompt opens. Click Yes to confirm the delete. The Physical Sites window is updated.

LOM Servers

Lights Out Management servers are used to recover servers that host MCS network elements. LOM servers are configured by selecting **Network Data** > **LOM Servers** in the config view. Provisioning an LOM Server requires an administrative role with LOMServerService privilege. Administrators that use the LOM Servers to power on, power off, or reset a server require ServerLOMCommandService privileges.

Configuring an LOM server

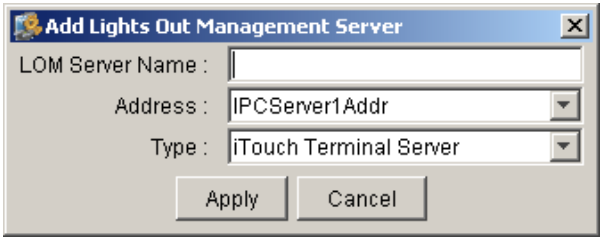
Before an LOM Server can be configured, the IP address of the server must be configured at the Addresses window.

1 Select **Network Data** > **LOM Servers** from the config view.

The LOM Servers window opens the work area.

2 Click **Add** or select an entry and click **Edit**.

The Lights Out Management Server dialog box opens.



3 Enter the configuration information and click **Apply**.

The dialog box closes and the LOM Servers window is updated. The new entry is used when configuring a server..

Deleting an LOM server

An LOM Server cannot be deleted if it is associated with a server that is configured in the Servers folder of the config view.

1 Select an entry from the LOM Servers window and click **Delete**.

A confirmation prompt opens. Click Yes to confirm the delete. The LOM Servers window is updated.

Third Party Trusted Devices

Operations on this data require an administrative role with TrustedNodeService privilege.

Configuring a third party trusted device

1 Select **Network Data** > **Third Party Trusted Devices** from the config view.

The Third Party Trusted Devices window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The Trusted Devices dialog box opens.

3 Enter the configuration data:

- Name - the name of the device such as MAS110
- DeviceAddress - use the pull down to select the address of the device
- Port - enter an integer, 0 to 65 534

Click **Apply**.

The dialog box closes and the Third Party Trusted Devices window is updated.

Deleting a third party trusted device

1 Select an entry on the Third Party Trusted Devices window and click **Delete**.

A confirmation prompt opens. Click Yes to confirm the delete. The Third Party Trusted Devices window is updated.

Cipher Suites

Cipher Suites are used to configure the type of encryption used for commuication between the System Manager and the MCS network elements. Operations on this data require an administrative role with CipherSuiteService privilege. Cipher suites are not added to the MCS system, they are enabled and disabled.

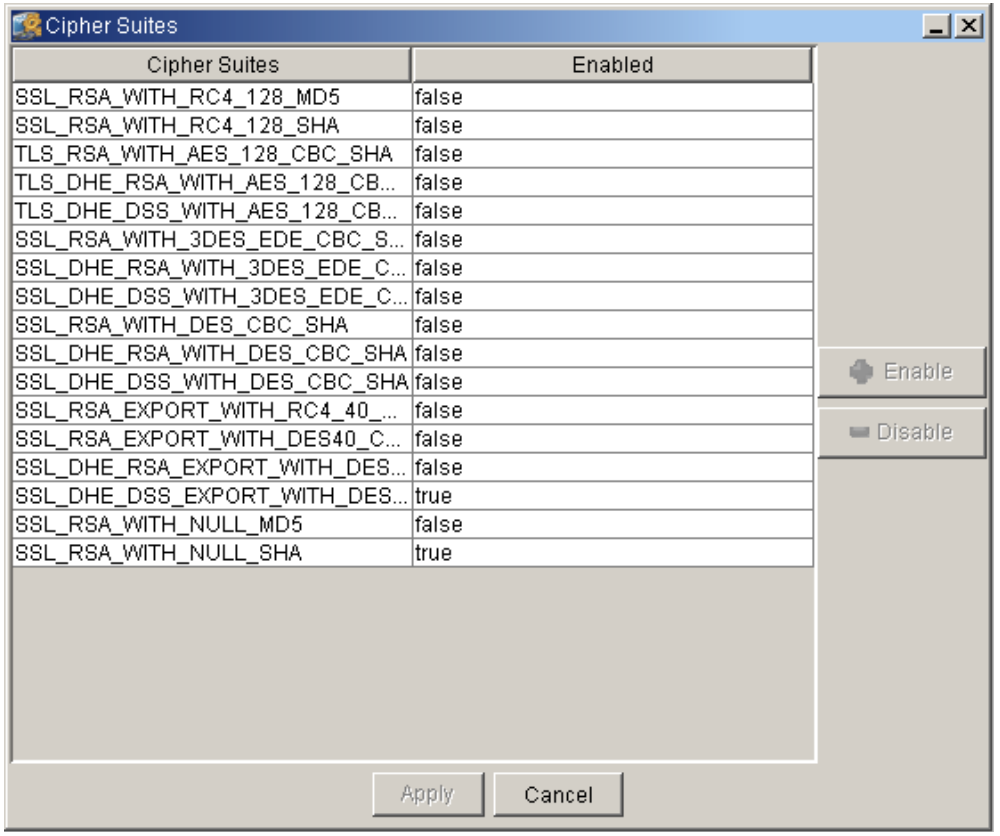
When a new list of cipher suites is applied to the network, all configuration streams, log streams, alarm streams, OM streams, and accounting streams between network elements are brought down and then brought up. They are then secured with the newly applied cipher suites. Restart of network element instances is not required. There are two cipher suites which can not be disabled. These two cipher suites ensure that network element commuication can always continue over a common negotiated cipher suite.

The normal alarms associated with communication for the particular subsystem will be shown and logged momentarily while the connections are reestablished.

Configuring cipher suite usage

1 Select **Network Data** > **Cipher Suites** from the config view.

The Cipher Suites window opens the work area.



2 Select an entry for the cipher suite to enable or disable and click **Enable** or **Disable**.

The Apply button becomes active.

3 Click **Apply**.

The Cipher Suites window is updated.

Gateways

After configuring gateways here, RTP Media Portal devices can associate one of these gateways as its default gateway. Operations on this data require an administrative role with GatewayService privilege.

Configuring a gateway

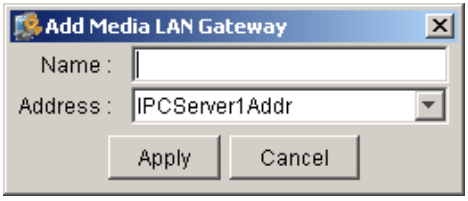
Before adding or editing a gateway entry, configure an IP Address at the Addresses window. Editing an IP Address for a gateway will disrupt service.

1 Select **Network Data** > **Gateways** from the config view.

The Gateways window opens the work area.

2 Click **Add** or select an entry and click **Edit**.

The Media LAN Gateway dialog box opens.



3 Enter the configuration data and click **Apply**.

The dialog box closes and the Gateways window is updated.

Deleting a gateway

Deleting a gateway will disrupt service. Contact Nortel support personnel before deleting a gateway.

1 Select an entry from the Gateways window and click **Delete**.

A confirmation prompt opens. Click Yes to confirm the delete. The Gateways window is updated.

Profiles

The Profiles folder of the config view organizes OSS (Operations Support System) information and log, OM (Operational Measurement), and accounting record format information.

OSS Server

To send alarms, logs, OMs, and accounting record information to a northbound OSS, the OSS destination is configured here. Open the OSS Server window by selecting **Network Data** > **Profiles** > **OSS Server** from the config view.

Before configuring a new OSS server, the IP address for the server must be added at the Addresses window. Operations at the OSS Server window require an administrative role with OssProfileService privilege.

When an OSS Server profile is created, it is associated with a Name and an Address. After the profile is created, it is available to be associated with FTP Push profiles and SNMP Manager profiles.

Record Format

The record format folder organizes the formatting of logs, OMs, and accounting record formats preferred by operating company personnel, and it organizes entry of this information in a single location.

Configuring a Log Record Format

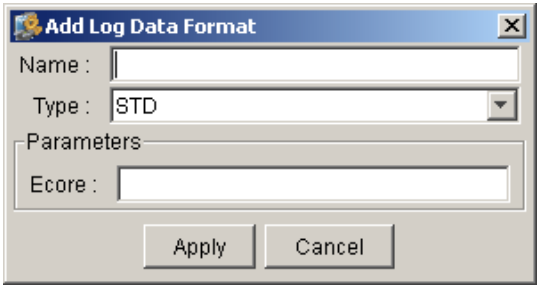
An administrative role with FPOssProfileService privilege is needed to work with log record formats.

1. Select **Network Data**> **Profiles** > **Record Format** > **Log Record Format** from the config view.

   The Log Record Format window opens in the work area.

2. Click **Add** or select an entry and click **Edit**.

The Log Record Format dialog box opens.



3 Enter the configuration data and click **Apply**.

Field	Value	Description
Name	string, 1 to 32 characters	This field identifies this profile. This value is used when creating a Format Path for log reports. For example, "mcp," "std," or "scc2."
Type	STD, MCP, or SCC2	STD is Nortel Network standard format. MCP is an extension of STD and offers log identifiers longer than four characters as well as long lines. SCC2 is a Telcordia standard format.
Ecore	true or false	If the log format is STD or SCC2 and this parameter is set to true, then the log header information includes a field that identifies the originating stream. The originating stream could be identified as a network element instance, for example.

Configuring an OM Record Format

An administrative role with FPOssProfileService privilege is needed to work with OM record formats.

1 Select **Network Data** > **Profiles** > **Record Format** > **OM Record Format** from the config view.

The OM Record Format window opens the work area.

2 Click **Add** on the OM Record Format window.

The Add OM Record Format dialog box opens.

Note: For the MCP 4.0 release, the only OM Record Format available is comma separated value (CSV), so only one OM Record Format is needed.

3 Specify a name for the format, such as "csv," and click **Apply**.

Configuring an Accounting Record Format

An administrative role with AMOssProfileService privilege is needed to work with accounting record formats.

1 Select **Network Data** > **Profiles** > **Record Format** > **Accounting Record Format** from the config view.

The Accounting Record Format window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The Accounting Data Format dialog box opens.

3 Enter a name for the format, such as "acct," and select MCPV3 or MCPV4 for the Type, then click **Apply**.

File Type

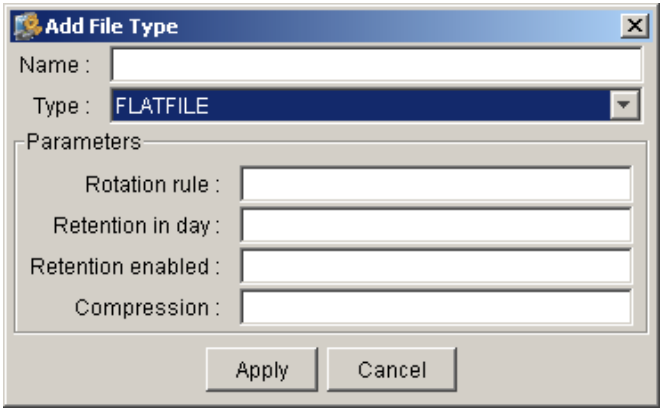
The File Type folder contains configuration data for all OSS file types such as FLATFILE, MCP3IPDRXML, or MCP4IPDRXML. FLATFILE is an ASCII file type and lines are terminated by a carriage return only. MCP3IPDRXML and MCP4IPDRXML formats are for accounting record formats. Operations with File Type data require an administrative role with OssProfileService privilege.

1 Select **Network Data** > **Profiles** > **File Type** from the config view.

The File Type window opens in the work area.

2 Click **Add** on the File Type window. The Edit button is enabled, but existing File Type configuration data cannot be modified.

The Add File Type dialog box opens.



3 Enter the configuration data and click **Apply**.

Field	Value	Description
Name	string, 1 to 32 characters	This value identifies this file type, and is needed when configuring the format path.
Type	FLATFILE, MCP3IPDRXML, MCP4IPDRXML	FLATFILE is an ASCII format with lines terminated by a carriage return. MCP3IPDRXML and MCP4IPDRXML are accounting record formats that used XML to record Internet Protocol Detail Record (IPDR) information.
Rotation rule	string	This creates a rule for closing active files and opening new files. Rules are based on time (interval or a specific hour and minute) and optionally by size (in kilobytes): *EVERY n | AT hh:mm AM|PM OR SIZE m* **EVERY n** - This keyword indicates to rotate a file a specific interval in minutes, such as 60. **AT hh:mm AM|PM** - This keyword indicates to rotate a file at a specific time each day, such as '06:00 AM.' **OR SIZE m** - This keyword modifies the rule so that a file can be rotated before the interval expires or the specified time if the file reaches the size specified in kilobytes. For example, OR SIZE 200. Example: EVERY 60 OR SIZE 200.
Retention in day	integer, 1 to 7	This value indicates the number of days to retain the files.

Field	Value	Description
Retention enabled	true or false	This value indicates if files should be retained the number of days specified in "Retention in day," or if the "Retention in day" value should be ignored and all files older than seven days are deleted.
Compression	true or false	This value indicates if the System Manager should record the files in a compressed format.

Format Path

The Format Path folder organizes configuration data for log,OM, and accounting records. In this folder, configuration data is entered to associate the format configured in Record Format with a File Type to create a Format Path.

Configuring a Log Format Path

1 Select **Network Data** > **Profiles** > **Format Path** > **Log Format Path** from the config view.

The Log Format Path window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The Log Format Path Profile dialog box opens.

3 Enter a name, then select a Data Format and File Type. The options for Data Format and File Type are determined by previously entered for Log Record Format and File Type. For example, enter a name of "mcp-file" if the Data Format is "mcp" and the File Type is "file."

Click **Apply**.

The Log Format Path Profile dialog box closes and an entry is added to the Log Format Path window. This data is used when configuring the Standard Log Stream for the System Manager or a Fault-Performance Manager..

Configuring an OM Format Path

1 Select **Network Data** > **Profiles** > **Format Path** > **OM Format Path** from the config view.

The OM Format Path window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The OM Format Path Profile dialog box opens.

3 Enter a name, then select a Data Format and File Type. Options for Data Format and File Type depend on previous configuration data. For example, enter a name of "csv-file" if the Data Format is "csv" and the File Type is "file."

Click **Apply**.

The OM Format Path Profile dialog box closes and an entry is added to the OM Format Path window. This data is used when configuring the Standard OM Stream for the System Manager or a Fault-Performance Manager..

Configuring an Accounting Format Path

1 Select **Network Data** > **Profiles** > **Format Path** > **Accounting Format Path** from the config view.

The Accounting Format Path window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The Accounting Format Path Profile dialog box opens.

3 Enter a name, then select a Data Format and File Type. Options for Data Format and File Type depend on previous configuration data. For example, enter a name of "mcp4-ipdr4" if the Data Format is "mcp4" and the File Type is "ipdr4."

Click **Apply**.

The Accounting Format Path Profile dialog box closes and an entry is added to the Accounting Format Path window. This data is used when configuring the Standard Accounting Stream for an Accounting Manager..

FTP Push

The FTP Push section of the config view organizes profiles for transferring logs, OMs, and accounting records from the System Manager or Fault-Performance Manager to an OSS server. Before creating an FTP Push profile, the OSS Server must be configured.

After creating an FTP Push profile, the System Manager and Fault-Performance Manager network elements can be configured to use the FTP Push profile for transmitting logs and OMs by associating the FTP Push profile with an FTP Push Log Stream or an FTP Push OM Stream.

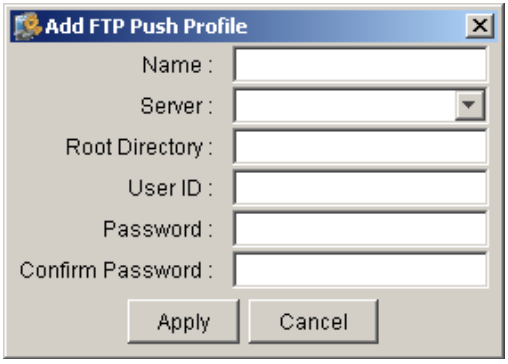
Accounting Manager network elements can be configured to use the FTP Push profile for transmitting accounting records by associating the FTP Push profile with an FTP Push Accounting Stream.

1 Select **Network Data** > **Profiles** > **FTP Push** from the config view.

The FTP Push window opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The FTP Push Profile dialog box opens.



3 Enter the configuration data and click the **Apply** button.

Field	Value	Description
Name	string, 1 to 32 characters	Enter a name to identify this profile. This value is needed when associating this profile with an FTP Push log, OM, or accounting stream
Server	pull down	Select a configured OSS Server from the pull down menu. An OSS Server must be configured before performing this procedure.
Root Directory	string	Enter the destination directory on the OSS server to place records. This directory must already exist on the OSS server. The transferred files are organized further by directory structure, refer to Pushed file directory structure.

Field	Value	Description
User ID	string	This value is a valid account for the OSS server.
Password	string	This value is the password for the account on the OSS server.
Confirm Password	string	This value is used to reduce typing errors.

Pushed file directory structure

When transferring records, the System Manager, Fault-Performance Manager, or Accounting Manager opens an FTP session to the OSS server and changes directory to the location specified by parameter "Root Directory." A strict file and directory structure organizes the records on the OSS server:

<Root Directory>/oss/<stream>/MCP_4.0/<ne>/<monitored_nes>

- **Root Directory** — this is the value defined for the Root Directory parameter
- **stream** — log, om, or acct
- **ne** — this identifies the network element instance that gathered the data such as SM_x, FPM_x, or AM_x
- **monitored_nes** — directories are created for each network element instance that is monitored by this System Manager, Fault-Performance Manager, or Accounting Manager

For example, if System Manager instance 0 (SM_0) is responsible for collecting logs from Accounting Module instance 0 (AM_0), and the records are transferred, the log files are placed in the following location:

```
.../oss/log/MCP_4.0/SM_0/AM_0/...
```

SNMP Manager

Network administrators can integrate alarms generated by MCS managed network elements into their current Network Management Layer (NML) manager.

Alarm generating events report to the SNMP (Simple Network Management Protocol) manager registered with the system. Operating with SNMP Manager data requires an administrative role with SnmpProfileService privileges.

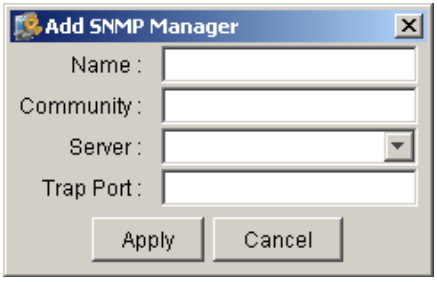
Use the following procedure to add an SNMP Manager. To start forwarding traps to an existing Network Management Layer (NML) manager, complete this procedure and then configure the System Manager and all Fault-Performance Managers to use this SNMP Manager profile.

1 Select **Network Data** > **Profiles** > **SNMP Manager** from the config view.

The SNMP Manager opens in the work area.

2 Click **Add** or select an entry and click **Edit**.

The SNMP Manager dialog box opens.



3 Enter the configuration data and click **Apply**.

Field	Value	Description
Name	string, 1 to 32 characters	This field identifies the SNMP Manager profile. This value is used when associating this SNMP Manager profile with the System Manager or a Fault-Performance Manager.
Community	string	This field indicates the community string that the SNMP trap daemon on the OSS server is configured to accept.
Server	pull down	Select a configured OSS server.
Trap Port	integer	This field identifies which port the traps should be sent to. This value must match the configuration of the SNMP daemon on the OSS server.

Servers configuration and management

Topics in this chapter

Servers configuration and management overview

Servers are typically added and configured during installation and commissioning. The number, type, and redundancy of servers depends on the specific network configuration.

Servers are deployed to host the following network element applications:

- System Manager
- Database Manager
- RTP Portals
- Fault-Performance Managers
- Accounting Managers
- Session Managers
- Provisioning Managers
- Personal Agent Managers
- IP Client Managers

- UFTP Servers

Note: These network element applications are deployed on managed servers. However, many network element applications are collocated on a single server. For example, a System Manager server hosts one instance of the System Manager and one instance of an Accounting Manager.

Server Configuration

Operating with server data requires an administrative role with PhysicalServerService, PhysicalSiteService, IPAdddressService, LOMServerService, and SnmpProfileService.

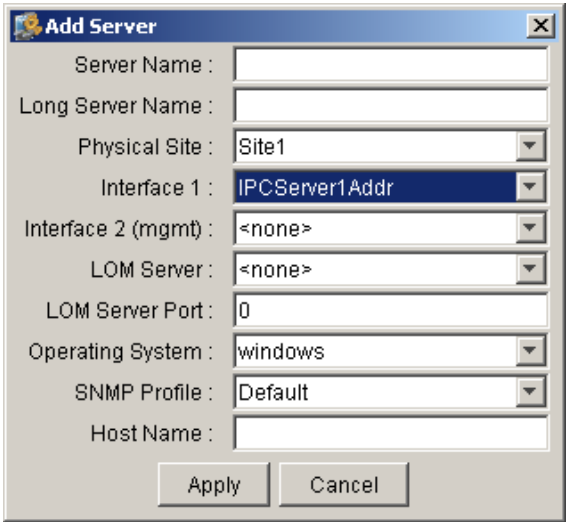
Configuring a server

1. Select **Servers** from the config view.

   The Servers window opens in the work area.

2. Click **Add** or select an entry and click **Edit**. Modifying an operational server will affect services deployed on that server.

   The Server dialog box opens.



3 Enter the configuration data and click the **Apply** button.

Field	Value	Description
Server Name	string, 1 to 6 characters	This field indicates the name of the server, for example, EMS1. This value is used when associating the network element application to the server.
Long Server Name	string, 1 to 32 characters	This field indicates the long name of the server, for example, EMS1Server.
Physical Site	pull down	Select the location of the server.
Interface 1	pull down	Select Logical Name of the IP address for this server.
Interface 2 (mgmt)	pull down	This optional field is used to configure a management LAN. If configured, all northbound OAM feeds are sent over this interface.
LOM Server	pull down	This optional field associates a lights out management server with this this server.
LOM Server Port	integer	This optional field identifies the LOM port on the LOM server that is connected to the LOM port on this server. Refer to "Advanced LOM of a Sun Netra 240 server" on page 58 for more information.
Operating System	pull down	This field is used for SNMP polling. If this field is set to "windows," then memory information will not be polled from the server.
SNMP Profile	pull down	Select the name of an SNMP profile. Ensure that the operating system SNMP deamon is configured to match the defined SNMP profile.
Host Name	string, 1 to 32 characters	This parameter identifies the hostname of the server. It is a required field for servers that use LOM. For servers that use LOM, the value entered here is checked against the server hostname configuration before any LOM commands are executed.

The Server dialog box closes and the Servers window is updated. This data is used to configure a network element instance.

Deleting a server

Administrators must delete all the hosted network elements deployed on the server before deleting the server. If an attempt is made to delete a server with services deployed on it, the request is rejected and indicates that the server is associated with NEInstanceData.

1 Select the server entry from the Servers window and click **Delete**.

The confirm Delete server dialog box opens. Click Yes to confirm the delete. The Servers window is updated.

Server operations and maintenance

Administrators can use the **Power On**, **Power Off**, and **Reset** operations on a server. These commands are out-of-band commands which allow an administrator at the System Management Console to turn the power on, off, or reset a server. All applications deployed on the server are affected.

These operations are only available for Sun Microsystems servers that support Lights Out Management (LOM) and requires that the server is associated with an LOM Server. Some servers use Advanced LOM. The Advanced LOM requires a password protected login before LOM actions are performed. The login information is normally configured during initial installation and commissioning.

Warning: All the services hosted on the server are impacted when an administrator Powers off or resets a server.

Using LOM

The power off operation powers down the selected server.

Note: If a System Manager server is powered off, the connection to the System Management Console is lost. Administrators need to power up the System Manager server either physically or via the terminal server before a new connection can be made.

1. Select **Servers** > **<server_name>** > **Maintenance** from the config view.

   The LOM Commands window opens in the work area.

2. Select an entry and click **Power On**, **Power Off**, or **Reset**.

   A Login Information dialog box opens.

3. Enter a LOM username and password for the operating system on the server. Click the **OK** button.

   If the request is Power Off or Reset, a confirmation dialog window opens. Click Yes.

A Command Status Display window opens in the work area. The status of connecting to the server, log in, and maintenance action are shown in the window.

If the server is a Sun Netra 240, administrators are prompted to login to access the advanced LOM. See Advanced LOM of a Sun Netra 240 server for more information.

Advanced LOM of a Sun Netra 240 server

The advanced LOM functionality of Sun Netra 240 servers is password protected. When performing a LOM related task on a Netra 240, administrators are prompted to login after confirming the operation. The login profile is configured on the Netra 240, typically during installation and commissioning. Configuration of advanced LOM passwords is described in the following Sun product documentation available on the Sun website (http://www.sun.com/products-n-solutions/hardware/docs/Servers/Netra_Servers/Netra_240/index.html):

- *Sun Advanced Lights Out Manager Software User's Guide for the Netra 240 Server*
- *Netra 240 Server System Administration Guide*

In addition to having a configured LOM login, the HostName field of the Sun Netra 240 server needs to be configured. The HostName field ensures that the server selected in the config view is the same server undergoing a LOM operation. The hostname of the server is set during installation and commissioning. If the Host Name field is not set, the System Management Console will return a 'HostName not provided' error message when trying to access the advanced LOM login.

Monitoring a server

When server configuration data is entered through the System Management Console, one of the parameters is SNMP Profile. In order to monitor the performance statistics for the server, the server monitor must be started. Before the monitor is started, a grey down arrow icon is associated with the server in the Logical and Physical View windows. After the monitor is started, the a green, yellow, orange, or red dot indicates the status of the server hardware.

1 Select **Servers** > **<server_name>** > **Monitor** from the config view.

The Monitor window for the server opens in the work area.

2 If the monitor is not running, the status line at the bottom left of the monitor window indicates "The server monitor is not running." Click **Start Monitor** to begin collecting statistics for the server.

The status line changes to indicate "The server monitor is running."

Note: If the monitor is running and no statistics are generated on the monitor window, check the Logical or Physical View window for a major SRVR101 alarm against the server. This alarm indicates that the SNMP deamon on the server is not responding. Verify that the server is running and then verify the configuration data related to the SNMP Profile associated with the server.

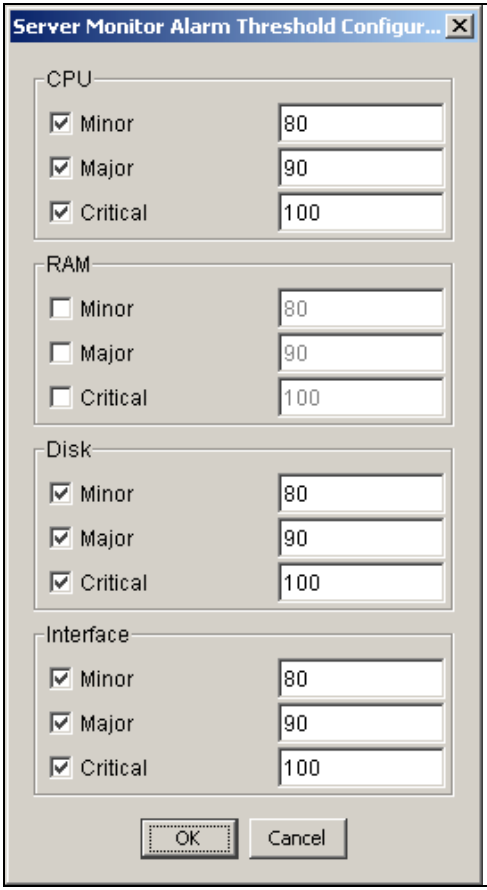
These statistics are recorded to disk on the server that hosts the System Manager. To view these records, configure an FTP Push job, and then set the System Manager's FTP Push OM Stream to use the FTP Push job.

Configuring server alarm thresholds

Altering thresholds requires an administrative role with ServerMonitorConfigService privilege.

1 Thresholds for CPU, memory, disk, and interface usage can be set from the Monitor window by clicking **Configure Thresholds**.

The Server Monitor Alarm Threshold Configuration window opens in the work area



Enter new values to set different thresholds.

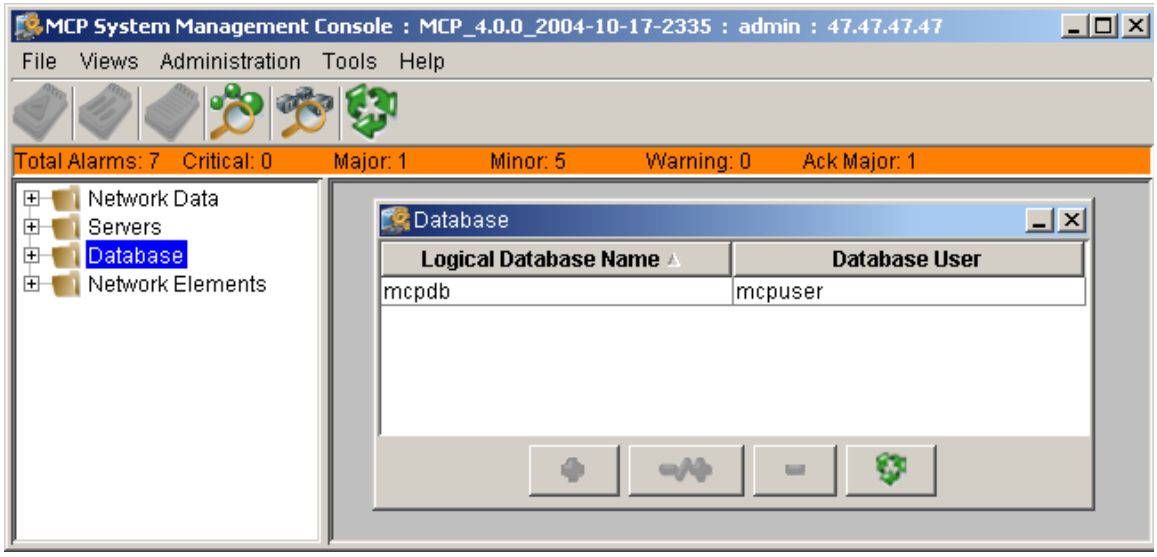
To remove alarming for threshold crossing, deselect the checkbox next to each item. In this example, no SRVR402 alarms or logs will be generated since the checkboxes for RAM are deselected.

SRVR401 - CPU
SRVR402 - RAM
SRVR403 - Disk
SRVR404 - Interface

2 Modify the thresholds by changing the threshold values or by enabling and disabling the alarm thresholds and then click **OK**.

Database configuration and management

Configuration and deployment of the database is completed during installation and commisioning. After commisioning, monitoring the database is the only operation to perform from the System Management Console.



Viewing the database monitor status

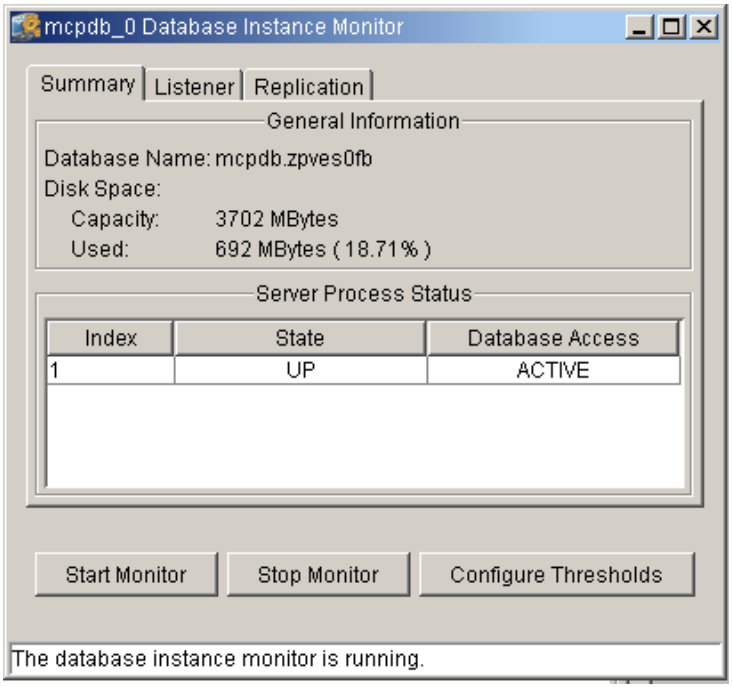
The database monitor indicates the capacity, disk space used, and status of the database. This procedure requires an administrative role with DBMonitorService privileges.

1 Select **Database** > **mcpdb** > **Monitor** from the config view.

The mcpdb Monitor window opens in the work area.

2 Select instance 0 or 1 from the mcpdb Monitor window and click **Monitor**.

The mcpdb_x Database Instance Monitor window opens. The Replication tab is only shown in replicated database configurations.



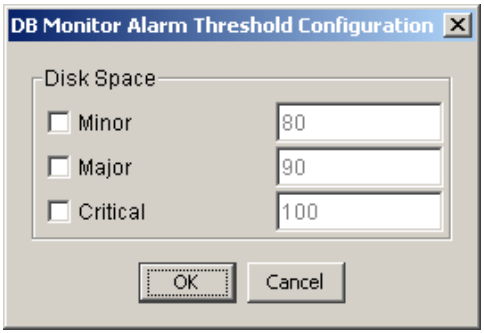
3 Ensure that the status line at the bottom of the Monitor window indicates "The database intance monitor is running." If not, click **Start Monitor**.

Configure resource thresholds

Thresholds for the database monitor control when DBMN401 alarms are raised. This procedure requires an administrative role with DBMonitorConfigService privileges.

1 From the mcpdb_x Database Instance Monitor window, click **Configure Thresholds**.

The DB Monitor Alarm Threshold Configuration window opens. The default thresholds are 80 for Minor, 90 for Major, and 100 for Critical.

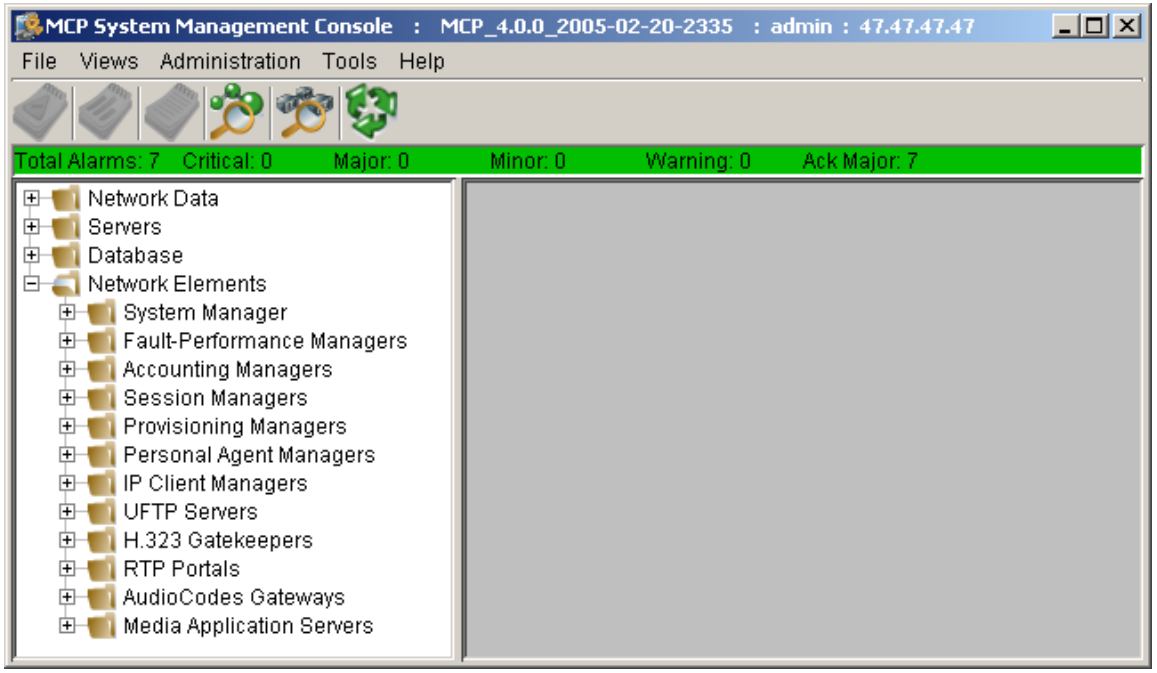


2 Select each threshold to enable for alarming and set a threshold. When done, click **OK**.

Network Elements configuration and management

Topics in this chapter

- Network Element configuration
- Network element software updates
- Network element management



Network element configuration overview

Administrators add, configure, and manage most network elements using the System Management Console. Refer to the individual network element guides for network element specific details. See Related publications for a list of network element documents.

The System Manager and Database Manager (Databases in the config view) are added manually without the use of the System Management Console. Both are monitored using the System Management Console.

Network Element configuration

Network elements are added, configured, and managed by the System Management Console. The following procedures are generic in nature, and do not apply to any one specific network element application. Refer to the individual network element guides for specific configuration details and service property descriptions. See "Related publications" on page x for a list of the related network element guides.

Adding a network element

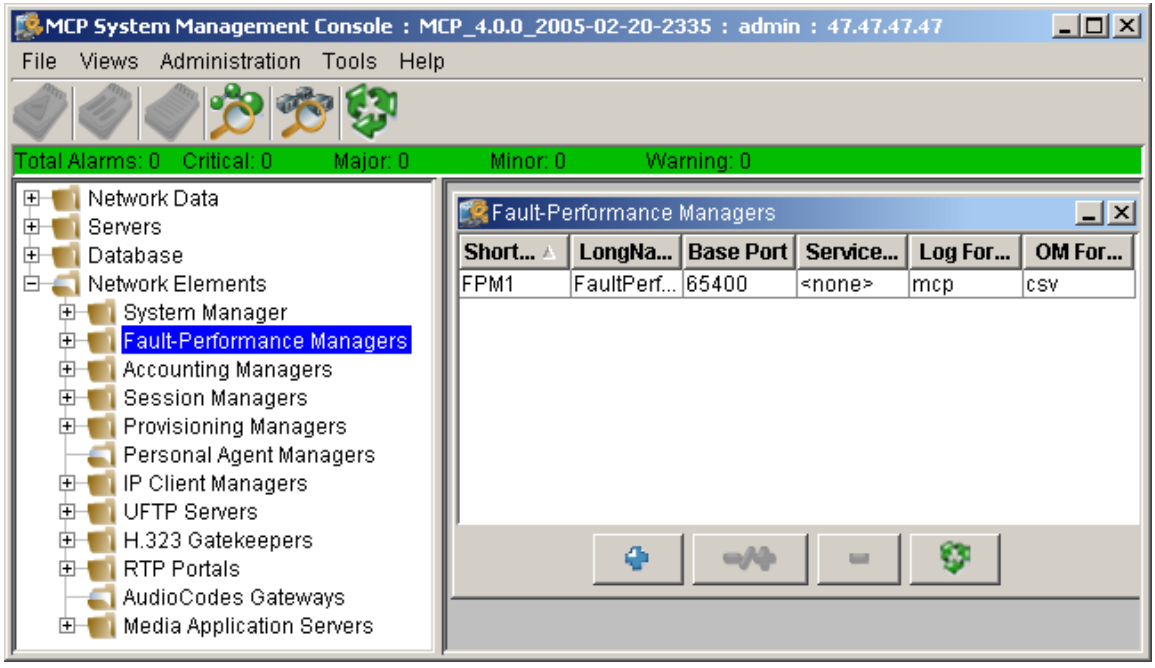
The System Manager network element is added manually and needs to be operational before administrators can connect with the System Management Console. Adding a network element requires an administrative role with NEService privilege.

The network elements added to a specific server will depend on the system architecture and operational requirements. Refer to the individual network element guides for specific details related to network element configuration.

To add a network element from the System Management Console, perform the following steps:

1 Select **Network Elements** > **<ne_type>** from the config view.

A window for the network element type opens in the work area. Existing network elements of this type are indicated by a row in the window. In the graphic below, no Fault-Performance Managers have been configured.

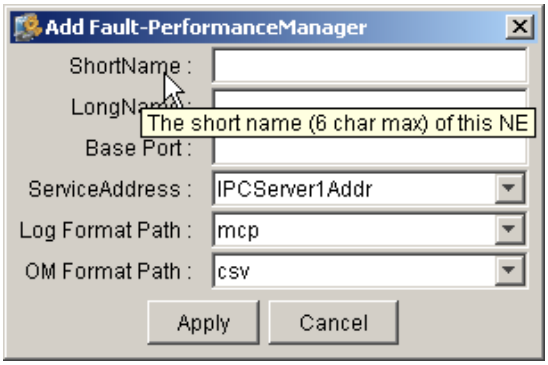


2 Click **Add** on the network element window.

The Add window opens. Different network element types require different configuration data.

3 Enter the configuration data on the Add window. Refer to the network element specific documentation for the configuration issues and property descriptions.

Mouse over help with property descriptions are available by moving the cursor over the property name.



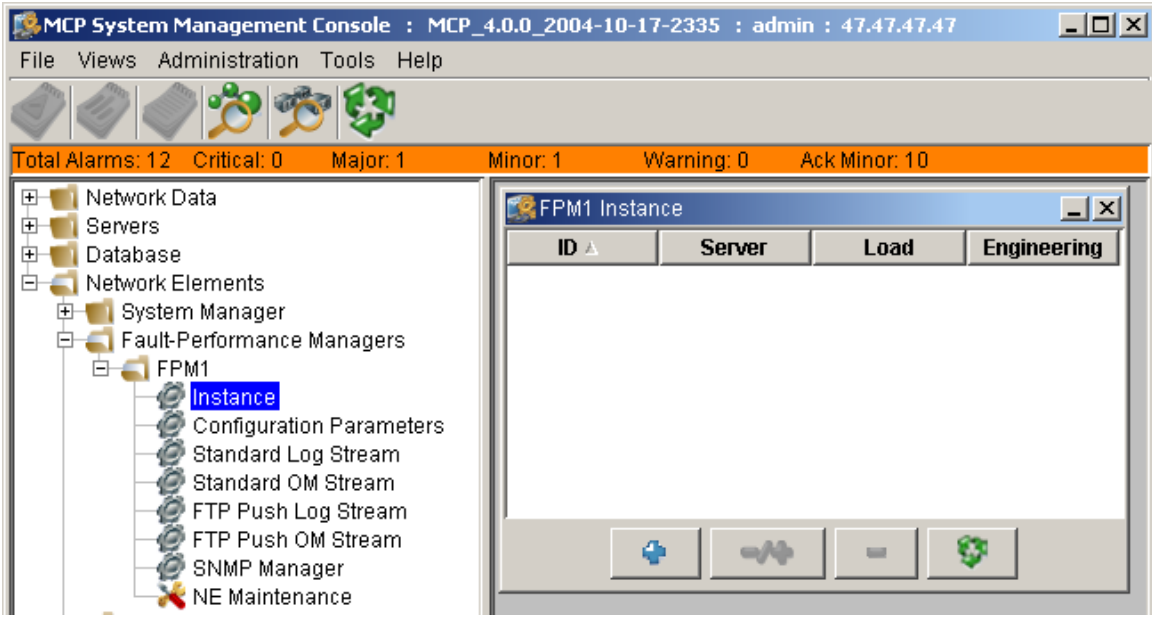
4 Click **Apply** on the Add window.

The Add window closes and an entry is added to the network element type window.

The network element is added to the config view, but it does not have any servers or software associated with it yet.

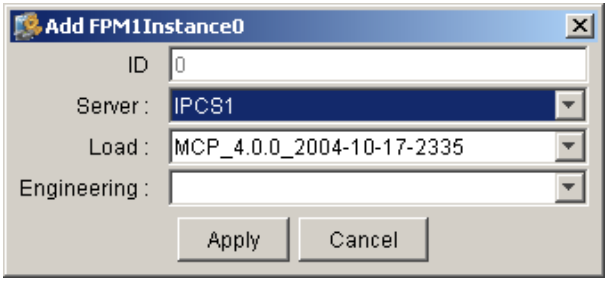
5 Expand the network element in the config view so that the newly configured element is visible, and select **Instance**.

The network element instance window opens in the work area.



6 Click **Add** to add an instance of this network element and associate the instance with a server.

The add instance dialog box opens in the work area.



7 Use the pull down menus to associate a server, a software load, and an engineering profile with the instance. The engineering profile controls the initial size of the Java Virtual Machine and establishes Engineering parameters appropriate for the hardware capabilities of the server.

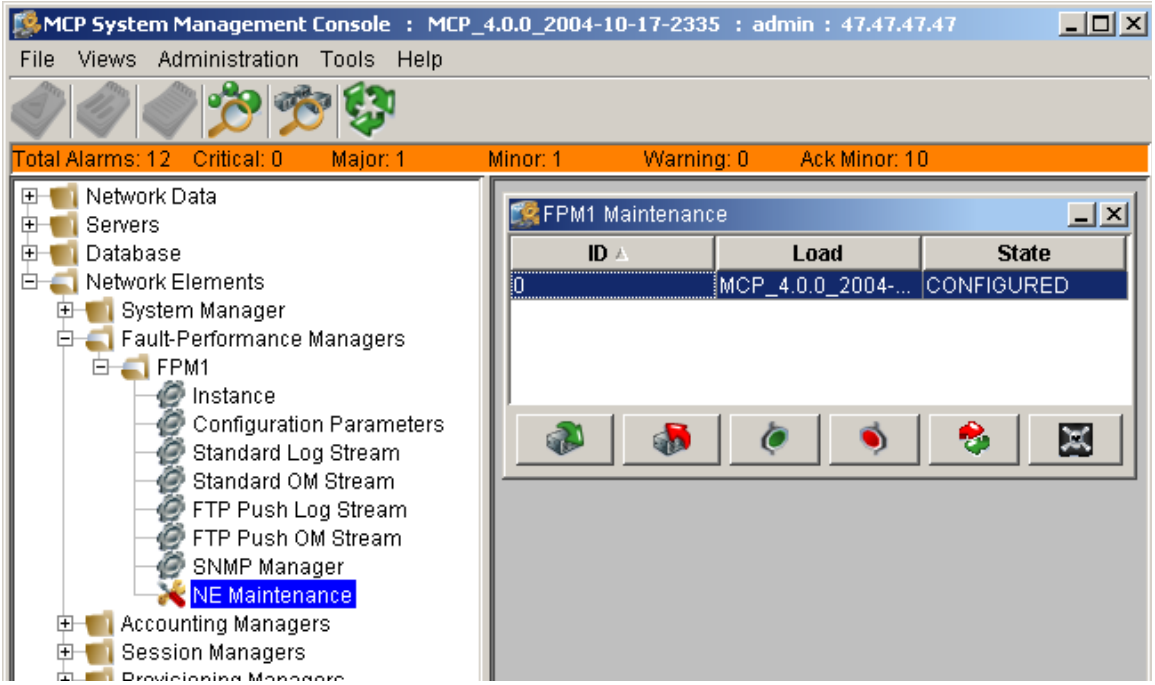
Click **Apply** on the add instance dialog box.

The add instance dialog box closes and an entry is added to the instance window for the network element.

8 If the network element offers fault tolerance and the network architecture is designed for a redundant unit, repeat steps 6 and 7 for the second unit.

9 Select **NE Maintenance** from the config view for the newly created network element.

The Maintenance window for the network element opens in the work area. The state is set to CONFIGURED and the network element is not providing service yet.



10 Select an instance and click **Deploy** on the Maintenance window.

Software is transferred from the System Manager to the server associated with the selected network element instance. The instance transitions from CONFIGURED to DEPLOYING. Once deployment is complete, the instance transitions to OFFLINE. If the network element is redundant, select the other instance and click Deploy again.

11 Select an instance and click **Start** on the Maintenance window.

The instance completes the following state transitions:

- *OFFLINE to STARTING - clicking the Start button causes this transition*
- *STARTING to CONNECTED - the instance has communication with the System Manager*
- *CONNECTED to INITIALIZING - bootstrapping is complete and subsystems on the instance are initializing*
- *INITALIZING to STANDBY - if the network element is fault tolerant, and the other instance is active, this instance remains in STANDBY until a switch of activity*
- *STANDBY to ACTIVATING - this instance has determined that it should become the active instance*
- *ACTIVATING to ACTIVE - this instance is now providing service*

The network element is installed and activated. The time needed for the install depends on the network element type and the hosting server.

Note: Installing a network element on a server may generate a threshold alarm indicating high CPU usage. The alarm clears once installation is complete.

Modifying a network element

Network elements can be modified in several ways:

- Modify a whole network element — this is used to modify the base port of a network element application, to associate a different Fault-Performance Manager with the network element, and many options that are specific to each network elment type
- Modify a network element instance — Engineering Parameters for each network element instance can be altered
- Modify Configuration Parameters — this option controls operating parameters can be modified while the network element is in service, and the changes apply to all network element instances of the network element

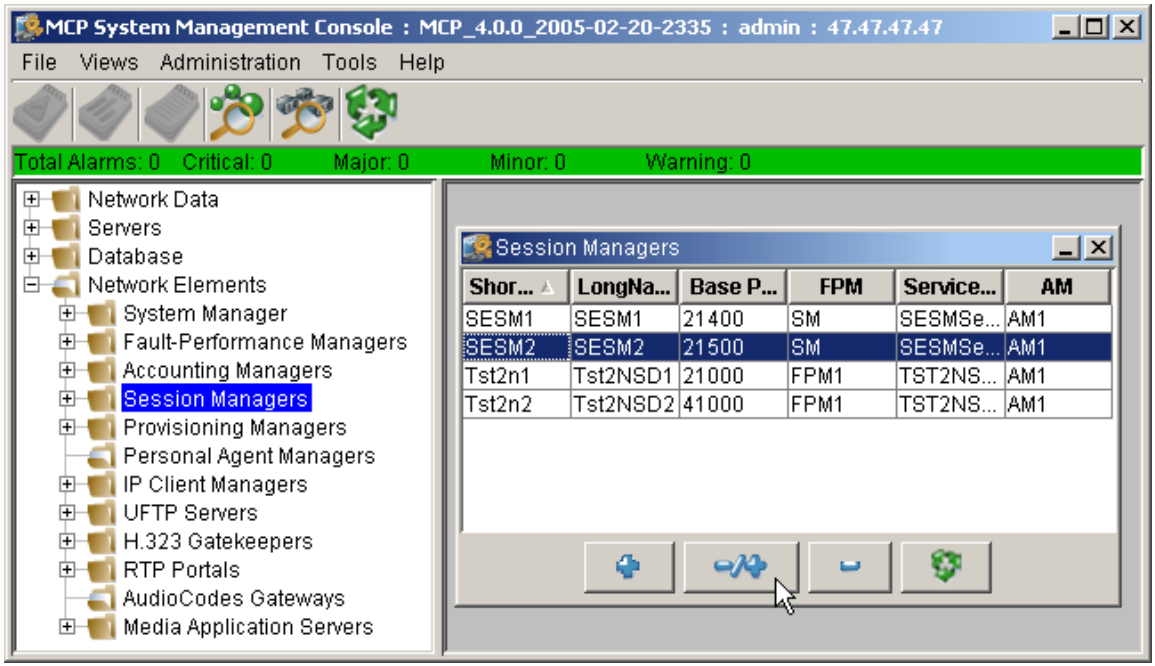
Modify a whole network element

This option is used to modify the configuration data that was entered when the network element was added to the config view. This procedure requires an administrative role with NEService privilege.

1 Select **Network Elements** > **<ne_type>** from the config view.

A window for the network element type opens in the work area.

2 Select the entry for the network element to modify and click **Edit**.



The Edit dialog box opens.

3 Modify the configuration data and click **Apply**. The properties for each network element type differ. Refer to the specific network element documentation for informaton about the properties.

A warning dialog box opens if other network elements need to be restarted as a result of the configuration change. Otherwise, the Edit dialog box closes and the data change is made to all instances of the network element immediately.

Modify a network element instance

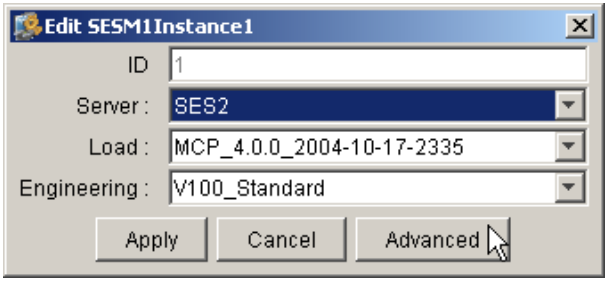
Before performing this procedure, contact your next level of support. Modifying the engineering parameters for a network element instance can reduce the performance and services of the network element. Any changes require a manual restart of the network element instance to take effect and the changes are only applied to a single network element instance; for redundant network elements, the change needs to be made to other network element instances too. This procedure requires an administrative role with NEInstanceService and EngParmService privileges.

1 Select **Network Elements** > **<ne_type>** > **<ne>** > **Instance** from the config view.

The Instance window opens in the work area.

2 Select the network element instance to modify from the Instance window and click **Edit**.

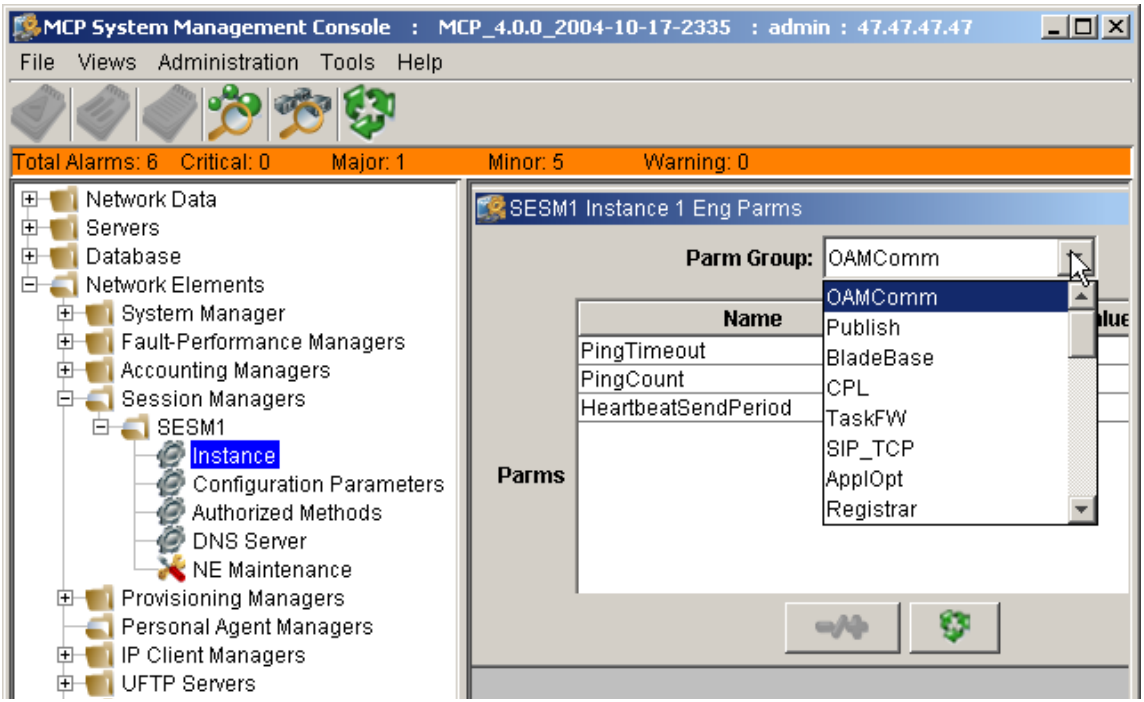
The Edit Instance dialog box opens.



3 Click **Advanced** on the Edit Instance dialog box.

The Edit Eng Parms window opens in the work area.

4 Engineering parameters are organized by Parm Group. Select the Parm Group to modify from the pull down menu.

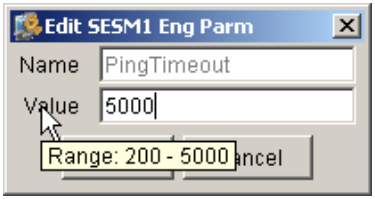


Once the Parm Group is selected, the engineering parameters are listed on the Instance Eng Parms window.

5 Select the engineering parameter to modify from the Instance Eng Parms window and click **Edit**.

The Edit Eng Parms dialog box opens.

6 Enter a new value for the engineering parameter and click **Apply**. Mouse over help is available.



After clicking Apply, the Engineering Parameter Update warning dialog box opens. Click OK to confirm the warning.

A manual restart is needed before the changes take effect. Refer to the documentation for the network element type for information on how to perform a manual restart.

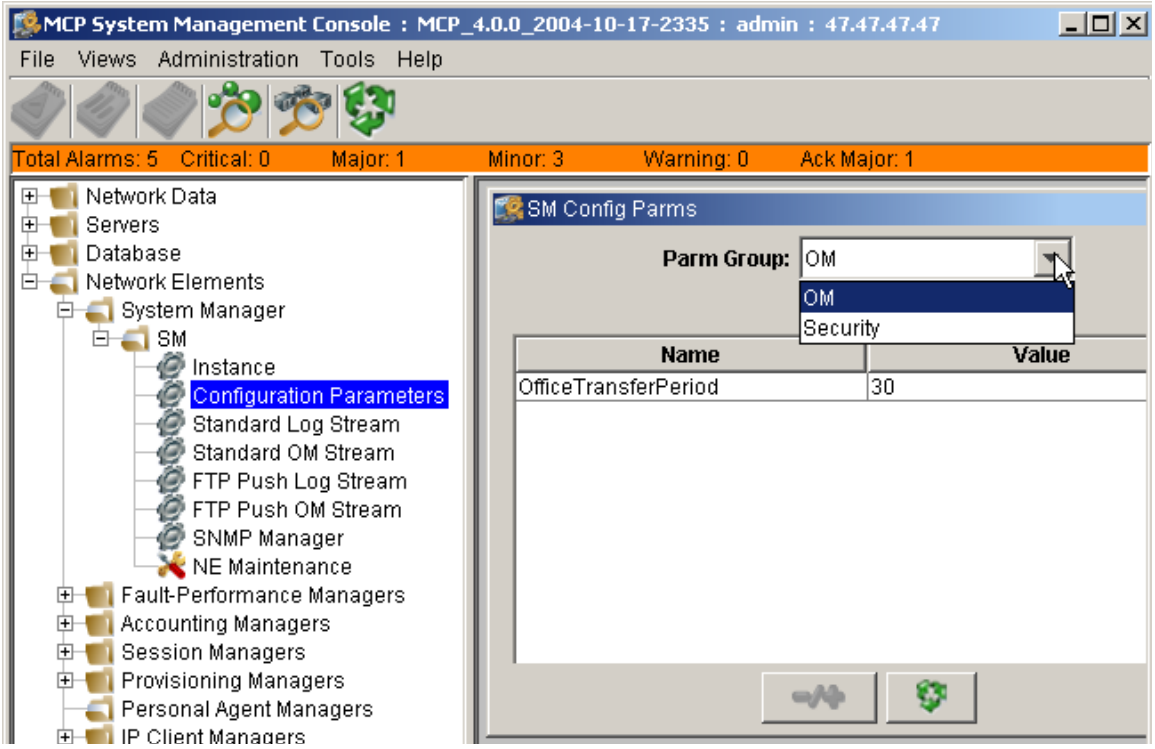
Modify Configuration Parameters

Every network element type offers some configurable operating parameters. The available configuration parameters depend on the network element type. This procedure requires an administrative role with ConfigParmService privilege.

1 Select **Network Elements** > **<ne_type>** > **<ne>** > **Configuration Parameters** from the config view.

The Config Parms window opens in the work area.

2 Select a parameter group from the pull down menu:



The list of configurable parameters is updated on the Config Parms window.

3 Select the parameter to modify and click **Edit**.

The Edit Config Parm dialog box opens.

4 Enter a new value for the configuration parameter and click **Apply**.

The new value is validated. If the value is allowable, the Edit Config Parm window closes and the configuration parameter is updated.

Deleting a network element

Administrators can delete a network element on a server. However, before removing any network elements, contact support personnel to determine if the network element should be deleted. This procedure requires an administrative role with NEService and NEInstanceService privileges.

1 Select the **Network Elements** > **<ne_type>** > **<ne>** > **NE Maintenance** from the config view.

The Maintenance window opens in the work area.

2 Select each network element instance and click **Stop** from the Maintenance window.

A confirmation prompt opens.

3 Confirm the Stop, click **Yes**.

The network element instance state changes to DEACTIVATING, DISCONNECTED, and then OFFLINE.

4 Select each network element instance and click **Undeploy** from the Maintenance window.

The network element instance state changes to CONFIGURED.

5 Select **Network Elements** > **<ne_type>** > **<ne>** > **Instance** from the config view to view a list of the configured network element instances for this network element.

The Instance window opens in the work area.

6 Select each entry and click **Delete**.

A confirmation dialog box opens. Confirm the deletion by clicking Yes. Each instance is removed from the Instance window.

7 Select **Network Elements** > **<ne_type>** from the config view.

A window that lists all the network elements of this type appears in the work area.

8 Select the network element to delete and click **Delete**.

A confirmation dialog box opens. Confirm the deletion by clicking Yes. The network elment is removed from the list of network elements.

Network element software updates

Administrators can update the software for network elements. The current configuration data is automatically transferred to the updated version, with the exception of any modified Engineering Parameters. Engineering Parameters are set to factory defaults during a software update. The update can be an upgrade to a new version, or a downgrade to a previous software version.

The service impacts of updating network element software will vary depending on the network element involved and system architecture. Refer to the individual network element and upgrade guides for more details.

Updating network element software

This procedure requires an administrative role with NEInstanceService privilege.

1 Select **Network Elements** > **<ne_type>** > **<ne>** > **NE Maintenance** from the config view.

The Maintenance window opens in the work area.

2 Select the STANDY instance for redundant network elements or the only instance for simplex network elements and click **Stop**.

A confirmation dialog box opens. Confirm the stop by clicking Yes. The network element instance transitions to OFFLINE.

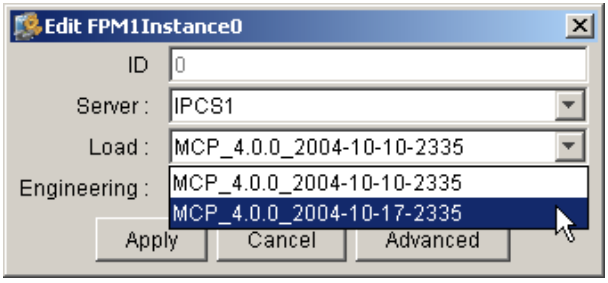
3 Select **Instance** from the config view for this network element.

The Instance window opens in the work area.

4 Select the instance that was stopped and click **Edit**.

The Edit Instance dialog box opens.

5 Select the software version to use from the Load pull down menu and click **Apply**.



The Edit Instance window closes and the network element instance transitions to CONFIGURED.

6 Go back to the NE Maintenance window and click **Deploy** to transfer the update software load to the server that hosts the network element.

The network element instance transitions from CONFIGURED to OFFLINE.

7 Click **Start** on the NE Maintenance window to run the updated software version and begin providing service.

The network element instance transitions through several state changes, starting from OFFLINE. If this network element instance is part of a redundant network element, the transitions stop at STANDBY. If the network element is simplex, the transitions stop at ACTIVE.

Network element management

Administrators use **Start**, **Stop**, and **Restart** operations when modifying the configured properties of network elements. When a network element instance is stopped, the state changes to OFFLINE and services become unavailable. Starting, stopping, and restarting a network element instance require an administrative role with NEInstanceService privilege.

Stopping a network element

A **Stop** operation stops the processes of a network element instance.

Warning: Stopping a network element instance may impact in-progress sessions.

For all network element types, if the network element is redundant, then stopping the STANDBY or WARM STANDBY instance does not affect service, it only causes a loss of redundancy. Administrators should refer to the individual network element guides for more details.

1. Select **Network Elements** > **<ne_type>** > **<ne>** > **NE Maintenance** from the config view.

   The Maintenance window opens in the work area.

2. Select the instance to stop from the Maintenance window and click **Stop**.

   A confirmation dialog box opens. Confirm the stop by clicking Yes. The network element instance transitions to OFFLINE.

Starting a network element

A **Start** operation starts the processes of a network element instance on a server. Software must be deployed to the server before the network element instance can be started. A network element instance in a state of OFFLINE has software deployed and is stopped. A network element instance in a state of CONFIGURED does not have software deployed.

1. Select **Network Elements** > **<ne_type>** > **<ne>** > **NE Maintenance** from the config view.

   The Maintenance window opens in the work area.

2. Select the instance to start from the Maintenance window and click **Start**.

   The network element instance transitions from OFFLINE, through a series of states, and finishes at ACTIVE. If this is a redundant unit and the other unit is ACTIVE already, this unit finishes at STANDBY or WARM STANDBY.

Restarting a network element

The **Restart** operation performs a combined stop and start. During the period of the restart, the network element instance is not providing service. There is no difference between performing a restart, or stopping and then starting a network element instance.

1. Select **Network Elements** > **<ne_type>** > **<ne>** > **NE Maintenance** from the config view.

   The Maintenance window opens in the work area.

2. Select the instance to restart from the Maintenance window and click **Restart**.

   A confirmation dialog box opens. Confirm the warning by clicking Yes.

   The network element instance transitions from ACTIVE, STANDBY, or WARM STANDBY, through a series of states, and finishes at ACTIVE. If this is a redundant unit and the other unit is ACTIVE already, this unit finishes at STANDBY or WARM STANDBY.

Killing a network element

The **Kill** operation stops the MCS software on the network element instance; the operating system continues to run. This operation may be useful if stop and restart do not work.

Alarm browser

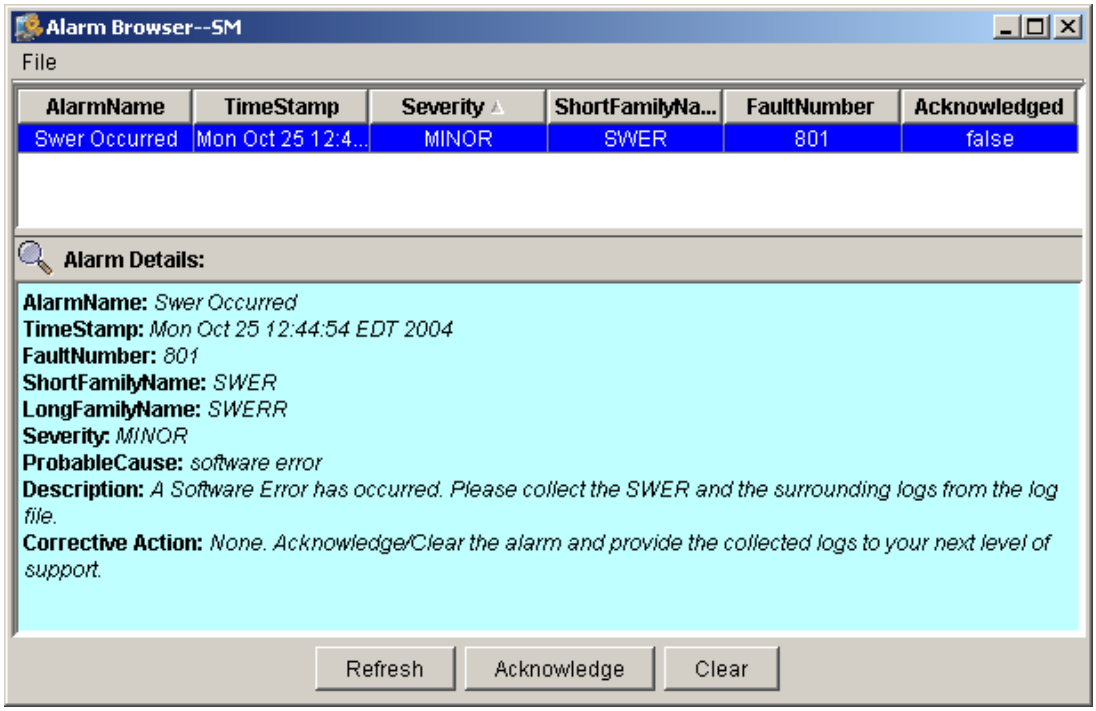
Refer to the *CVoIP Fault Management: Alarm and Log reference* for individual alarm descriptions. An administrative role with AlarmQueryService privilege is needed to view alarms from the alarm browser. To acknowledge or clear alarms, AlarmMtcService privilege is needed.

Alarm browser basics

Once in operation, network elements have the ability to raise and clear alarms. As faults occur, alarms are generated by the network element and sent to the Fault-Performance Manager (FPM) associated with the network element. The System Manager can be assigned as the the FPM. If the FPM is not the System Manager, then the FPM forwards the alarms to the System Manager for viewing at the System Management Console alarm browser.

When an alarm is raised, it is added to a list of active alarms and the alarm summary area of the System Management Console is updated to the new alarm count. The alarm remains on the active list until it is resolved. Most alarms require that the alarming condition be remedied and the alarm clears as a result of the remedy. Some alarms, like SWER alarms, require an administrator to select the alarm in the alarm browser and set it to clear. The alarms that require manual intervention to click Clear are designed to ensure that the condition is recognized. All alarms can be acknowledged at the alarm browser to prevent a single problem from being investigated by more than one administrator.

The following figure shows an alarm browser launched with the SM network element selected in the config view. See the section Alarm information displayed in the browsers for alarm information displayed in the browser.



Refer to the *CVoIP Fault Management: Alarm and Log reference* for individual alarm descriptions.

The alarm browser has two main areas, Alarm Display and Alarm Details. The Alarm Display area shows a list of all current active alarms and their details. The Alarm Details area displays text describing a single alarm selected in the Alarm Display area.

The alarm browser has the following functions available to the user.

Function	Description
Refresh	Updates the alarm browser with the current alarms and status.
Acknowledge	Sets the alarm to acknowledged to indicate that an administrator is investigating, but the alarm remains listed in the upper panel until the condition clears.
Clear	Clears the alarm from the system. The Refresh button must be clicked to remove the alarm from the alarm browser.

Alarm information displayed in the browsers

The Alarm browser can only be launched from:

- the alarm browser icon when a network element is selected in the config view
- the alarm browser icon when a server is selected in the config view
- the physical and logical view windows when a network element or server icon is selected

Note: There are two ways to view alarms for the database application. One way is to open the logical view window, expand the Logical DBs entry, and then select mcpdb_0 or mcpdb_1. The second way is to open the physical view window, expand the server or servers and DBInstance that host the database, and then select mcpdb_0 or mcpdb_1. Once an instance is selected, the alarm browser icon becomes available.

The alarms displayed in the alarm browser are dependent on the network element or server selected in the config view. For example, if a server is selected, the alarm browser shows only alarms for the server, not the network elements deployed on the server. If a network element is selected, only the alarms generated by the network element application are displayed, not alarms for the server or other applications on the server. Administrators can launch more than one browser, allowing them to view alarms for specific elements separately.

All alarms viewed in the alarm browser list the following information:

Alarm attribute	Description
Alarm Name	the name of the alarm
TImestamp	the time when the alarm was raised
Severity	the severity assigned to the alarm
ShortFamilyName	managed object family originating the alarm
FaultNumber	the number identifier of the alarm
Acknowledged	indicates whether the alarm has been acknowledged by an administrator
Probable Cause *	a brief indication of the probable cause
Description *	a full text explanation of the alarm condition
Corrective Action *	suggested course of action for correcting the condition
* — These attributes are available in the Alarm Details section of the alarm browser after an alarm is selected.	

Alarm browser operations

The alarm browser displays all the alarms originating from the network element or server selected. Administrators can launch more than one browser, allowing them to view alarms for specific elements separately.

See the following procedures for the using the information on working with alarms:

- Viewing alarms
- Viewing alarm details
- Sorting alarms based on alarm attribute
- Copying alarm information
- Clearing alarms
- Refreshing alarm information

Viewing alarms

The alarm browser displays all the alarms originating from services and servers under the selected element in the config view.

1. Select a network element or server in the config view.
2. Cick the **Alarm Browser** icon  in the toolbar.

   The alarm browser opens and shows all the alarms associated with selected network element or server.

Viewing alarm details

Select an alarm in the alarm browser to display details in the Alarm Details area.

1. Click an alarm entry in upper panel of the alarm browser.

   Information about the alarm displays in the Alarm Details area.
2. To clear the Alarm Details area, click **Refresh**.

Sorting alarms based on alarm attribute

Administrators can sort the order of the alarms in the browser according to any of the attributes used in the alarm format. By default, alarms are sorted by severity, with the most severe alarm listed at the top of the upper panel.

1. Click a column header in the upper panel of the alarm browser.

   The alarms are sorted either alphabetically or numerically depending on the alarm attribute.
2. Click the column header a second time to reverse the order.

Copying alarm information

Alarm information can be copied to the PC clipboard. This allows administrators to paste one or more alarm rows from the display, or alarm details text into other PC based documents (e.g. E-mail).

1. To select display text, click on alarm in the display to highlight the row.

   To select alarm detail's text, click and highlight the text using the cursor.

2. Press **Ctrl** + **c**.

   The text is copied to the PC clipboard.

3. Paste the text into other PC application documents.

Clearing alarms

Some alarms are manually clearable. When a manually clearable alarm is selected in the alarm browser, the **Clear** button becomes active.

1. Click the alarm in the upper panel of the alarm browser.
2. If the Clear button is active, and the corrective action suggested in the alarm details has been noted, click **Clear**.
3. Click **Refresh** to clear the Alarm Details area and remove the alarm entry from the upper panel of the alarm browser.

Refreshing alarm information

Clicking the **Refresh** button updates the alarms in the browser to reflect the current system faults.

1. To refresh the alarm information, click **Refresh**.

Log browser

Topics in this chapter

Log browser basics

Logs are used to record information related to an event so that it may be analyzed at a later point in time. Every log event is captured and archived to disk by the Fault-Performance Manager assigned to the network element or server. At the same time, the log stream is sent to the System Manager for display at the System Management Console.

The log browser has the following limitations:

- only current log reports are available for viewing at the System Managment Console
- the log browser displays 10 000 characters of data, approximately 50 log reports, and old logs are removed as new logs are added
- logs for servers are not available for display

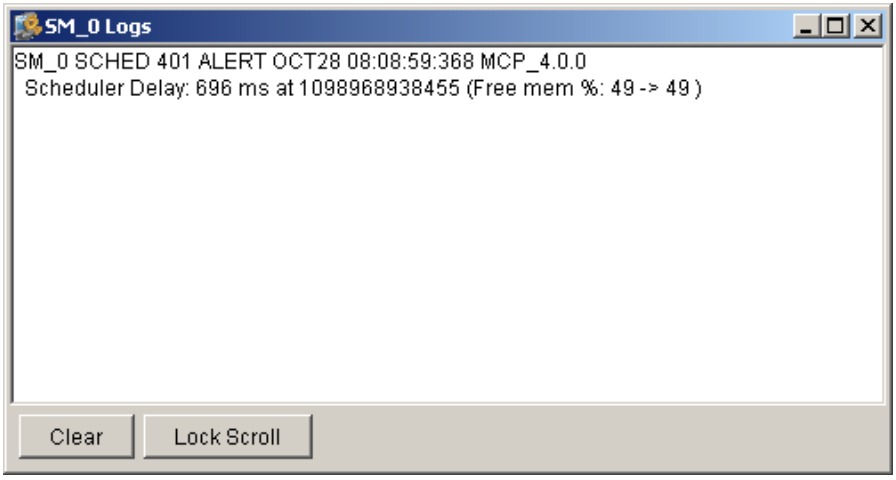
To view archived logs or logs for servers, configure an FTP Push profile and associate it with the FTP Push Log Stream for the System Manager or Fault-Performance Manager and view the archived logs from an OSS.

Current logs are a live stream of logs and alarms being reported to the System Manager from the Fault-Performance Managers. As the logs are received, they are saved to the current (*.active) log file on the System Manager server. After a configured period of time, or when the file reaches a configured size in kilobytes, the log file is closed and renamed (rotated) to an archived log file and a new active log file is opened.

The log browser displays information for a single network element, similar to the way that the alarm browser displays alarms for the selected network element.

Log browser operations

A log browser can only be launched when a network element is selected in the config view, the physical view window, or the logical view window. Administrators can have multiple log browsers open at the same time to monitor multiple components concurrently. The following figure shows a log browser for the active System Manager instance.



The following functions are available in the log browser:

Function	Description
Clear	Removes all of the existing log text from the window of the log browser.
Lock Scroll/ Unlock Scroll	Toggles the scrolling of log text in the window of the current log browser.

Log browser operations

The log browser displays all the logs originating from the selected network element. Administrators can launch more than one log browser, allowing them to view logs for different components concurrently.

See the following procedures for the using the information on working with logs in the log browsers:

- Launching the log browser from the config view
- Clearing log details
- Saving logs
- Configuring log file rotation periods

Launching the log browser from the config view

1 Select **Nework Elements** > **<ne_type>** > **<ne>** from the config view.

The log browser icon become active in the icon toolbar.

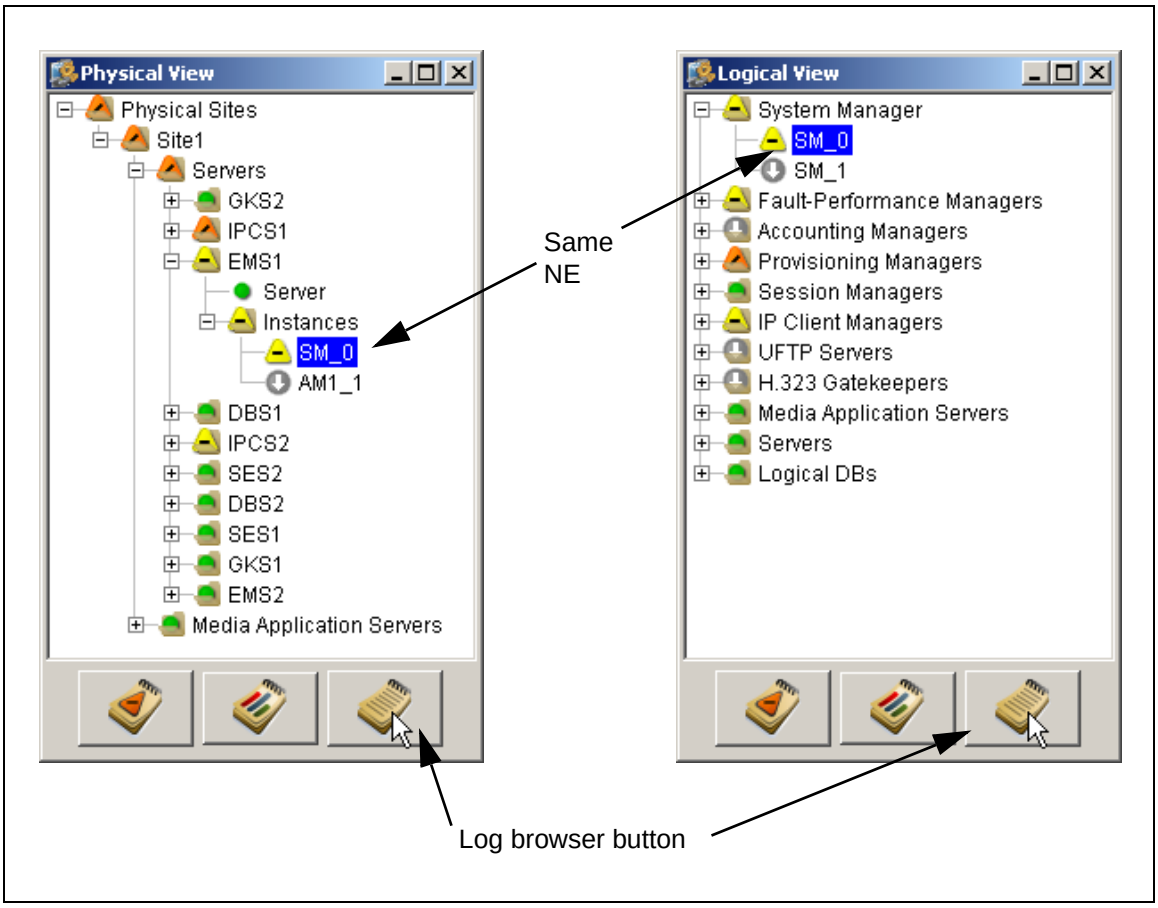
2 Click the log browser icon  from the icon toolbar.

The log browser opens. If the selected network element type is redundant, then a log browser for each instance opens.

Launching the log browser from the logical or physical view

1 Select the network element in the physical or logical view window.

The log browser icon at the bottom of the window becomes active.



2 Click the log browser button.

The log browser opens. Unlike a config view launch, only one log browser opens, and it is for the selected network element instance regardless of redundancy.

Clearing log details

Administrators can clear the log text in the browser display.

1 Click **Clear**.

Saving logs

Log text can be selected from the log browser window and pasted into other applications.

1. Select the log text from the log browser with a mouse or a **Ctrl + a** to select all the text.

   The text is highlighted.

2. Press **Ctrl + c** to copy the text to the clipboard.
3. Paste the text into another application.

Configuring log file rotation periods

Administrators can configure the log rotation interval and file size based on a File Type profile configured at the System Management Console. Different profiles can be created and these profiles can be assigned on a component by component basis, server by server basis, or at the system level. Typically, a single profile is configured at the system level. For information on configuring File Type profiles, see the information about rotation rules for File Type on page 45.

Operational measurement browser

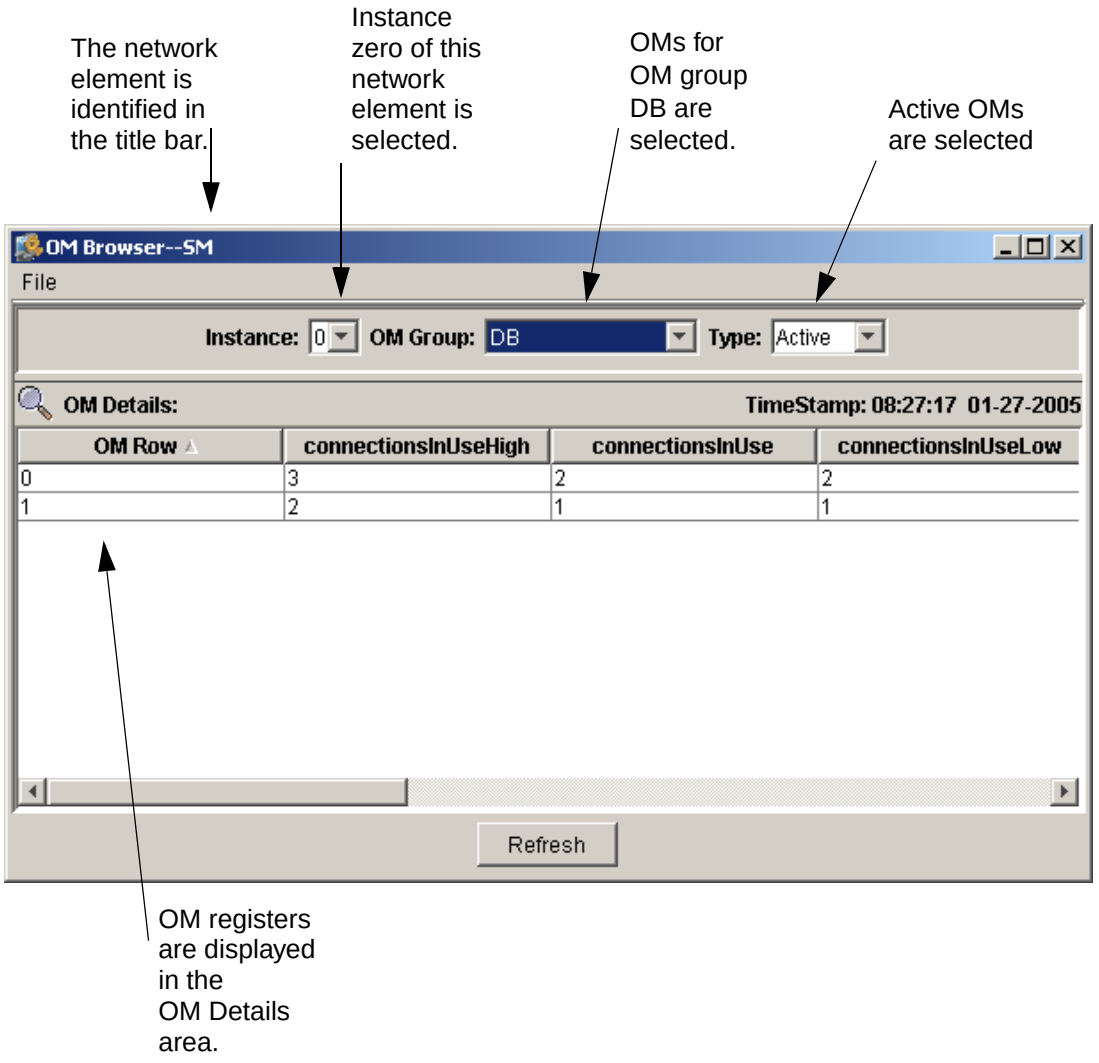
Topics in this chapter

Operational measurements browser basics

Operational measurements (OMs) provide statistical information on the server operations and performances. OMs are represented in terms of groups, which contain registers (counters and gauges) that provide performance-related data.

There are two types of OMs, active and holding. Active OMs are a snapshot of the current OMs since the interval began. Holding OMs have already been archived to files on the System Manager server.

The OM browser is used to view both active and holding OMs. The OM information displayed in a browser is for a single network element instance. The information displayed and use of the browser is essentially the same for both the active and holding browsers. The following figure shows an active OM browser.



The OM browser has two main areas, the upper panel and the OM Details area. The upper panel identifies the network element instance, the OM group displayed in the OM Details area, and if the OMs are for the active or holding period. The OM Details area displays the register information of the selected OM group. OMs for non-active services may not be reported. As a result, the OMs for a non-active group may not be displayed in the OM browser.

OMs viewed in the browsers display the following information.

Information	Description
Instance	This pull down menu indicates the instance of the network element from which the OMs were collected. If a network element has a second instance and that instance is in service, use the pull down menu to query the second instance.
OM group	This pull down menu determines the registers shown in the OM Details area.
Type	This pull down menu determines if active OMs or holding OMs are displayed in the OM Details area.
TimeStamp	If active OMs are queried, then this field indicates the time the OMs were fetched. If holding OMs are queried, this field indicates the ending time of the most recent OM collection period.
OM Row	This field is in the OM Details area and identifies a register, such as UFTP2_0:log:Standard or a tuple, such as 0 or 1.
The remaining columns in the OM Details area are specific to the OM group selected.	

OM browser operations

The OM browser can only be launched when a network element is selected in the config view, the physical view window, or the logical view window. Administrators can open multiple OM browsers at the same time to monitor separate network elements.

- Launching the OM browser from the config view
- Launching the OM browser from the physical or logical view
- Viewing register information of a specific OM group
- Saving OM data
- Refreshing data in the OM browser
- Configuring OM file rotation periods
- Configuring OM interval periods

Launching the OM browser from the config view

1. Select **Network Elements** > **<nt_type>** > **<ne>** from the config view.

   The OM browser icon becomes active in the icon toolbar.

2. Click the OM browser icon  in the toolbar.

   The OM browser for the selected network element opens. Active OMs are queried by default.

Launching the OM browser from the physical or logical view

When a network element is selected in the logical or physical view window, the OM browser icon becomes active. Click the icon to open the OM browser.

Note: If the OM browser is launched from the physical view window for a specific instance of a network element, such as SM_0, the Instance pull down menu is not available on the launched OM browser.

Viewing register information of a specific OM group

1. Select an OM group from the upper panel.

   The registers and statistics are displayed in the OM Details area.

Saving OM data

OM data cannot be saved from the OM browser. Configure an FTP Push OM Stream for the System Manager and any Fault-Performance Managers and then view the transferred data.

Refreshing data in the OM browser

OM data is updated according to the interval configured for the OfficeTransferPeriod configuration parameter. When the browser has been open for an extended period, administrators can query the latest OM data.

1. Select Active or Holding from the Type pull down menu.

2 Click **Refresh**.

The OM Details area updates.

Configuring OM file rotation periods

Administrators can configure the active OM rotation interval and file size based on a File Type profile configured at the System Management Console. Different profiles can be created and these profiles can be assigned on a network element by network element basis, or at the system level. Typically, a single profile is configured at the system level. For information on configuring File Type profiles, see the information about rotation rules in File Type on page 45.

Configuring OM interval periods

Administrators can configure the length of OM interval periods to determine if the active OM period lasts 5, 15, 30, or 60 minutes. After the configured interval, the OMs are tallied and moved to holding status, and a new active OM interval period begins. The interval is controlled by the OfficeTransferPeriod configuration parameter, and is set on a component by component bases. See the information about modifying configuration parameters in Modify Configuration Parameters on page 75.

Administrator tools

Topics in this chapter

User administration

Administrator access to the MCS system through the System Manangement Console can be added, modified and deleted. User administration procedures require an administrative role with SecurityService privilege.

Adding or modifying an administrator

Before adding an administrator, know the administrative role and password policy to apply to the new administrator.

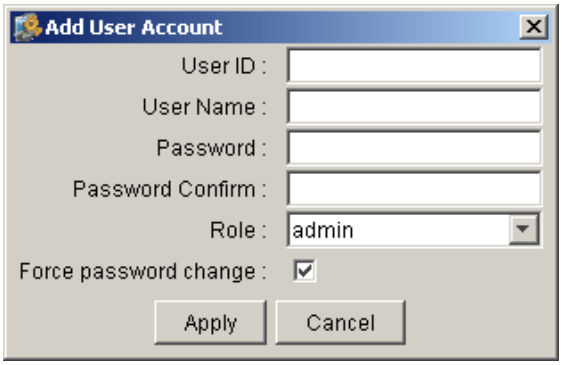
1 Select **Administration** > **User Administration** from the menu bar.

The Users window opens opens in the work area.

2 Click **Add** or select an existing entry and click **Edit**.

The User Account dialog box opens.

3 Provision the data on the User Account dialog box and click **Apply**.



The configuration data is validated. The User Account dialog box closes and the Users window is updated with the change.

Field	Value	Description
User ID	string, 5 to 16 characters	This value is the identity of the account. This value is entered during log in by the administrator. Integers are allowed, for example, admin20.
User Name	string	Use this value to record the administrator's first and last name.
Password	string, 4 to 200 characters	All characters are acceptable.
Password Confirm	string, 4 to 200 characters	
Role	pull down	Specify the administrative role for this administrator.
Force password change	enabled or disabled	If enabled, the administrator is required to change his or her password upon the initial login.

Deleting an administrator

An administrator can delete another administrator from the system. This prevents the administrator from logging in again, but does not force a logged in administrator off the system.

1. Select **Administration** > **User Administration** from the menu bar.

   The Users window opens in the work area.

2. Select the entry for the user on the User window and click **Delete**.

   A confirmation dialog opens. Confirm the dialog by clicking Yes.

Role administration

Roles are configured by administrators with SecurityService privilege, and then administrators are assigned a role.

Adding or modifying a role

If a role is modified, the effect is immediate because every maintenance or configuration action at the System Management Console initiates a privilege check against the administrator's role.

1. Select **Administration** > **Role Administration** from the menu bar.

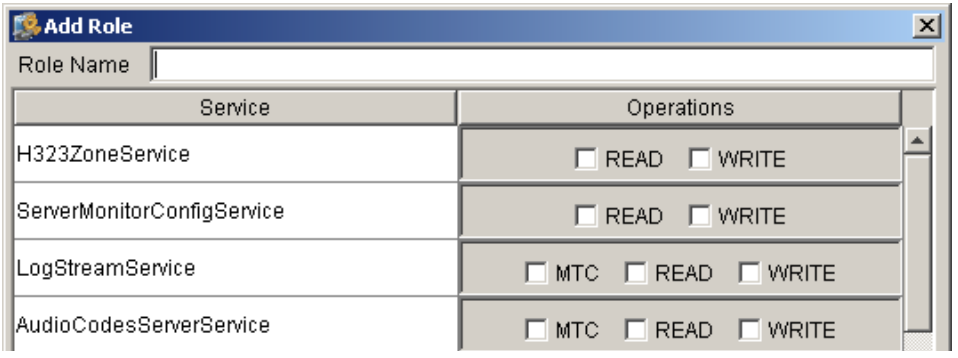
   The Roles window opens in the work area.

2. Click **Add** or select an existing entry and click **Edit**.

   The Role window opens.

3. If adding a new role, enter a Role Name.

   Configure the privileges for this role by selecting the checkboxes and click **Apply** at the bottom of the window.



The implications READ, WRITE, and MTC differs according to the type of service selected, but some generalizations are possible:

- READ — This privilege typically permits viewing configuration data, but does not allow modifying configuration data.
- WRITE — Selecting WRITE enables READ automatically. WRITE privilege allows adding and modifying configuration data.
- MTC — This privilege typically allows operations such as starting and stopping services, but does not allow changing configuration data. READ is usually needed in addition to MTC.

The privilege changes are made.

The following table list the privileges and the associated actions.

Privilege	Description
AlarmMtcService	Acknowledgement/clearing of alarms
AlarmQueryService	Alarm viewing
AMOssProfileService	OSS Profile data configuration (distributed to AM)
AudioCodesNumMapIP2TelService	IPToTelephonyMap configuration
AudioCodesServerService	AudioCodes gateway configuration
AudioCodesServerStateService	AudioCodes gateway state configuration
AudioCodesTrunkService	AudioCodes trunk configuration
AuthenticationService	SessMgr trusted node authorized method configuration
CipherSuiteService	OAMP SSL/TLS cipher suite configuration
ConfigParmService	Configuration parameters
DBInstanceService	Database instance configuration
DBMonitorConfigService	Database monitor threshold configuration
DBMonitorService	Database instance monitoring
DeviceService	IPCM device maintenance
EngParmService	Engineering parameters
ExportImportService	Bulk configuration export/import tools
FPOssProfileService	OSS profile data configuration(distributed to FPM)
GatewayService	Gateway configuration
H323DomainService	H323 domain configuration
H323EndpointService	H323 endpoint configuration and maintenance

Privilege	Description
H323ZoneService	H323 zone configuration
IPAddressService	IP address configuration
LicenseKeyService	License key configuration
LocationServiceMgr	SessMgr DNS server configuration
LogicalDBService	Database configuration
LogStreamService	Log viewing
LOMServerService	LOM server configuration
MASService	Media Application Server configuration
MediaCardService	UAS media card configuration
MediaGatewayService	UAS media gateway configuration
NEInstanceService	Network element instance configuration and maintenance
NERecordStreamService	NE log, OM and accounting format path configuration
NEService	Network element configuration
NumberQualifier	H323 gatekeeper number qualifier configuration
OMQueryService	OM viewing
OssProfileService	OSS Profile data configuration (distributed to all Element Managers)
PasswordRulesService	User password rules configuration
PhysicalServerService	Server configuration
PhysicalSiteService	Physical site configuration
RTPPortalBladeService	RTP Portal blade configuration
SecurityService	User/Role configuration and user display/forceoff capability
ServerLOMCommandService	Server maintenance for servers configured with a LOM server
ServerMonitorConfigService	Server monitor threshold configuration
ServerMonitorService	Server monitoring
SnmpProfileService	SNMP profile configuration
TrustedNodeService	Third party trusted device configuration

Deleting a role

A role cannot be deleted if a user is assigned to the role.

1. Select **Administration** > **Role Administration** from the menu bar.

   The Roles window opens in the work area.

2. Select the role to delete from the Roles window and click **Delete**.

   A confirmation dialog box opens. Click Yes to confirm. The dialog box closes.

If the role is not referenced by any users, the entry is removed from the Roles window. If the role is referenced, the deletetion is rejected and a warning dialog box opens, indicating that the entry is referenced by data of type UserData.

User display and forceoff

Administrators with SecurityService privileges can display all logged in administrators and can force an administrator off the MCS system.

1. Select **Administration** > **User Display/Forceoff** from the menu bar.

   The Logged-in Users window opens in the work area.

2. To force an administrator off the MCS system, select an entry and click **Force Off**.

   A confirmation dialog box opens. Click Yes. The entry is removed from the Logged-in Users window and the administrator is logged off.

User password rules

Administrators with PasswordRulesService privilege can configure the password complexity for logging in to the System Managment Console.

1. Select **Administration** > **User Password Rules** from the menu bar.

   The Password Complexity Rules window opens in the work area.

2 Provision the the changes and click **Apply**.

The Password Complexity Rules window closes.

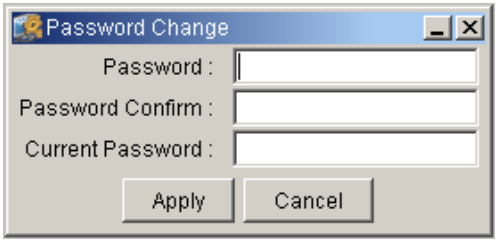
Password change

This menu item is used to change your password, while you are logged in. All administrators are able to change their own passwords. To change another administrator's password, select **Administration** > **User Administration**, select the user, and click **Edit**.

1 Select **Administration** > **Password Change** from the menu bar.

The Password Change window opens in the work area.

2 Enter your new password twice, your current password, and click **Apply**.



The entries are validated and the Password Change window closes.

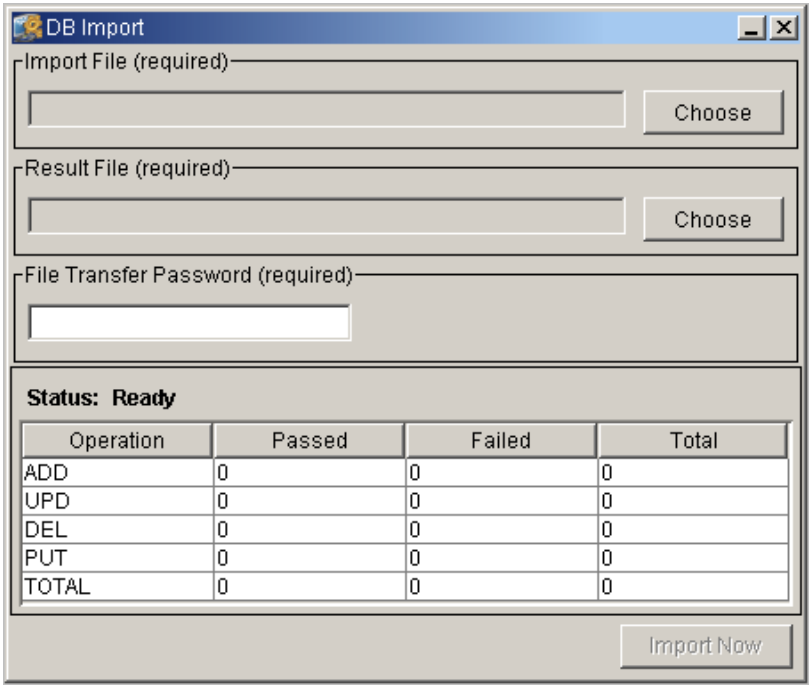
Database import

Database import is used to restore the configuration data in the database. This procedure requires an administrative role with ExportImportService privilege.

Note: The configuration data does not include the provisioning data that is entered at the Provisioning Client.

1 Select **Tools** > **DB Import** from the menu bar.

The DB Import window opens in the work area.



2 From the Import File area, click **Choose** and navigate to the location of an exported database file on the local workstation.

3 From the Result File area, click **Choose** and specify a directory and filename on the local workstation for the results of the import operation.

4 Enter the password used to connect to the System Manager with FTP.

5 Click **Import Now**.

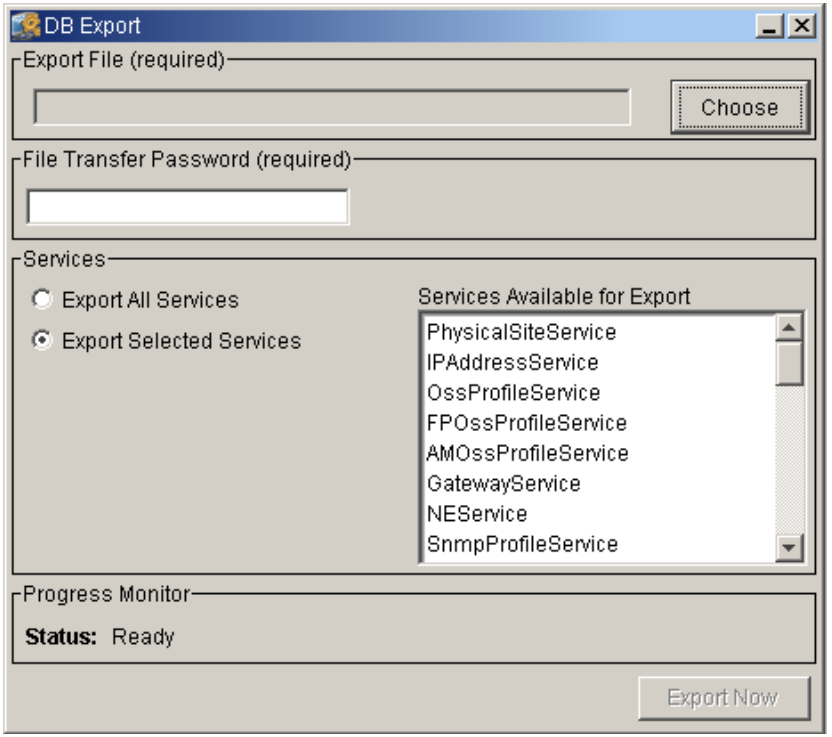
Database export

Database export is used to take a snapshot of the configuration data. This procedure requires an administrative role with ExportImportService privilege.

Note: The configuration data does not include the provisioning data that is entered at the Provisioning Client.

1 Select **Tools** > **DB Export** from the menu bar.

The DB Export window opens in the work area.



2 Click **Choose** and specify a directory and file name on the local workstation for the exported data.

3 Enter the password used to connect to the System Manager with FTP.

4 From the Services area, select Export All Services, or select Export Selected Services and choose the services from the Services Available for Export list. Hold the Ctrl key down and click to select more than one service.

5 Click **Export Now** to start the export operation.

Refresh

The Refresh tool refreshes configuration, logical and physical view windows of the System Management Console. Whenever Refresh is clicked, it queries the System Manager for the latest topology information and updates this information on the System Management Console. Refresh is not normally needed since the System Management Console updates whenever an event occurs.

1 Select **Tools** > **Refresh** or click the Refresh icon in the tool bar.

The trees in the config view and logical and physical view windows collapse. The data in these displays is updated to the latest topology information.

Logical view window

The logical view window provides a graphical view of the network elements, servers, and the logical databases. In this view, it is not possible to determine which network elements are deployed on which servers.

Launching the logical view window

1 Click the logical view window icon in the icon toolbar.  or right click on the alarm summary area.

The Logical View window opens.

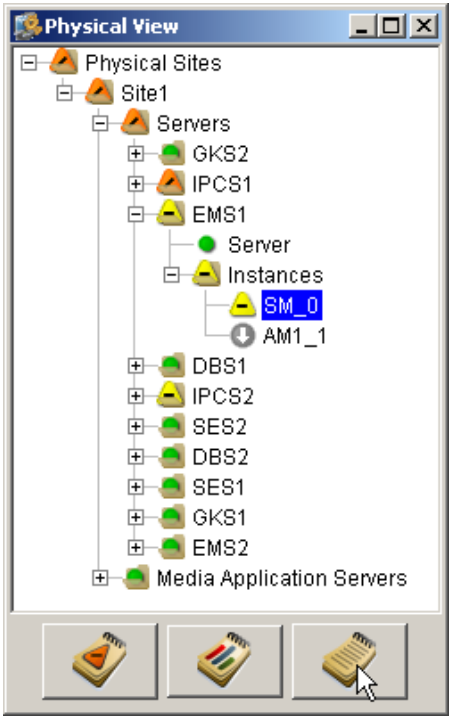
Physical view window

The physical view window provides a graphical view of the MCS system. First, elements are organized by site, server, and then the network element applications deployed on the server.

Launching the physical view window

1 Click the physical view window icon in the icon toolbar  or right click on the alarm summary area.

The Physical View window opens.



Logical and physical view icons

For both view windows, a green dot indicates the state of the network element or server is clear. A yellow, orange, or red triangle indicates an alarm. If the bar icon in the triangle is horizontal, then no alarms for that network element or server have been acknowledged. If the bar is angled, then at least one alarm has been acknowledged for that network element or server.

Unmanaged network elements and servers are identified by a grey down arrow icon. For a server, this indicates that the monitor for the server is not running. For a network element, this indicates that the network element is OFFLINE.

Message of the day

The System Management Console supports presenting administrators with a Message of the Day window upon successful login. If enabled, after successfully logging in, a window like the following opens.

To enable this feature, an administrator must log in to the System Manager server and create a file named motd.txt. This file must be located in /var/mcp/run/MCP_4.0/SM_x/data/motd.txt. Administrators should create this file with an editor like vi. If this file is not created, no Message of the Day window appears.

Note that this file is not persisted after any software upgrade or update. During a software upgrade or update, the data directory and its contents are overwritten. It also is not automatically created on the second instance of the System Manager in redundant configurations. In redundant configurations, the file must be transferred or created on the second instance.

Troubleshooting

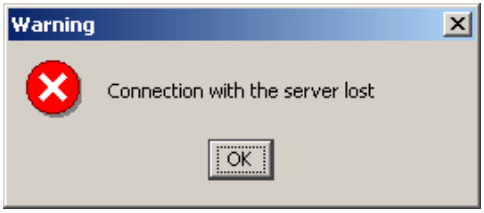
The following procedures describe troubleshooting and resolving some known System Management Console issues:

- System Management Console connection is lost
- System Management Console fails to start

System Management Console connection is lost

When the connection between the System Manager and System Management Console is lost, the following dialog box appears on the administrator's workstation screen.

Figure 1 Connection lost dialog box



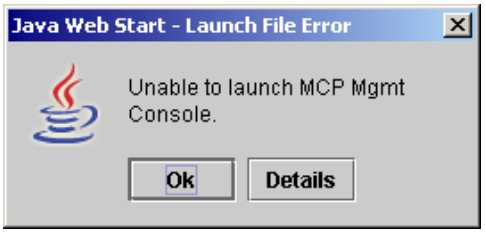
The lost connection may be a network or connection related problem, or an indication that the System Manager or its hosting server has failed. Perform basic troubleshooting to determine if the fault is a network or connection related problem.

If the problem is the result of a failed System Manager or it's hosting server, administrators can manually failover the System Manager operations to the secondary System Manager. Once the secondary System Manager is operational, a System Management Console connection can be re-established.

For more information on the failover procedure, refer to *System Manager Basics*.

System Management Console fails to start

If the System Management Console fails to start such as indicated in the following figure, and the problem is related to having different version of a Java Runtime Environment installed on the workstation, perform the following procedure.



1. Start Java Web Start by selecting **Start** > **Programs** > **Java Web Start** > **Java Web Start**.

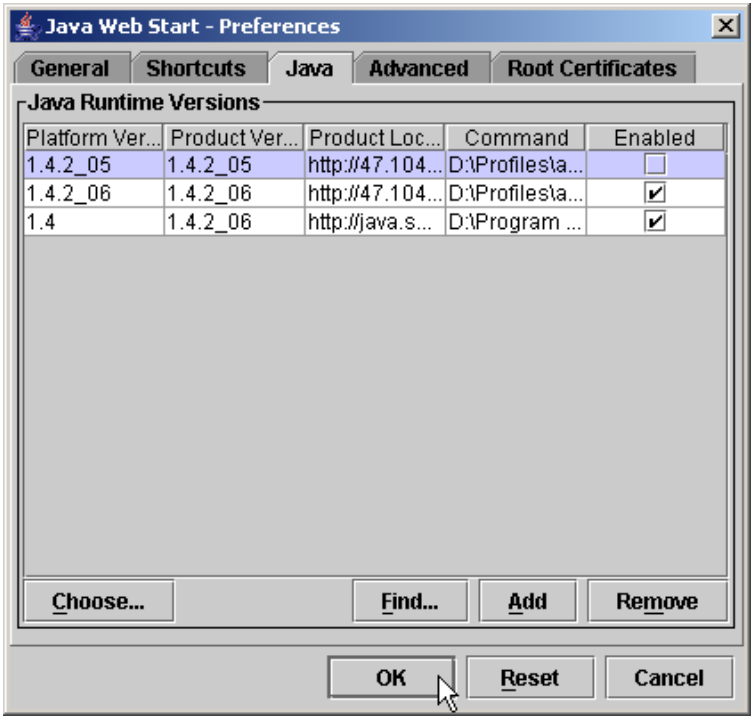
   A splash screen appears and closes. The Java Web Start Application Manager window opens.

2. Select **File** > **Preferences**.

   The Java Web Start - Preferences window opens.

3. Click the **Java** tab.

The list of installed Java Runtime Environments is listed.



4 Disable or remove older versions of the Java Runtime Environment that are not needed and click **OK**.

In the figure above, Java Runtime Environment version 1.4.2_05 is disabled by deselecting the Enabled checkbox.