[Standard—Nortel Confidential]

(I)SN07
Part No. NN10370-111
December 2004

Carrier Voice over IP System Management Console User Guide

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, and i2004 Internet Telephone are trademarks of Nortel Networks.

Microsoft, Windows, Windows NT, Internet Explorer and Outlook are trademarks of Microsoft Corporation.

Netscape is a trademark of Netscape Communications Corporation.

The asterisk after a name denotes a trademarked item.

Contents

About this guide

Overview

This guide provides system administrators with instructions on using the System Management Console. The System Management Console is used to configure, monitor, and manage the following CVoIP component software and their hosting servers:

- RTP Media Portal
- Database Module
- Management Module
- Oracle Monitor

Audience

This guide is intended for administrators using the System Management Console to manage the CVoIP 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 Management Module Basic*

<**ElementName**>	Indicates a configured element name in the system tree Example: <ApplicationServerName>
separator >	Indicates a menu path Example: **Configuration** > **Query**

Acronyms

This guide uses the following acronyms:

BPS	Business Policy Switch
GIA	general information area
GUI	graphical user interface
IP	Internet Protocol
IPCM	IP Client Manager
MB	mega-byte
MCS	Multimedia Communications Server
MCP	Multimedia Communications Portfolio
MgmtSite	management site
MgmtSvr	management server
MO	managed object
OAM	operations, administration, maintenance
OEM	Oracle Enterprise Manager
OM	operational measurement
PC	personal computer
PRI	primary route interface
RAM	random access memory
RTP	Real-Time Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SysMgr	Management Module component

UAS	Universal Audio Server
UFTP	UNIStim File Transfer Protocol
URL	universal resource locator (internet address)
XML	EXtensible Markup Language

Related publications

The System Management Console interacts with CVoIP system hardware and software components via the Management Module. 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 documents

Document	Part no.
CVoIP Management Module Basics	NN10369-111
CVoIP Database Module Basics	NN10368-111
CVoIP RTP Media Portal Basics	NN10367-111

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 element manager (Management Module) 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 service components
- deploying and configuring system sites, servers, components, and component services
- monitoring system using alarms, logs, and performance measurements
- managing collection of operations, administration, and maintenance information

System Management Console installation

The System Management Console is installed on administrator workstations during system deployment. The Management Module needs to be deployed and operational before administrators can connect with the System Management Console.

See the following topics for more information:

System requirements

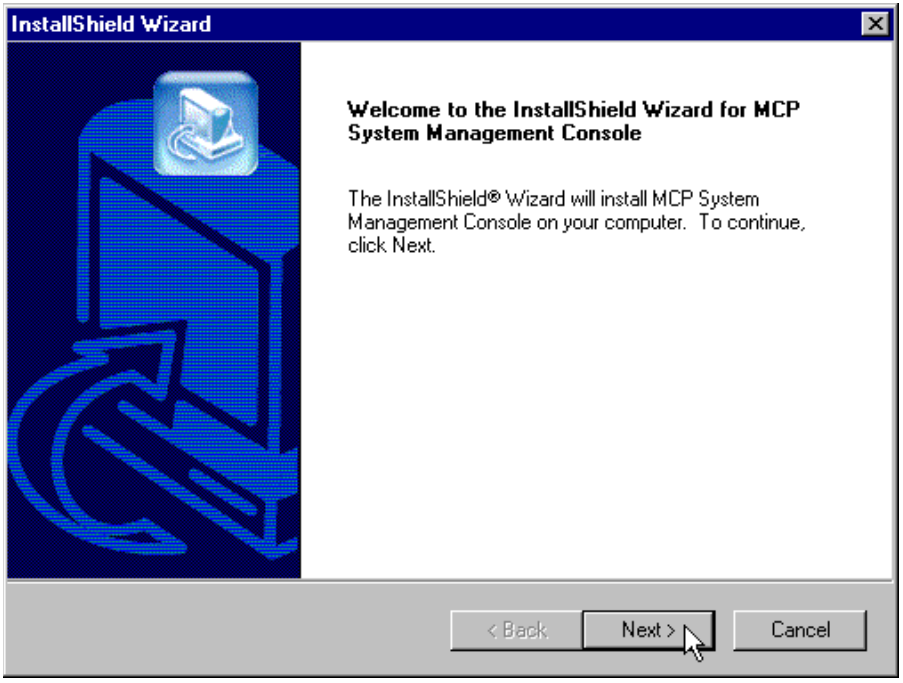
Nortel Networks recommends the workstation meets the following hardware requirements:

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 (If the console is installed on a drive other than drive C, then 50 MB of free space is required on that drive as well. In this case, the free 50 MB on drive C will not be used.)	50 MB (If the console is installed on a drive other than drive C, then 50 MB of free space is required on that drive as well. In this case, the free 50 MB on drive C will not be used.)
CD ROM drive	Optional (Only required if CD is the mechanism for installing the Management Console.)	Optional (Only required if CD is the mechanism for installing the Management Console.)
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.)
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 software installation CD is number seven of the IMSC0002 package of installation CDs. The name of the installation software is called *Multimedia Communications Platform Management Console* (MCPMC).

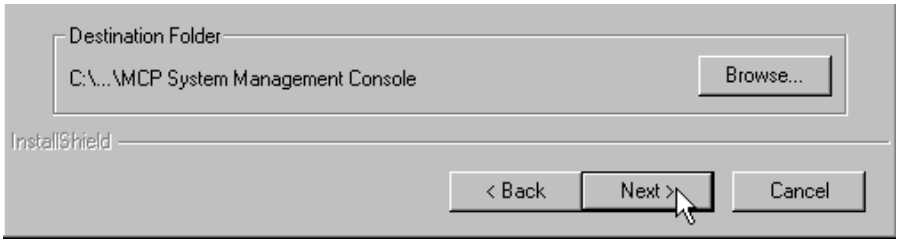
1 On the administrator's workstation, run the **mcpmc_setup.exe** file from the System Management Console installation CD. This launches the installation wizard. Click **Next**.



2 Optionally assign a destination directory for the System Management Console program files. By default, the program files are installed to the following directory on the C: drive of the workstation:

C: /Program Files/Nortel Networks/MCP System Management Console

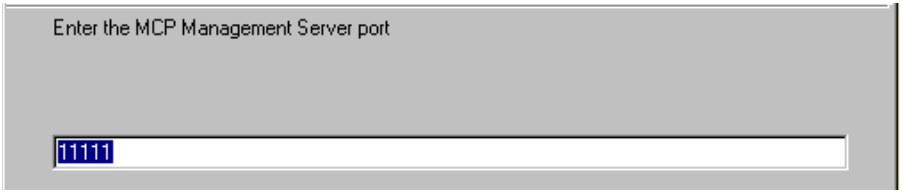
Click **Next**.



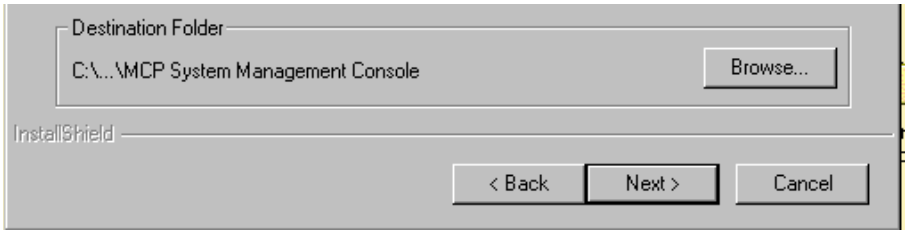
Note: During the installation of the System Management Console, the user can install the console to any valid drive. However, the install shield itself (the software performing the install) loads onto the C: drive. The install shield only loads when 50 MB of free disk space is available on the C: drive (regardless of the drive the Management Console is actually being installed onto).

3 Enter the logical IP address of the Management Module component. Click **Next**.

4 Leave the port at the default 11111. Click **Next**.



5 Optionally assign the file location and name used for saving formats and filters.Click **Next**.



6 The Start Copying Files dialog box opens. Click **Next**.

7 The Setup Status dialog box opens. Once installation is complete, the Installation successfully completed dialog box launches. Click **OK**.

By default, program files are installed to the following directory, unless configured to a different location during step 2:

C: /Program Files/Nortel Networks/MCP System Management Console

Uninstalling the System Management Console

Use the following procedure to uninstall the System Management Console:

1 On the workstation select **Start** > **Programs** > **MCP** > **Console UnInstaller**

Figure 1 Launching the Console UnInstaller

The uninstall wizard launches and removes the System Management Console and its related program files from the workstation.

Updating the System Management Console

The System Management Console version should correspond to the load version being installed. Administrators can view their current System Management Console version by selecting **Help** > **About MCP System Management Console**. Before deploying software upgrades, the administrator should upgrade the System Management Console to the equivalent version.

Only one version of the System Management Console is allowed on a workstation. When installing a new version of the System Management Console, the installation wizard checks for existing versions. If a version already exists on the workstation, the administrator is prompted to uninstall the current version.

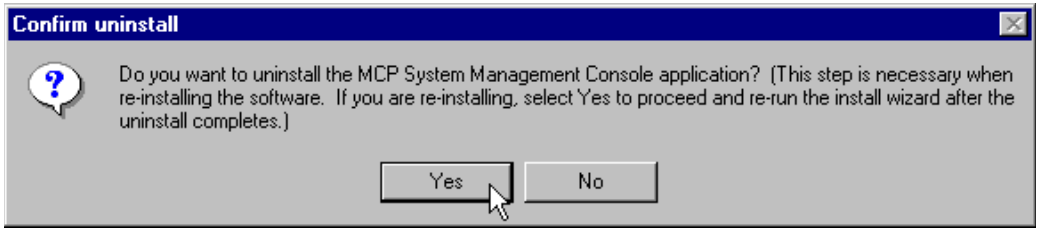
1. On the administrator's workstation, run the **mcpmc_setup.exe** file for the upgraded System Management Console.

   The installation wizard launches.

2. The installation wizard will find the existing System Management Console. The following confirmation box prompts the administrator to uninstall the existing version.

   Click **Yes**.

Figure 2 Prompt to confirm the Uninstall of an existing version



3. When the uninstall process begins the administrator is prompted to confirm the file deletion. Click **OK**.

   A confirmation box indicates when the uninstall is complete.

4. Run the **mcpmc_setup.exe** file for the new System Management Console again.

   The install wizard will launch again, and restart the installation of the new System Management Console. The server IP addresses used by the uninstalled System Management Console are preserved and will appear in the server field of the new Console's login dialog box.

Note: There is a known issue with the System Management Console not uninstalling correctly on some workstations. If this occurs, the prompt described in step 2 will open each time you try to run the mcpmc_setup.exe file. See the Troubleshooting section for information on resolving this problem.

System Management Console login

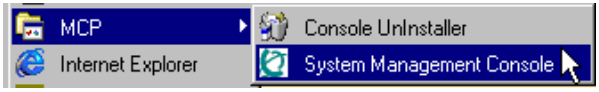
Logging onto the System Management Console requires a username and password. Username and passwords are provisioned using a database script. Please refer to *CVoIP Database Module Basics* for more information.

Logging onto the System Management Console

Use the following procedure to log onto the System Management Console.

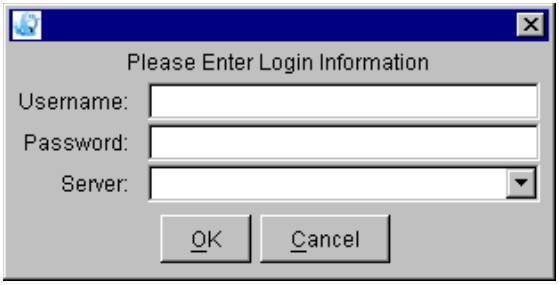
1 From the workstation, select **Start** > **Programs** > **MCP** > **System Management Console**.

Figure 3 Launching System Management Console



The login dialog box opens.

Figure 4 System Management Console Login dialog box



2 Enter the required login information.

User name:	the username of the administrator
Password:	the administrator's password
Server:	the logical IP address of the Management Module component

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.

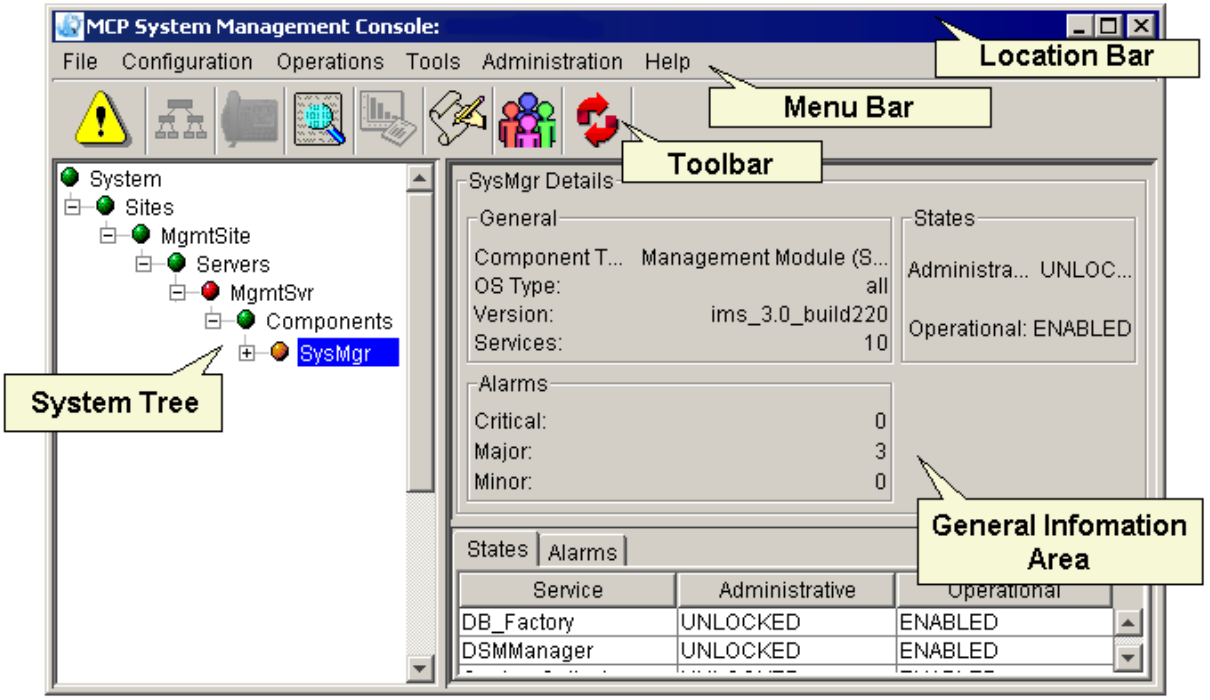
Navigating the System Management Console

Topics in this chapter

System Management Console GUI layout

The System Management Console GUI 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 tool bar. Under those are the system tree in the left panel, and the general information area in the right panel.

Figure 5 System Management Console

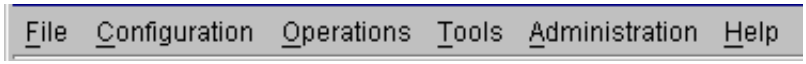


Menu bar

The menu bar accesses all the options available in the System Management Console. Not all menu options are available for every component or server. Unavailable menu options are grayed out.

Menu options are discussed in this guide with the related procedures.

Figure 6 System Management Console menu bar



Tip: You can access all the available menu options for an element selected in the system tree by right-clicking the mouse, opening the shortcut menu.

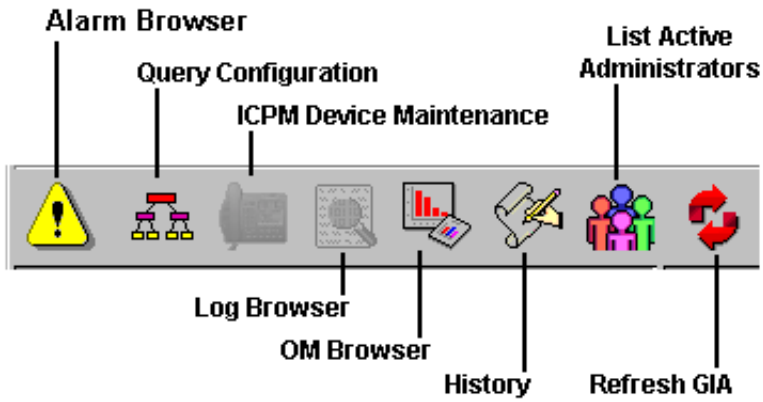
Toolbar

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 system tree.

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

Note: The IPCM device Maintenance icon is not supported in the CVoIP deployment.

Figure 7 System Management Console toolbar icons

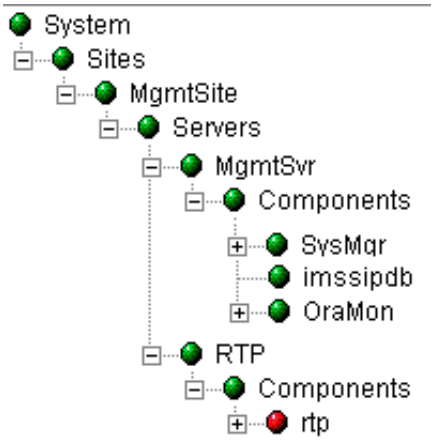


Tip: You can separate the Toolbar from the Console by dragging and dropping the Toolbar onto the desktop. When you want to re-incorporate the toolbar back on the System Management Console, click the close button on the separated toolbar.

System tree

The system tree displays all the configured sites, servers, services, and service components. Users can collapse and expand the tree structure as required. The initial system installation adds the management site (MgmtSite), management server (MgmtSrv), and Management Module (SysMgr) by default.

Figure 8 System tree



The color of the system tree nodes indicate the alarm status of the displayed network elements. When collapsed, the color shown is that of the most severe alarm being generated by an element in the collapsed portion of the tree. The alarm color codes are:

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

For alarm details, refer to the component documents.

General information area

The general information area (GIA) of the System Management Console provides the current details of the element selected in the system tree. The system tree logical nodes (Sites, Servers and Components) have no associated displays.

Depending on the element selected in the system tree, the GIA displays the following:

- number of system components associated with the selected system element
- component software versions
- number of current critical, major, and minor alarms
- server usage statistics
- operational state

A description of the displayed GIA information is discussed with the respective system tree level in the subsequent chapters.

Clicking the **Refresh** icon on the toolbar updates the information in the GIA.

System level configuration and management

Topics in this chapter

System level configuration and management overview

System is the root node of the system tree. All other network elements managed by the System Management Console fall under this node. The configuration and management operations performed at the system level apply to all the managed elements that comprise the system.

Use the General Information Area (GIA) to view system level information. See the section System level information in the GIA for more information.

System level information in the GIA

When an administrator selects **System** in the system tree, the GIA displays the following system level information:

- General

  Sites: the total number of sites

  Servers: the total number of servers for all sites

- Highest Usage

  CPU: server, identified by site, with the highest percentage CPU usage

  Disk: server, identified by site, with the highest percentage disk usage

I/O: server, identified by site, handling the highest number of packets

Memory: server, identified by site, using the highest percentage of memory

- Alarms

  Critical: total numbers of current critical alarms across the system

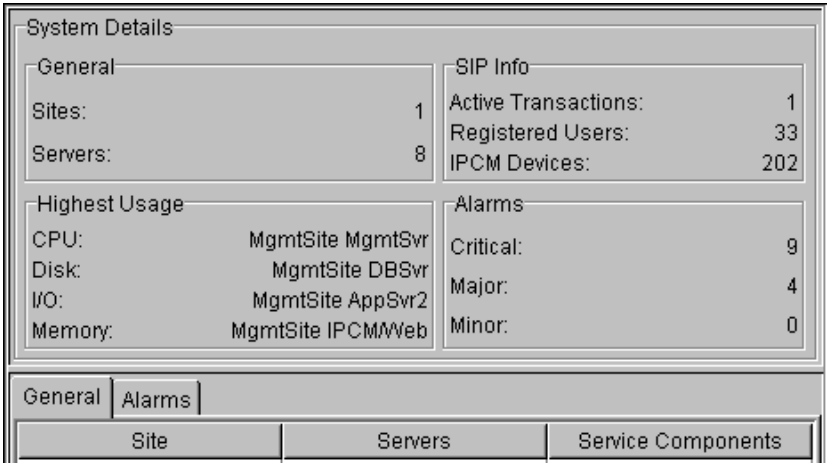
  Major: total number of current major alarms across the system

  Minor: total number of current minor alarms across the system

- SIP information

  Not supported or applicable to CVoIP solution deployments.

Figure 9 GIA display when System is selected



SNMP manager administration

Network administrators can integrate alarms generated by CVoIP managed objects into their current Network Management Layer (NML) manager.

Alarm generating events report to the SNMP (Simple Network Management Protocol) manager registered with the system.

See the following procedures for more information:

- Adding an SNMP Manager
- Removing an SNMP Manager
- Updating an SNMP Trap portt

Adding an SNMP Manager

Use the following procedure to add an SNMP Manager and start forwarding traps to an existing Network Management Layer (NML) manager.

1. Select the **System** logical node in the system tree.
2. From the menu bar, select **Administration** > **Administer SNMP MGR** > **Add SNMP Manager**

   The AddSNMPMgr dialog box opens.

Figure 10 AddSNMPMgr dialog box

3. Enter the configuration information.

Configuration field	Description
SNMP Mgr IP Address	IP address of the SNMP manager.
SNMP Community String	Read only SNMP community string (6-20 characters)

4. Click **Apply**

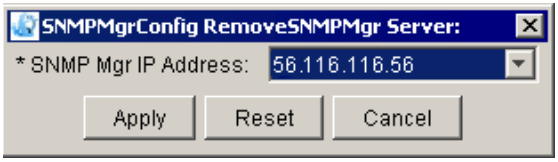
Removing an SNMP Manager

Use the following procedure to remove an SNMP Manager and stop forwarding traps to an existing Network Management Layer (NML) manager.

1. Select the **System** logical node in the system tree.
2. From the menu bar, select **Administration** > **Administer SNMP MGR** > **Remove SNMP Manager**.

   The RemoveSNMPMgr dialog box opens.

Figure 11 RemoveSNMPMgr dialog box



3. Select the IP address of the SNMP manager being dropped from the drop down list.
4. Click **Apply**.

Updating an SNMP Trap port

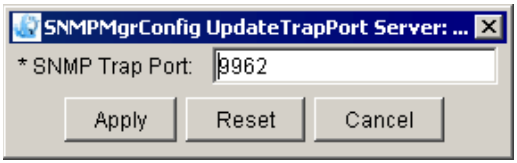
Each hardware platform may contain several SNMP agents, each using a different port. The management server's (MgmtSvr) default trap port is 9962 but it can be set to other values. The SysMgr polls each server in the network at port 161 to get the CPU and I/O usage, but does not listen on port 161. Each server listens on port 161 for the SNMP requests.

Use the following procedure to update the destination port on the NML manager that receives MCS traps.

1. Select the **System** logical node in the system tree.
2. From the menu bar, select **Administration** > **Administer SNMP MGR** > **Update SNMP Trap Port**.

   The UpdateTrapPort dialog box opens, displaying the current port number.

Figure 12 UpdateTrapPort dialog box



3 Change the port number to the new value.

4 Click **Apply**.

License key management

A valid license key is required before the user can perform any OAM operations from the System Management Console. When an administrator begins a Management Console session, the database is queried for a license key. If a valid license key exists in the database, then "normal" login processing continues and the System tree is displayed on the System Management Console.

If a valid key is not in the database, the system administrator is prompted to enter a key before the system definition is sent to the System Management Console.

See the following procedures for more information:

- Adding a license key
- Updating a license key
- Querying a license key

Adding a license key

All the elements managed by System Management Console use a single license key. Keycodes within the key define the capabilities of the deployment. Typically, a license key is added during the initial system deployment, and during system updates. The inputted key is valid for all the administrators using the System Management Console.

The License Key file contains header information defining; who and when the License Key was generated, the applicable software release, and comment information.

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.

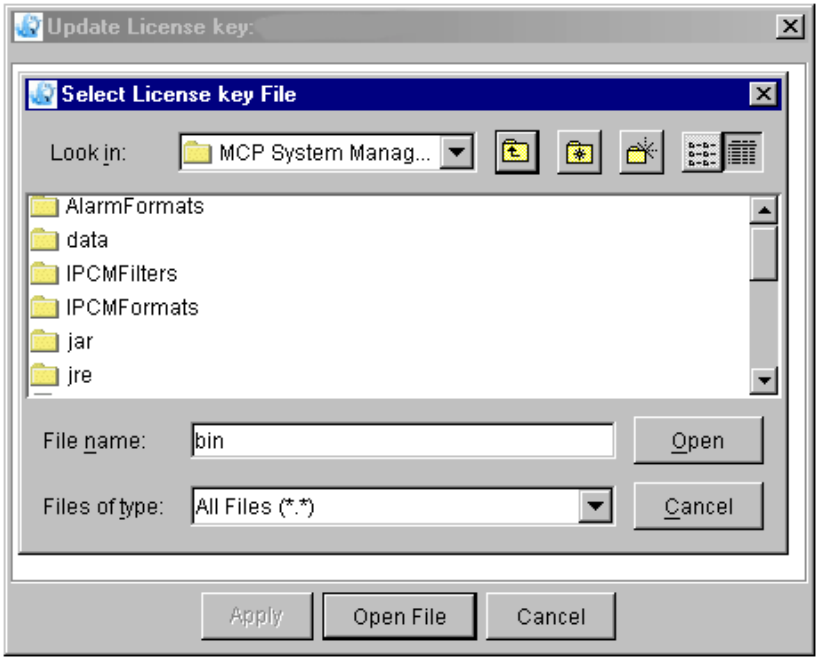
Updates to a license key can only increase system capabilities. For example, licenses can be updated to allow capabilities for more subscribers, not fewer.

Administrators update license keys using the **License Key** > **Update** menu option 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 From the menu bar, select **Administration** > **License Key** > **Update**.

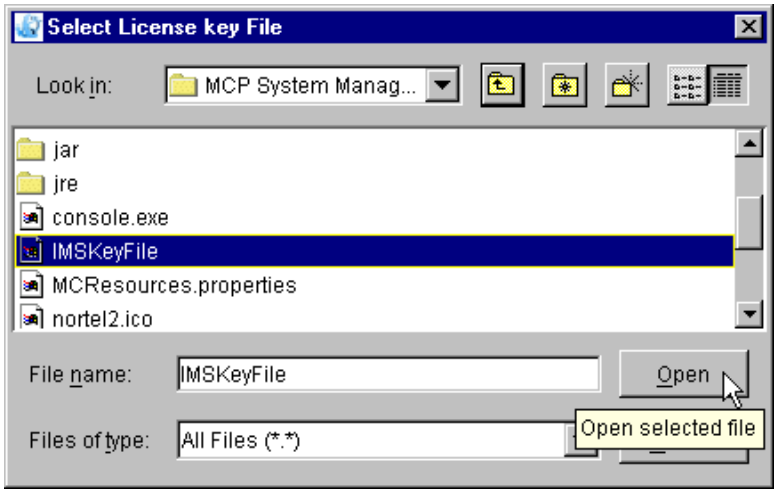
The Update License key and Select License key File dialog box opens.

Figure 13 Update License key and Select Key File dialog boxes



2 In the Select License key File dialog box, navigate to the keyfile on the workstation. Select the keyfile and click **Open**.

Figure 14 Select License Key File dialog box



The license key displays in the Update License key dialog box text area.

3 In the Update License key dialog box, click **Apply.**

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

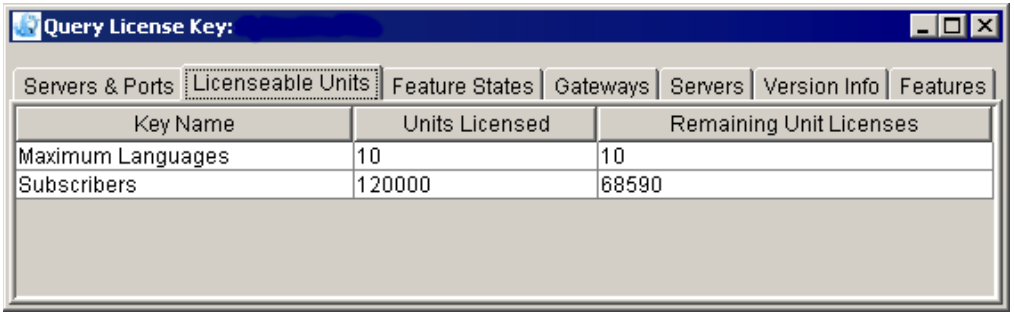
Administrators query license keys using the **License Key** > **Query** menu option of the System Management Console. The parameters displayed in the fields will depend on the license key.

1 Select the **System** node in the system tree.

2 From the menu, Select **Administration** > **License Key** > **Query**

The Query License key dialog box opens. The key cannot be modified in this dialog box.

Figure 15 Query License Key dialog box



OAM file configuration

System OAM information includes logs and operational measurement (OM). Logs and OMs generated by the managed elements are stored in files on the server hosting the Management Module, and viewed in the log and OM browsers of the System Management Console.

The OAM file rotation and retention properties are configurable. OAM file retention is only configured at the system level. OAM file rotation properties can be configured on the system level, on a server by server basis, or a component by component basis. Typically, rotation properties are configured at the system level.

See the following procedures for more information:

- Configuring the OAM file retention periods
- Configuring OAM file rotation properties

Logs and OMs are described in the component guides.

Configuring the OAM file retention periods

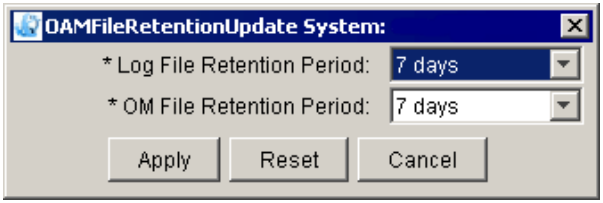
The OAM file retention period defines the time the archived log files and holding OM files are retained by the Management Module. OAM files older than the configured retention period are permanently deleted. Files can be saved to a workstation using the browsers, or pulled from the server directory using FTP.

Note: The OAM File Retention configuration dialog box locks the System Management Console until the dialog box is closed.

1. Select the **System** node in the system tree.
2. From the menu bar, select **Administration** > **Configure OAM File Retention Period**

   The OAM File Retention Period configuration dialog box opens.

Figure 16 OAM File Retention Period configuration dialog box



3. Select the number of days to retain Log and OM files from the drop-down menu. The retention period can range from 1 to 7 days.
4. Click **Apply**.

Configuring OAM file rotation properties

Administrators can configure the report scan interval and file size on a component by component basis or at the system level. Typically, OAM file rotation parameters are configured at a system level.

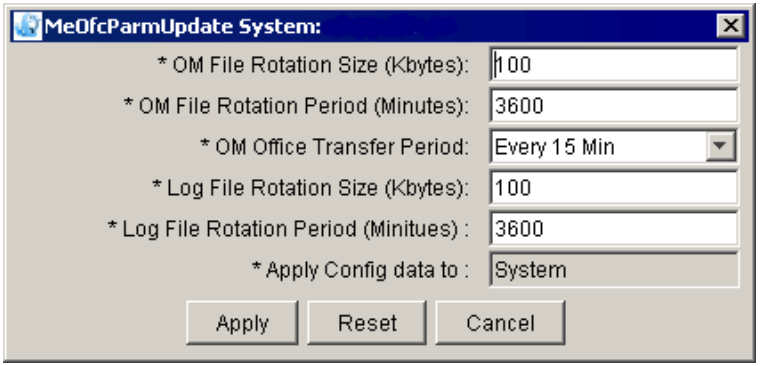
Note: The OAM configuration dialog box locks the System Management Console until the dialog box is closed.

1. Select a **System** node in the system tree.

2 In the menu bar, select **Administration** > **OAM Configuration**

The OAM Configuration dialog box opens.

Figure 17 OAM Configuration dialog box



3 Configure the OAM file parameters.

Table 2 OAM file configuration fields

Field	Description
OM File Rotation size:	Sets the maximum file size, in Kilobytes, for the active OM. If the file reaches the configured size, it is rotated to the holding OM directory, even if there is time left in the rotation period.
OM File Rotation Period:	Sets the time period, in minutes, the OM data is kept in the active browser.
OM Office Transfer Period:	Sets the OM scan cycle interval.
Log File Rotation size:	Sets the maximum file size, in Kilobytes, for current logs. If the file reaches the configured size, it is rotated to the archived logs directory, even if there is time left in the rotation period.
Log File Rotation Period:	Sets the time period, in minutes, the log data is kept in the current Log browser.
Apply Config data to:	Allows administrators to apply the configuration to only the selected component or all components hosted on the server. When configuring OAM file rotation parameters at the system level this field is grayed out.

4 Click **Apply**.

Site configuration and management

Topics in this chapter

Site level configuration and management overview

Each system is composed of one or more sites. A site is purely a logical grouping of servers and the service components being hosted. Administrators can configure any set of sites they deem appropriate for their system, and group servers into those sites.

The management site is added during the initial deployment. Other sites can be added once the System Management Console is operational.

Use the General Information Area (GIA) to view site level information. See the section Site level information in the GIA for more information.

Site level information in the GIA

When an administrator selects a site in the system tree, the GIA displays the following site level information:

- General

  Servers: the total number of servers on the site

  Components: total number of components deployed on the site

- Highest Usage

  CPU: site server with the highest percentage CPU usage

Disk: site server with the highest percentage disk usage

I/O: site server handling the highest number of packets

Memory: site server using the highest percentage of memory

- Alarms

  Critical: total numbers of current critical alarms generated by the site components

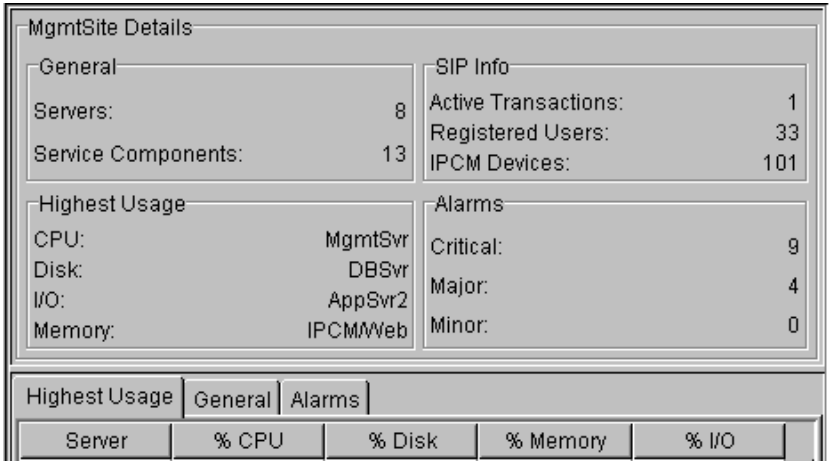
  Major: total number of current major alarms generated by the site components

  Minor: total number of current minor alarms generated by the site components

- SIP information (for sites with Application and IPCM modules)

  Not supported or applicable to CVoIP solution deployments.

GIA display when a site is selected



Site configuration

Refer to the following procedures for information on site configuration:

- Adding a site
- Querying a site’s configuration

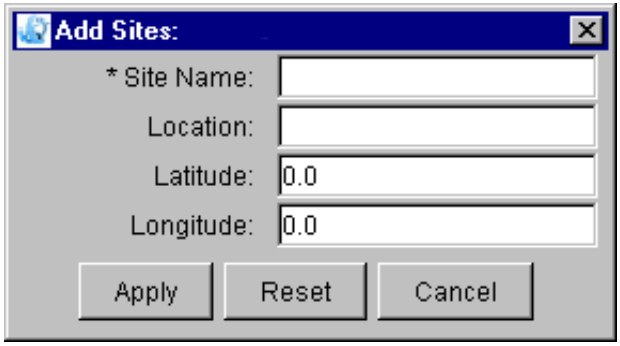
- Modifying a site's configuration
- Deleting a site

Adding a site

The following procedure describes how to add a site:

1. Select **Sites** from the system tree.
2. Right-click and select **Add** from the shortcut menu.

   The following site configuration dialog box appears. Property fields that require configuration values are indicated with an * in front of the property name.



3. Enter the required properties and select **Apply**. Use the **Reset** button to return the property fields to their defaults.

Site name	alphanumeric (1-20 characters)	A unique name identifying the site
Location	alphanumeric (1-20 characters)	Geographic location of this server
Latitude	(default is 0.0)	Latitude of server
Longitude	(default is 0.0)	Longitude of server

Querying a site's configuration

Administrators can query a site to see the current configuration values. All the property fields are grayed out and cannot be changed.

1. Select the site in the system tree.
2. Right-click and select **Query** from the shortcut menu.

   The site configuration dialog box launches.

Modifying a site's configuration

The configured properties of all sites but the management site can be modified. Modifying a site's properties is non-service affecting. Property fields that cannot be modified are grayed out.

1. Select the site in the system tree.
2. Right-click and select **Modify** from the shortcut menu.

   The site configuration dialog box opens.
3. Modify the desired properties and select **Apply**. Use the **Reset** button to return the property fields to their premodified values.

Deleting a site

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

1. Select the site in the system tree.
2. Right-click and select **Delete** from the shortcut menu.

   The Confirm deletion prompt opens.
3. Confirm the delete. Click **Yes**.

Server 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.

There are four server type options available: general, media, BPS, and AudioCodes Gateway. For CVoIP solution deployments, only general type servers are applicable.

Use the General Information Area (GIA) to view site level information. See the section Server level information in the GIA for more information.

Server level information in the GIA

When an administrator selects a server in the system tree, the GIA displays the following server level information:

- General

  Type: the server type (media, general, BPSswitch, AudioCodes Gateway)

Service components: total number of service components hosted on the server

Memory Usage: percentage of server memory in use

System Uptime: length of server uptime in hours

- CPU Usage

  Percentage of CPU usage: Servers with multiple CPUs list usage for each CPU

- Disk Usage

  Percentage of disk usage: Servers with multiple disks list usage for each disk

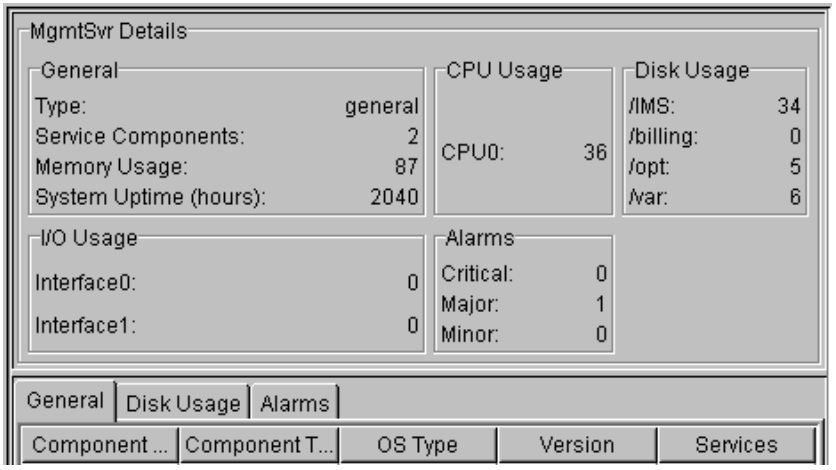
- Alarms

  Critical: total number of current critical alarms generated by the server components

  Major: total number of current major alarms generated by the server components

  Minor: total number of current minor alarms generated by the server components

Figure 18 GIA display when a server is selected



Server Configuration

See the following procedures for information on configuring servers:

- Adding a general server
- Querying a server configuration
- Modifying a server configuration
- Deleting a server

Adding a general server

General servers host the Management, Database, and RTP media portal. General type servers run Sun or Linux operating systems.

Note: The Add server configuration panel locks the System Management Console until the panel is closed. To view the query panel of an existing server while adding or modifying, open the query panel before opening the add server panel.

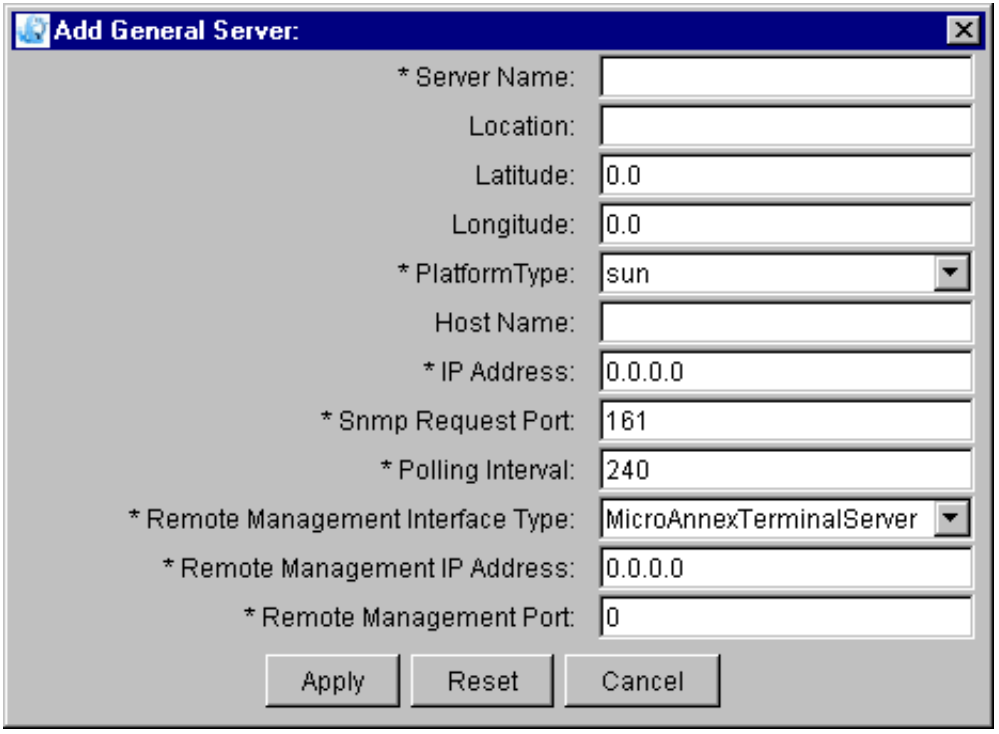
Use the following procedure to add a general type server:

1 Select the **Servers** node in the system tree.

2 From the menu bar, select **Configuration** > **Add** > **General**

The Add General Server dialog box opens.

Figure 19 General server configuration dialog box



3 Enter the configuration values. Properties that require configuration values are indicated with a * in front of the property name in the configuration dialog box.

Table 3 General server configuration properties

Property field	Format [default]	Description [range]
Server Name	alphanumeric [n/a]	A unique name identifying the server [1-20 characters].
Location	alphanumeric [n/a]	Geographic location of this server [1-20 characters].
Latitude	[0.0]	Geographical latitude [n/a].

Table 3 General server configuration properties

Property field	Format [default]	Description [range]
Longitude	[0.0]	Geographical longitude [n/a].
Platform Type	Server OS [sun]	Indicates the type of server being added [sun, linux].
Host Name	alphanumeric [n/a]	Host Name of the server machine. The host name of the server is configured during the installation and commissioning of the server. This field has to match exactly the host name configured on the server for LOM commands sent from the System Management Console to be allowed.
IP Address	IP address [0.0.0.0]	Physical IP address of the server.
Snmp Request Port	Integer [161]	Server port on which the SNMP agent is running. This is the port on the server where the SNMP daemon listens for SNMP requests [0-65536].
Polling Interval	Integer [240]	Indicates how frequently, in seconds, the server is polled for SNMP updates [240-1800].
Remote Management Interface Type	drop down menu [MicroAnnexTerminalServer]	The type of Lights out Management (LOM) interface [ITouchTerminalServer, MicroAnnexTerminalServer, EthernetInterface]. A terminal server is used for remote access.
Remote Management IP Address	IP address [0.0.0.0]	IP Address of Remote Management interface used to access this server [0.0.0.0]. I BFN x.x.x.x[(Blade_number0] An IP address of 0.0.0.0 tells the Management Module no terminal server exists for this system; therefore, no attempt to connect to the terminal server occurs.
Remote Management Port	Integer [0]	The LOM interface port this server is connected to [0-65536].

4 Click **Apply**.

Querying a server configuration

Administrators can query a server configuration. The procedure is the same for all four server types. The property fields are grayed out, and cannot be modified.

1 Select the <**ServerName>** server in the system tree.

2 From the menu bar, select **Configuration** > **Query**

The Query <ServerName> dialog box opens. The dialog box fields are the same as in the add server dialog boxes.

Modifying a server configuration

Once a server is operational, administrators can modify the configuration properties for servers. The procedure is the same for all four server types. The property fields that cannot be modified are grayed out.

Modifying the server configuration fields is not service affecting.

Note: The Modify server configuration dialog box locks the System Management Console until the dialog box is closed. To view the query dialog box of an existing server while adding or modifying, open the query dialog box before opening the add server dialog box.

1. Select the <**ServerName**> server in the system tree.
2. From the menu bar, select **Configuration** > **Modify**

   The server configuration dialog box launches.
3. Modify the server configuration properties.
4. Click **Apply**. Use the **Reset** button to return the property fields to their premodified values.

Deleting a server

Administrators must delete all the hosted components before deleting the server.

1. Select the <**ServerName**> server in the system tree.
2. From the menu bar, select **Configuration** > **Delete**

   The confirm Delete server dialog box opens.
3. Verify the deletion. Click **Yes**.

Server SNMP community string

The read-only community string of the internal and external SNMP agents of the CVoIP network components can be configured on a server by server basis. The value set for the server's community string is applied to all the SNMP agents running on the server.

See the procedure Modifying a server's SNMP community string for more information.

Modifying a server's SNMP community string

The default SNMP community string value is set to **public**. Use the Modify SNMP Community String function to change the default to some other value.

1. Select the <**ServerName**> server in the system tree.
2. From the menu bar, select **Administration** > **Modify SNMP Community String**

   The Modify SNMP Community String dialog box opens.

Figure 20 Modify SNMP Community String dialog box

3. Modify the SNMP community string value. The value can be between 6 to 20 characters.
4. Click **Apply**.

   All the SNMP agents residing on the server will restart and use the new read-only community string value.

Server base software

Base software is deployed from the System Management Console. Once deployed, base software is not monitored by the Management Module. Base software does not require configuration.

Refer to the component documents for any base software requirements for the individual components.

See the procedure Adding Base software to a server for more information.

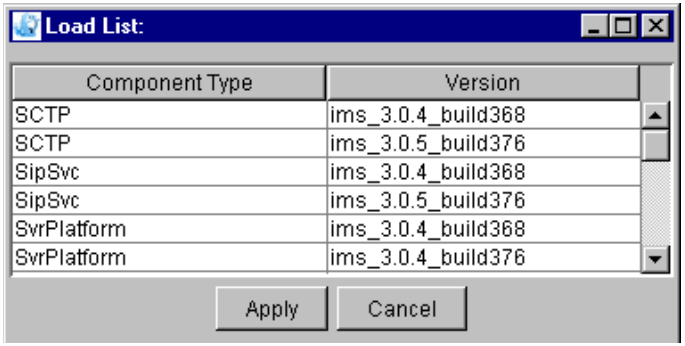
Adding Base software to a server

Refer to the component documents for the base software requirements for the individual components.

1. Select the **Components** node of the <**ServerName**> server to host the software.
2. From the menu, **Configuration** > **Add** > **BaseSoftware**.

   The Base Software load list dialog box opens. The listed component types and versions can be sorted by clicking on a column header.

Figure 21 Base software load list dialog box



3. Select the base software version to install.
4. Click **Apply**.

   The software is deployed to the server. Base software does not require configuration.

Server operations and maintenance

Administrators use **Power On**, **Power Off**, and **Reset** operations on servers. These commands are out-of-band commands which allow an administrator at the System Management Console to Start/Stop/Restart a server remotely.

These operations are only available for Sun servers that support Lights Out Management (LOM). Sun Netra 240 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 of the Netra 240.

Warning: All the services hosted on the server will be impacted when an administrator Powers off a server.

See the following operations procedures for more information:

- Powering off a server
- Powering on a server
- Resetting a server
- Advanced LOM of a Sun Netra 240 server

Powering off a server

The power off operation powers down the selected server.

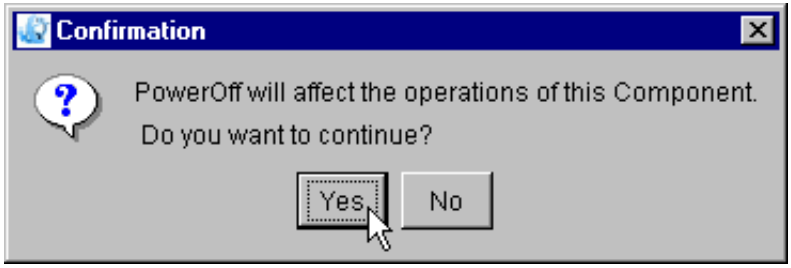
Note: If a management server is powered off, the connection to the System Management Console is lost. Administrators need to power up the management server either physically or via the terminal server before a new connection can be made.

1 Select the <**ServerName**> server in the system tree.

2 In the menu bar, select **Operations** > **Power OFF**

The Power Off confirmation prompt opens.

Figure 22 Confirmation dialog box for Power Off operation



3 Confirm the Power Off operation, click **Yes**.

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.

Powering on a server

The Power On operation powers up the selected server.

1 Select the <**ServerName**> server in the system tree.

2 From the menu bar, select **Operations** > **Power On**

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.

Resetting a server

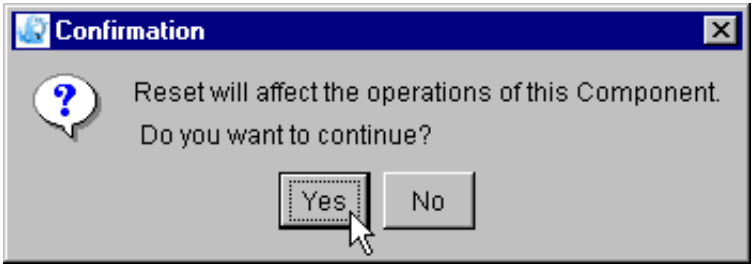
The Reset operation reboots the selected server.

1 Select the <**ServerName**> server in the system tree.

2 From the menu bar, select **Operations** > **Reset**

The Reset Server confirmation prompt opens.

Figure 23 Confirm Reset operation dialog box.



3 Confirm the server reset, Click **Yes**

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 will be 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 system tree is the same as server undergoing a LOM operation. The Host Name 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. See the procedure Adding a general server for more information.

Component configuration and management

Topics in this chapter

Component configuration overview

Administrators add, configure, and manage the CVoIP components using the System Management Console. Refer to the individual component guides for component specific details. See Related publications for a list of component documents.

The Management Module (SysMgr in the system tree) and Database Module (imssipdb in the system tree) are added manually without the use of the System Management Console. In addition, the Database Module is managed using the Oracle Element Manager. Both are monitored using the System Management Console.

Use the General Information Area (GIA) to view component level information. See the section Component level information displayed in the GIA for more information.

Component level information displayed in the GIA

When an administrator selects a component in the system tree, the GIA displays the following component level information:

- General

Component type: name of the component module (e.g. Management Module)

OS Type: the operating system running the component services (Sun, Linux, Win, all)

Version: software version of the component

Services: total number of component services

- States

  Administrative: current administrative state of the component (locked, unlocked)

  Operational: current operational state of the component (enabled, disabled)

- Alarms

  Critical: total numbers of current critical alarms generated by the component

  Major: total number of current major alarms generated by the component

  Minor: total number of current minor alarms generated by the component

- DB Info (for Oracle Monitor only)

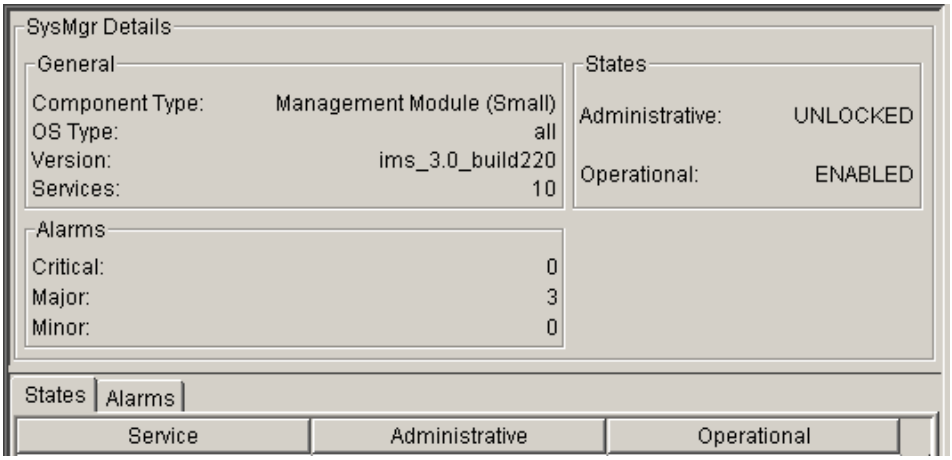
  Database Mode: whether or not the database is replicated

  Number of Replication Conflicts

  Replication Queue Size

  Number of Broken Jobs

Figure 24 GIA display when a component is selected



Component configuration

The CVoIP components 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 component. Refer to the individual component guides for specific configuration details and service property descriptions. See "Related publications" on page 9 for a list of the related component guides.

See the following for component related procedures:

- Adding a component
- Querying a components's configuration
- Modifying a component's configuration
- Deleting a component

Adding a component

The Management Module component is added manually and needs to be operational before administrators can connect with the System Management Console.

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

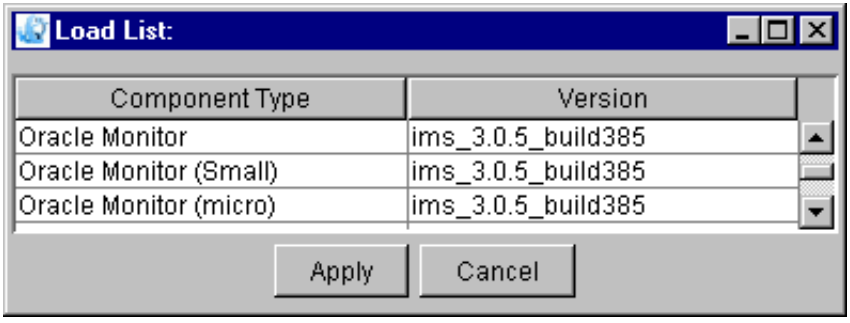
In the loadlist, same versions of some component software are labeled with small, small shared, and micro. The difference between the versions is the size of the memory footprint of the software on the server. For example, the Oracle Module (micro) has a smaller memory footprint than the same version labelled Oracle Module (Small). The size used will depend on the system architecture and the servers used.

To add a service component from the System Management Console, perform the following steps:

1. Select the server to host the component.
2. Right click and select **Add** > **Component**

   The load list dialog box opens listing all the available component software. The listed component types and versions can be sorted by clicking on either column header.

Figure 25 Component load list dialog box



3. Select the component software version to install.

The different versions of the component module software are indicated in the version column.

4 Click **Apply**.

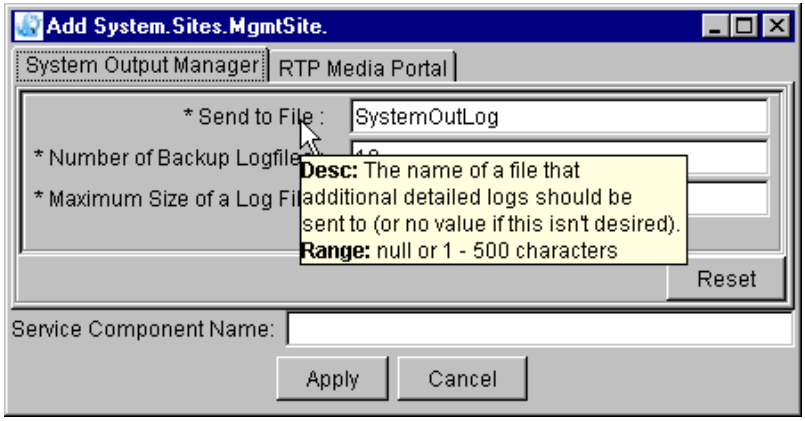
The component configuration dialog box opens. There are separate tabs for each component service with configurable properties.

The name entered into the **Service Component Name** field is used to identify the component in the system tree. The component name is limited to six characters.

5 Configure the service properties. Properties that require configuration values are indicated with a * in front of the property name. Grayed out property values can not be changed. Refer to the component 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.

Figure 26 Mouse over help for property descriptions



6 Click **Apply**.

The component is installed and activated. The time needed for the install depends on the component and the hosting server.

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

Querying a components's configuration

Administrators can query a server configuration to view the current configuration values. The property fields are grayed out, and cannot be modified.

1. Select the <**ComponentName**> component in the system tree.
2. Right-click and select **Query** from the shortcut menu.

   The component configuration dialog box appears displaying all the services with configurable properties.

Modifying a component's configuration

Administrators can modify configured properties of services hosted on the different components to reflect changing network requirements. Properties that cannot be modified are grayed out in the configuration dialog box. Modify requires locking the service.

1. Select the <**ComponentName**> component in the system tree
2. From the menu bar, select **Operations** > **Lock**

Note: The Management Module and Database module components can not be locked.

   This opens the lock confirmation prompt.

3. Confirm the component lock, click **Yes**.

   The component's administrative state changes to locked.

4. Select the <**ComponentName**> component in the system tree
5. From the menu bar, select **Operations** > **Modify**

   The component's configuration dialog box opens.

6. Modify the configuration properties with the new values. Properties that can not be changed are grayed out.
7. Click **Apply**
8. To unlock the component, right click and select **Unlock**

The component's services resume with the modified configuration.

Deleting a component

Administrators can delete a service component on a server.

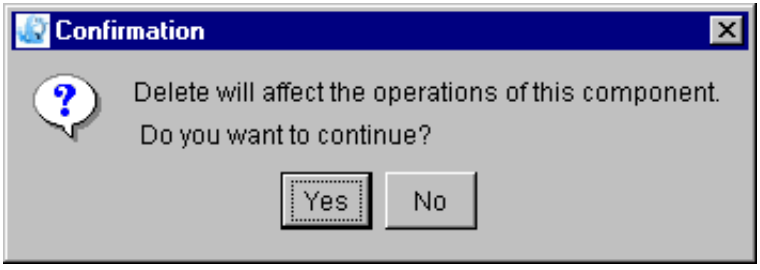
1. Select the <**ComponentName**> component in the system tree
2. From the menu bar, select **Operations** > **Lock**

   The lock confirmation prompt opens.
3. Confirm the lock, click **Yes**.

   The component's administrative state changes to locked.
4. From the menu bar, select **Operations** > **Delete**.

   The delete component confirmation prompt opens.

Figure 27 Delete component confirmation prompt



5. Confirm the component deletion, click **Yes**.

Component software updates

Administrators can update the software version for a specific component if more than one version is available. The current configuration data is automatically transferred to the updated version. The update can be an upgrade to a new version, or a downgrade to a previous software version.

During the update, a comparison is made between the two software versions checking for added or removed property fields. Differences between the software versions are indicated in the updated version as follows:

- Service tabs with added or removed configuration fields are indicated by green text.
- New property fields in the service tab are indicated by blue text.
- Removed property fields in the service tab are indicated by grayed out text.

For more information, see the procedure Updating component software. The service impacts of updating component software will vary depending on the component involved and system architecture. Refer to the individual MCS component and MCS upgrade guides for more details.

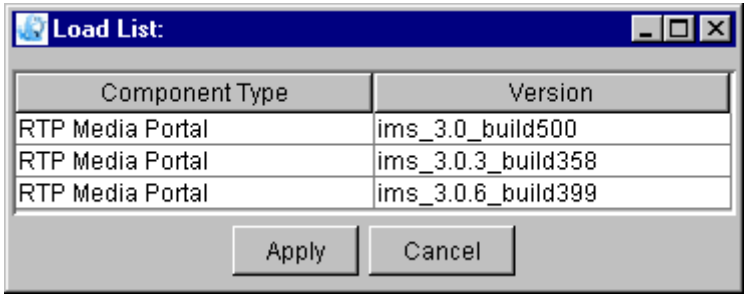
Updating component software

Use the following procedure to perform a software update:

1. Select the <**ComponentName**> component in the system tree
2. From the menu bar, select **Configuration** > **Update**

   The load list dialog box opens showing the available software versions of the selected component.

Figure 28 Update load list dialog box



3 Select the software version from the list.

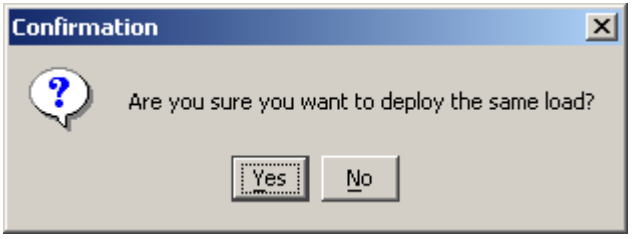
Use the same software size (i.e. micro, Small, etc.) as the software being updated. The GIA displays the version currently installed.

4 Click **Apply**

The dialog box for the selected component opens. The updated component configuration fields are data filled with the configuration data from the previous version. Changed tabs and fields are indicated as described above.

If you select the same load as the version currently installed, you are prompted to confirm the deployment of the same load.

Figure 29 Confirmation prompt to deploy same load

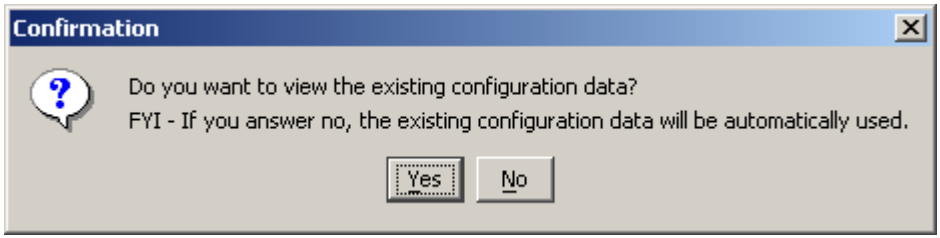


To deploy the same load use the following sub steps

a Confirm the selection of same version to re-install, click **Yes**.

A second confirmation prompt opens.

Figure 30 Confirmation prompt to view existing configuration



b To apply the existing configuration as is, click **No**. The same load is deployed, and the configuration dialog boxes do not open.

To modify the existing configuration, click **Yes**. The configuration dialog box opens with all the tabs available.

5 Enter configuration values for any new fields and/or change the existing configuration.

6 Click **Apply**.

Component management

Administrators use **Lock**, **Unlock**, and **Shutdown** operations when modifying the configured properties of components and component services. When a component is locked, the administrative state changes to locked and services become unavailable.

The **Shutdown** operation is only available for an RTP Portal component. A shutdown is a graceful lock. It will change the component to a locked administrative state, but only after the services have completed all current service requests. During this time, no new service requests are accepted.

See the following procedures for more information:

- Locking a component
- Unlocking a component
- Shutting down the RTP Media portal
- Stopping a service component
- Restarting a component

Locking a component

A **Lock** stops the processes of a component. Administrators must lock a component to modify the configuration of most services

Warning: Locking a component may impact in-progress sessions.

The following table lists the results of performing a lock on the different components. Administrators should refer to the individual component guides for more details.

Table 4 Results of a lock operation

Component	Result of lock
Management Module (SysMgr)	N/A - the SysMgr cannot be locked.
Database Module (imssipdb)	N/A - the database cannot be locked
Oracle Monitor	Locking the Oracle Monitor is not service impacting. The monitoring of the Oracle database stops.
RTP Media Portal	We recommend that shutdown is used to lock the RTP Media Portal. A shutdown will close off all active sessions before the component transitions into a locked administrative state.

1. Select the <**ComponentName**> component in the system tree
2. From the menu bar, select **Operations** > **Lock**

   The component changes to a locked administrative state.

   To unlock the component, see the procedure Unlocking a component.

Unlocking a component

Unlock returns the component to an unlocked administrative state

1. Select the <**ComponentName**> component in the system tree.
2. From the menu bar, select **Operations** > **Unlock**

The component changes to an unlocked administrative state. Alarms generated by the component's locked administrative state will clear.

Shutting down the RTP Media portal

The **Shutdown** operation is only available for an RTP Portal component. A shutdown is a graceful lock. It will change the component to a locked administrative state, but only after the services have completed all current service requests. During this time, no new service requests are accepted.

1. Select the RTP Media Portal component in the system tree.
2. From the menu bar, select **Operations** > **Shutdown**

   The Shut down confirmation prompt opens.
3. Confirm the shut down, click **Yes**

   The component changes to a locked administrative state when all services requests have finished processing. The **Modify** option becomes available.

   To unlock the component, see the procedure Unlocking a component.

Stopping a service component

Stop terminates a service component's processes. When a component is stopped, the operational status changes to Unknown and all services are terminated.

1. Select the <**ComponentName**> component in the system tree
2. From the menu bar, select **Operations** > **Stop**

Note: The Stop operation is not available for the Management Module and Database Module components.

   The stop confirmation prompt opens.
3. Confirm the stop, click **Yes**.

   The component changes to a disabled operational state.
4. To restart a component, select the <**ComponentName**> component in the system tree.

5 From the menu bar, select **Operations** > **Start**

When the component starts properly, the operational state changes to enabled.

Restarting a component

The **Restart** operation performs a combined stop and start. During the period of the restart, the component is in a disabled operational state. Restart sets the operational status to either Enabled/Disabled based on whether the application comes up properly.

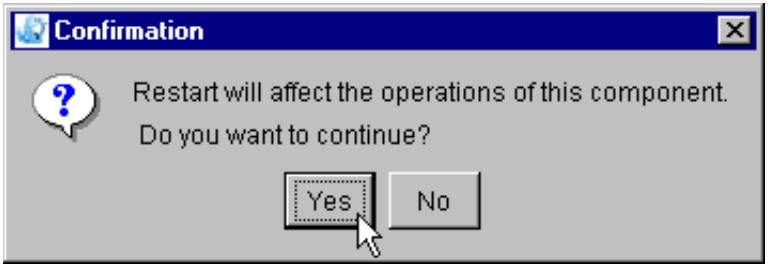
1 Select the <**ComponentName**> component in the system tree.

2 From the menu bar, select **Operations** > **Restart**

Note: The Restart operation is not available for the Management Module and Database Module components.

This opens the Restart confirmation prompt.

Figure 31 Restart confirmation prompt



3 Confirm the Restart, Click **Yes**

When the component starts properly, the operational state changes to Enabled.

Service configuration and management

Topics in this chapter

Service configuration overview

Services are typically configured and managed as part of a component. However, the System Management Console gives administrators the ability to query and modify component services individually.

Use the General Information Area (GIA) to view service level information. See the section Service level information displayed in the GIA for more information.

Service level information displayed in the GIA

When an administrator selects an individual component service in the system tree, the GIA displays the following service level information:

- States

  Administrative: current administrative state of the service (locked, unlocked)

  Operational: current operational state of the service (enabled, disabled)

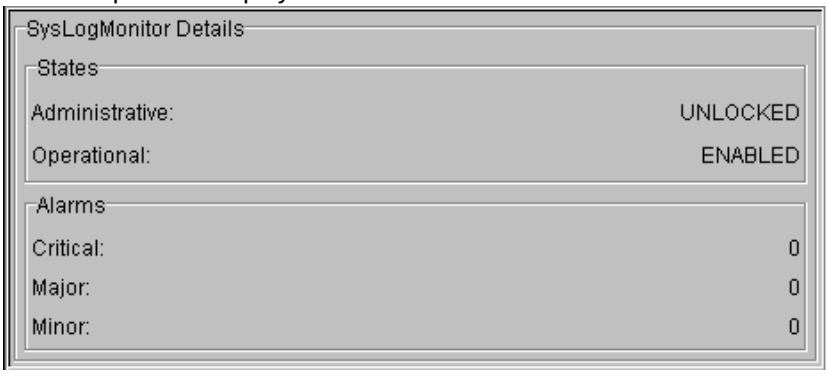
- Alarms

  Critical: total numbers of current critical alarms generated by the service

  Major: total number of current major alarms generated by the service

  Minor: total number of current minor alarms generated by the service

Figure 32 Example GIA display when a service is selected



Service configuration

Only configurable services can be modified. Modifying an individual service component requires the locking of the component.

See the following service level procedures for more information on service configuration and management:

- Querying a service's configuration
- Modifying a service's configuration

To modify or query a service as part of a component, refer to the section Component configuration.

Querying a service's configuration

Not all services of a component have configurable properties. Only configurable services can be queried. All the service configuration fields are grayed out and cannot be modified.

1. Select the <**ServiceName**> service in the system tree
2. From the menu bar, select **Configuration** > **Query**

   The service's Query dialog box opens.

Modifying a service's configuration

Only configurable services can be modified. Use the following procedure to modify a service's configuration using only the configuration dialog box of the service. Field descriptions for the service configuration dialog box are described in the related component document. See "Related publications" on page 9 for a list of component guides.

Modifying an individual service component requires the locking of the component. The exception is the SysLogMonitor service of the Management Module (SysMgr) component. Since the Management Module cannot be locked, the SysLogMonitor service can be locked individually. See *CVoIP Management Module Basics* for more information.

To modify a service from the component level, refer to the procedure Modifying a component's configuration.

1. Select the <**ComponentName**> name in the system tree
2. From the menu bar, select **Operations** > **Lock**
3. Confirm the lock, click **Yes**
4. Select the <**ServiceName**> service in the system tree
5. From the menu bar, select **Configuration** > **Modify**

   This opens the configuration tab of the selected component service.
6. Modify the configuration properties
7. Click **Apply**
8. Select the <**ComponentName**> name in the system tree
9. From the menu bar, select **Operations** > **Unlock**

Alarm browser

Topics in this chapter

Refer to the CVoIP component guide for the individual alarm descriptions.

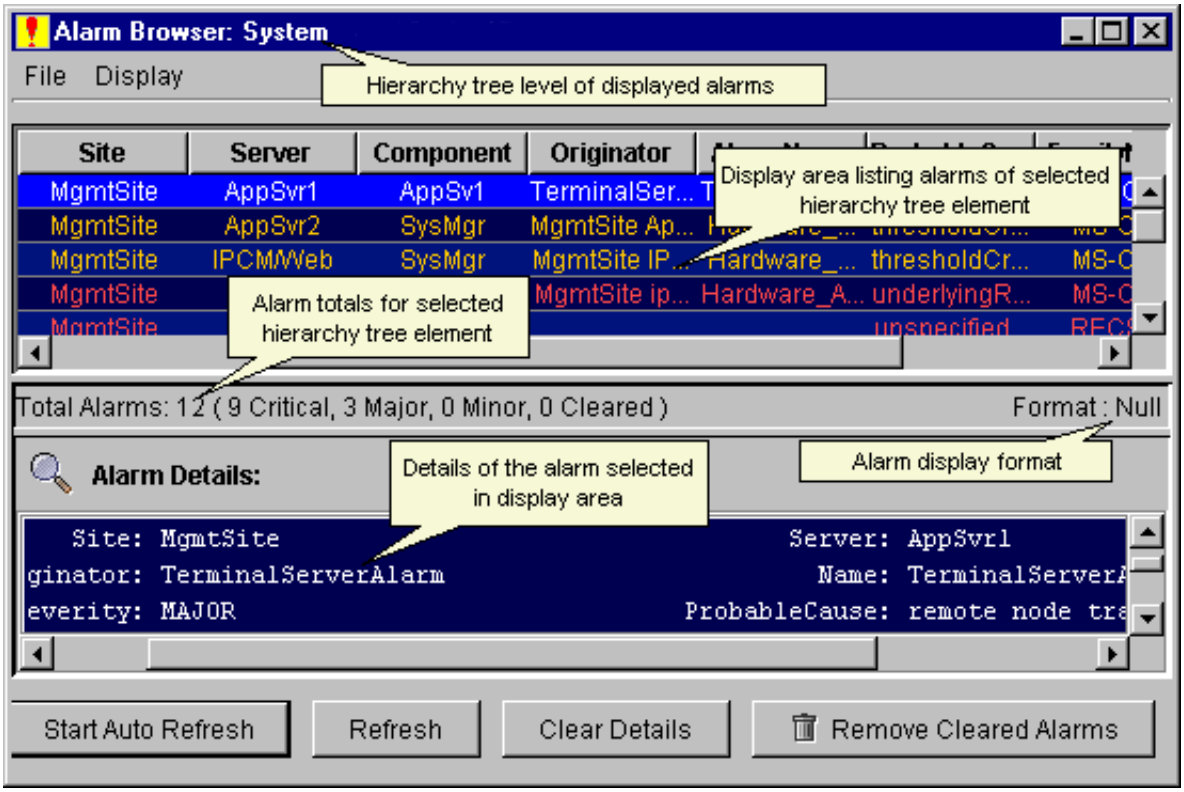
Alarm browser basics

Once in operation, system elements have the ability to raise and clear alarms/ faults. As faults occur, alarms are generated by the managed element and sent to the Management Module component. Once at the Management Module, administrators view the alarms using the System Management Console's alarm browser.

When an alarm is raised, it is added to a list of active alarms. The alarm remains on the active list until it is resolved. Once the problem is resolved, the alarm is cleared and removed from the list of active alarms.

The following figure shows an alarm browser launched with the system element selected in the system tree. Not all the alarm browser columns are shown in the figure. See the section Alarm information displayed in the browsers for alarm information displayed in the browser.

Figure 33 Alarm browser



The alarm browser has two main areas: the Alarm Display and Alarm Details area. 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 display.

The middle bar has two fields: Total Alarms and Format fields. The total alarms field lists the total number of alarms, and the subtotals for critical, major, minor, and cleared alarms. The display field lists the format being used for the alarm display area.

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

Table 5 Alarm browser functions

Function	Description
Start | Stop Auto Refresh	The System Management Console begins polling the service components in order to allow the alarm browser to dynamically update the alarm status. The elements are polled approximately every 5 seconds when this function is enabled.
Refresh	Updates the Alarm Display area with the current alarms and their status
Clear Details	Clears the text from the Alarm Details area of the alarm browser
Remove Cleared Alarms	Removes cleared alarms from this alarm browser's display. Cleared alarms are indicated by a trash can icon in the CLR column.

Alarm information displayed in the browsers

The Alarm browser can be launched from all levels of the system tree.

The information displayed in the alarm browser is dependent on the element selected in the system tree. For example, if a server is selected, the alarm browser shows the alarms for all the components hosted on the server, if a component is selected only the alarms generated by the component services are displayed. 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:

Table 6 Alarm information displayed in the alarm browser

Alarm attribute	Description
TImestamp	the time when the alarm was raised
Severity	the severity assigned to the alarm
Originator	the service originating the alarm
Alarm Name	the name of the alarm
ProbableCause	the general problem causing the alarm
Family Name	managed object family originating the alarm
AlarmNumber	the number identifier of the alarm
CLR	Indicates whether the alarm has been cleared. When cleared, a trash icon appears in the column.

Additional information is included to help identify the service originating the alarm when the following nodes are selected in the system tree:

- System: alarm browser also displays the site, server, and component hosting the alarm originator
- Site: alarm browser also displays the server and component hosting the alarm originator
- Server: alarm browser also displays the component hosting the alarm originator

Alarm browser operations

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

The Management Module throttles excessive alarms from a single network element. When a network element generates more than fifty alarms, only the first fifty are sent to the System Management Console from the Management Module. Under this condition, the network element name (text) turns red in the system tree.

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

- Viewing alarms
- View alarm details
- Sort alarms based on alarm attribute
- Copy alarm information
- Remove cleared alarms
- Refresh alarm information

Viewing alarms

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

1. Select a managed element in the system tree.
2. In the menu bar, select **Tools** > **Alarm Browser**.

   Alternatively, click the **Alarm Browser** icon  in the toolbar.

   The alarm browser opens and shows all the alarms associated with selected managed element.

View alarm details

Alarm information for a selected alarm display in the Alarm Details area.

1. Double-click on an alarm listed in Alarm Display area of the browser.

   Information on the alarm displays in the Alarm Details area.
2. To clear the Alarm Details area, click **Clear Details**.

Sort 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 going from critical to warning.

1. Click a column header.

   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.

Copy 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 document.

Remove cleared alarms

When alarms are cleared, a trash can icon appears in the CLR column. Use the following procedure to remove these alarms from the browser display.

1. Click **Remove Cleared Alarms**.

Refresh alarm information

Clicking the **Refresh** button updates the alarms in the browser to reflect the current system faults. The **Auto Refresh** option updates the alarm information as changes occur.

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

2 To enable auto refresh, click the **Start Auto Refresh**.

Auto refresh is enabled, and the button toggles to **Stop Auto Refresh**.

Alarm browser display formats

Administrators can modify, save, and apply formats to the Alarm Display area to best suit their administrative needs. See the following procedures for more information:

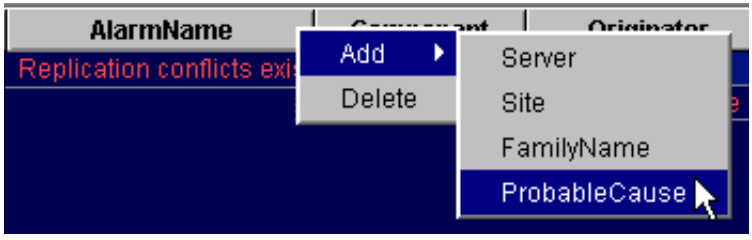
- Modifying the alarm display format
- Saving an alarm display format
- Applying an alarm display format

Modifying the alarm display format

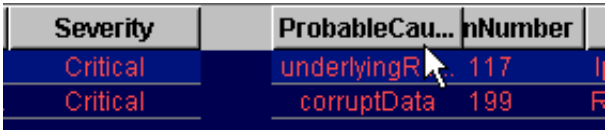
Alarm attribute columns can be hidden, rearranged, resized, and the color scheme changed. Modify the format using the following procedure:

1 Hide any unneeded columns. Right-click on the column header and select **Delete**.

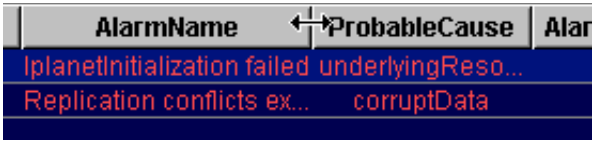
2 Show any previously hidden columns. Right-click on the column header and select **Add** > attribute_name. Added columns appear in the far left of the display.



3 Rearrange the column order. Click and drag column header to desired place.



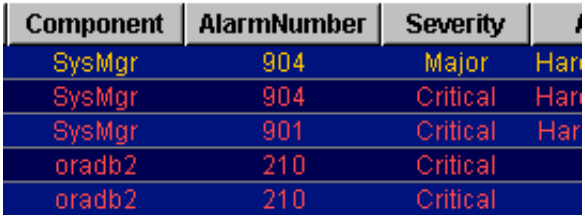
4 Resize columns using the cursor. Use the scroll bar to view columns not in display.



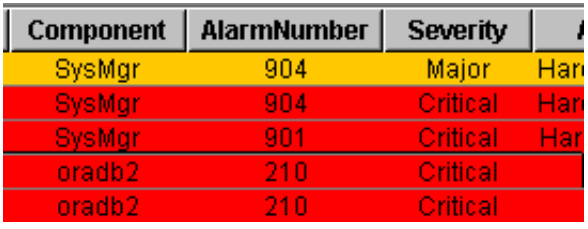
5 Select color scheme. Click **Display** > **Color** > color_scheme.

Two color schemes are available:

- Dark Blue Background Color Scheme (default)



- Red Yellow Gray Color Scheme



Saving an alarm display format

Once the alarm display area is setup, the format can be saved and applied in subsequent administration sessions. Formats are saved to the AlarmFormat directory in the MCP System Management Console folder on the administrator's PC.

Formats save the following display properties:

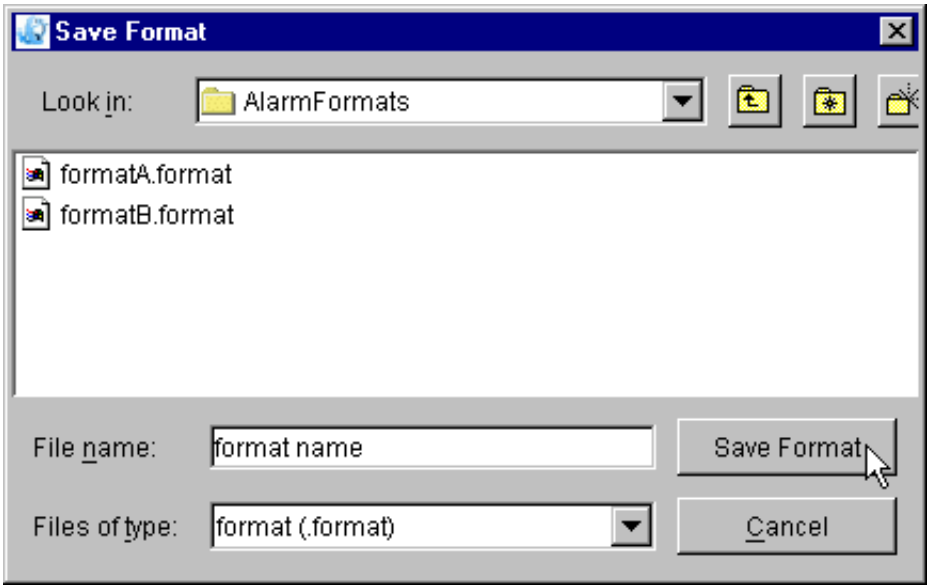
- the column name/attributes that are displayed

- the order of columns
- the size of each column
- the color scheme

1 Select **Display** > **Save Format**.

The Save Format dialog box opens.

Figure 34 Save Alarm Format dialog box



2 Enter a file name for the Format and click Save Format. The format is now saved for future sessions.

To delete unwanted alarm display formats

1 Select **Display** > **Delete Format**.

The Delete Format dialog box launches.

2 Select the unwanted Format file, and click **Delete Format**.

Applying an alarm display format

Apply saved alarm display formats as needed. When applied, the format name appears in the Display Format field.

1. Select **Display** > **Apply Format**..

   The Apply Format dialog box opens.

2. Select the desired Format file, and click **Apply Format**.

   The format name appears in the Format field.

Log browser

Topics in this chapter

Log browser basics

Logs are events that occur during the operation of the service components. They 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 in Standard (STD) format to disk on the management server.

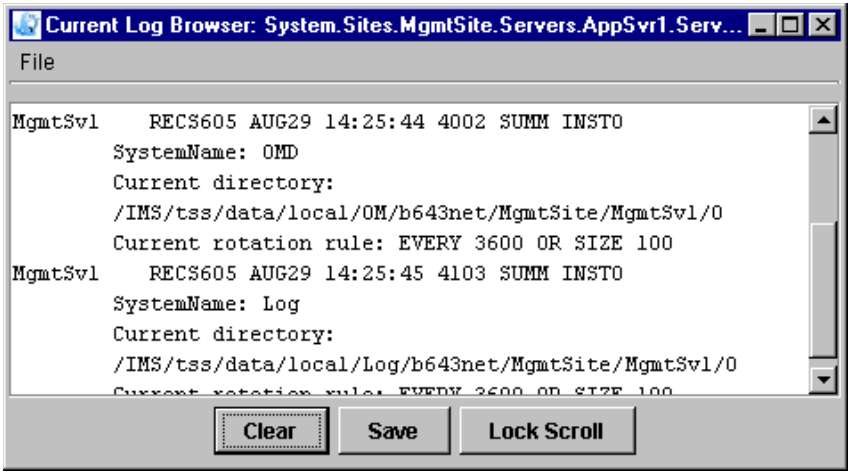
There are two types of logs users can request to view from the System Management Console: Current and Archived. Current logs are a live stream of logs/events being reported to the Management Module. As the logs are received, they are saved to the current (*.active) log file. After a configured period 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 current log file is opened.

There are separate log browsers for the current and archived logs. The log information displayed is limited to a single component. The displayed information and the functionality of the two log browsers is essentially the same. See the following for more information:

Current log browser

A current log browser can only be launched when a component is selected in the system tree. Administrators can have multiple log browsers open at the same time to concurrently monitor multiple components. The following figure shows a current log browser.

Figure 35 Current Log Browser



The following functions are available in the current log browser:

Table 7 Function buttons in the log browser

Function	Description
Clear	Removes all of the existing log text from the window of the log browser.
Save	Saves all of the logs displayed in the window of the current log browser to a local file on the workstation running the System Management Console.
Lock Scroll/ Unlock Scroll	Toggles the scrolling of log text in the window of the current log browser.

Archive log browser

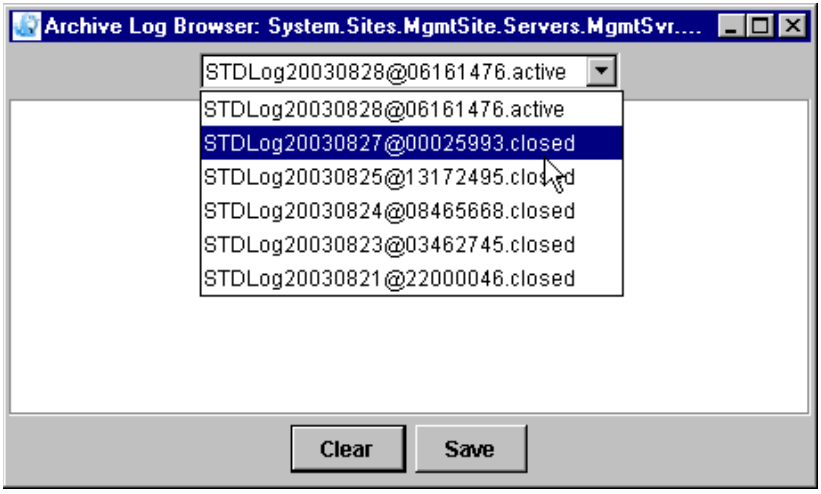
The archive log browser is launched from a current log browser. Only the archived log files for the component selected to launch the current log browser can be viewed. The archived files are selected from the drop-down menu. The *.active file contains the logs collected to date in the current log browser.

Archive log filenames use the following format:

```
STDLog<Date>@<Time>.<closed|active>
```

where
<Date> format is: YYYYMMDD
<Time> format is: HHMMSSMM (HourHour MinuteMinute SecondSecond MillisecondMillisecond)

Figure 36 Archive log browser



The following functions are available in the archive log browser:

Table 8 Archive log browser functions

Function	Description
Clear	Removes all of the existing log text from the window of the log browser.
Save	Saves all of the log text displayed in the window of the log browser to a local file on the workstation running the Management Console.

Log browser operations

The log browser displays all the logs originating from the selected component in the system tree. 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 current log browser
- Launching the archive log browser
- Clearing log details
- Saving logs
- Viewing saved logs
- Configuring log file rotation periods

Launching the current log browser

Current log browsers can only be launched from the component level of the system tree.

1 From the menu bar, select **Tools** > **Log Browser**

Alternatively, click the Log Browser icon  on the tool bar.

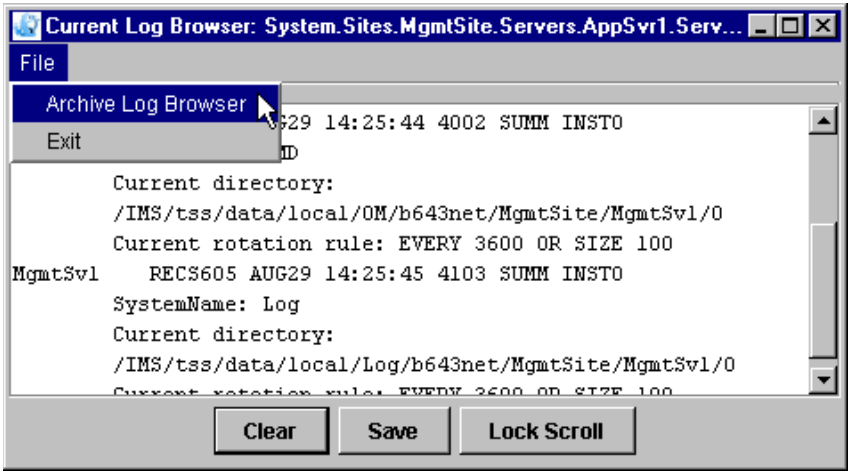
The Current Log Browser opens

Launching the archive log browser

The archived log browser is launched from an open current log browser.

1 In the Current Log browser, select **File** > **Archive Log Browser**.

Figure 37 Launching the Archive Log Browser



The Archive Log Browser launches.

2 Select an archived log file from the drop down list.

Clearing log details

Administrators can clear the log text in the browser display.

1 Click **Clear**.

Saving logs

Logs can be saved to a local directory on an administrator's workstation.

1 Click **Save**.

The Save Log dialog box opens.

2 Name the log file being saved and select the local workstation folder used for the saved logs.

3 Click **Save**.

Viewing saved logs

Logs saved to a workstation directory are viewable using workstation applications that read *.txt files.

1 Open the folder on the workstation containing the saved logs.

2 Double-click the saved log.

The log file opens in the workstations default *.txt file application.

Configuring log file rotation periods

Administrators can configure the current log rotation interval and file size on a component by component basis, server by server basis, or at the system level. Typically, this is configured at the system level. For information on configuring the log file rotation parameters, see Configuring OAM file rotation properties in the System level configuration chapter.

Operational measurement browser

Topics in this chapter

Refer to the CVoIP component guides for descriptions of the individual OMs.

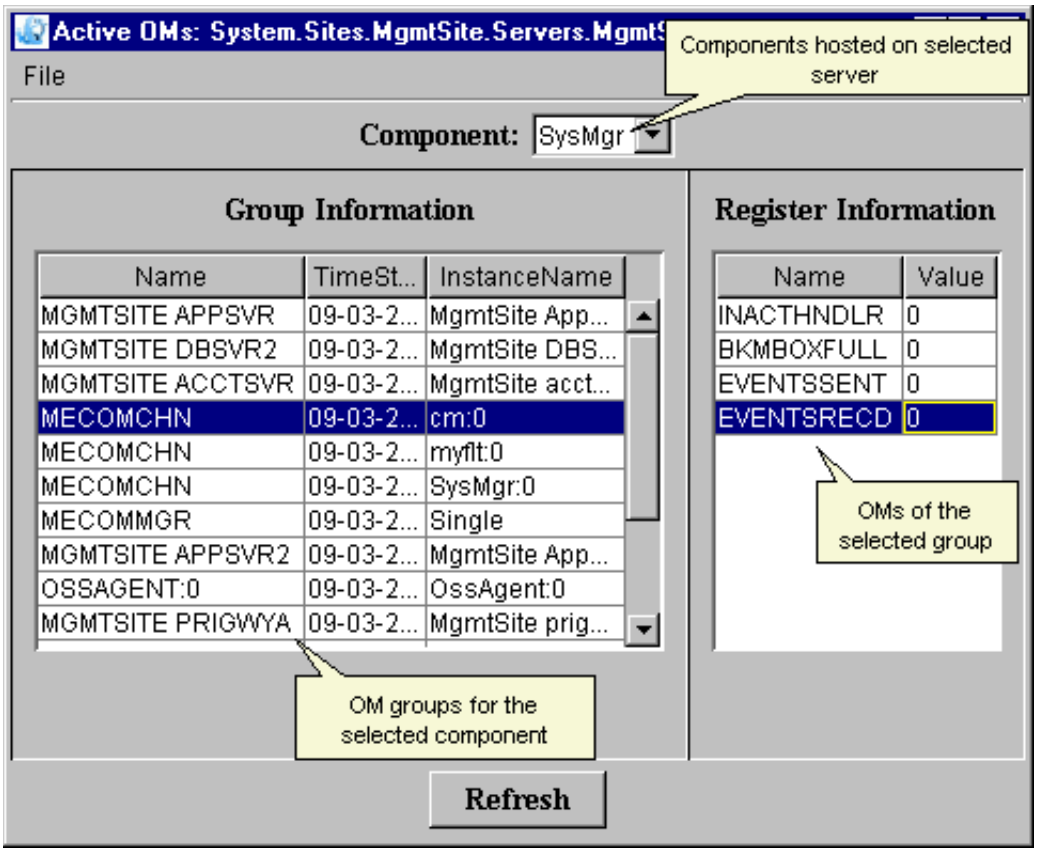
Operational measurements browser basics

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 displayed as they are reported by the server to the management server/management console. Holding OMs have already been archived to files on the Management Server.

The OM browser is used to view both active and holding OM. The OM information displayed in a browser is for a single server. 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.

Figure 38 Active OM browser



The OM browsers have two main areas: the Group Information and Register Information area. The Group Information area shows a list of OM groups of the selected service component. The Register Information area displays the register information of a 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.

The Component drop-down menu lists the service components hosted on the server.

OMs viewed in the browsers display the following information:

Table 9 OM details displayed in the OM browser

Information	Description
Group Name	The name of the OM group where the scanned information resides.
TimeStamp	The time when the OM information was scanned.
InstanceName	The name of the service originating the OM information.
Register Name	The name of the OM register at the time of the scan.
Register Value	The value of the OM register at the time of the scan.

OM browser operations

An active OM browser can only be launched when a server is selected in the system tree. Administrators can have multiple OM browsers open at the same time to monitor separate servers.

- Launching the active OM browser
- Launching the holding OM browser
- Viewing specific service component OM
- Viewing register information of a specific group
- Refreshing data in the OM browser
- Configuring OM file rotation periods

Launching the active OM browser

OM Browsers are only available at the server level in the system tree.

1 Select a <**ServerName**> server in the system tree.

2 From the menu bar, select **Tools** > **OM Browser**.

Alternatively, click the OM Browser icon  in the toolbar.

The active OM browser for the selected server opens.

Launching the holding OM browser

The Holding OM Browser is launched from an open Active OM Browser.

1 Select **Menu** > **Holding OM Browser**.

The Holding OM Browser launches.

Viewing specific service component OM

OM information is available for the different service components of the selected server. Only the OM of one service component is displayed at a time.

1 Select the Service Component from the Component drop-down menu.

The browser displays the service component’s OM.

Viewing register information of a specific group

The Register Information is displayed for a specific group.

1 Select a group from the Group Information area.

The selected group’s register information displays in the Register Information area.

Refreshing data in the OM browser

OM data is updated according to the configured interval. When the browser has been open for an extended period, administrators can refresh the browser to display the latest OM data.

1 Click **Refresh**.

Configuring OM file rotation periods

Administrators can configure the active OM rotation interval and file size on a component by component basis, server by server basis, or at the system level. Typically, this is configured at the system level. For information on configuring the OM file rotation parameters, see Configuring OAM file rotation properties in the System level configuration chapter.

Administrator tools

Topics in this chapter

The following menu items are not applicabale or available in CVoIP solution deployments: **IPCM Device Maintenance**, **H.323 EndPoint Maintenance**, **Media Server Maintenance**, **Launch BPS GUI**, and **Provisioning**.

Session history

The History tool of the System Management Console allows administrators to view a record of their actions during a management session.

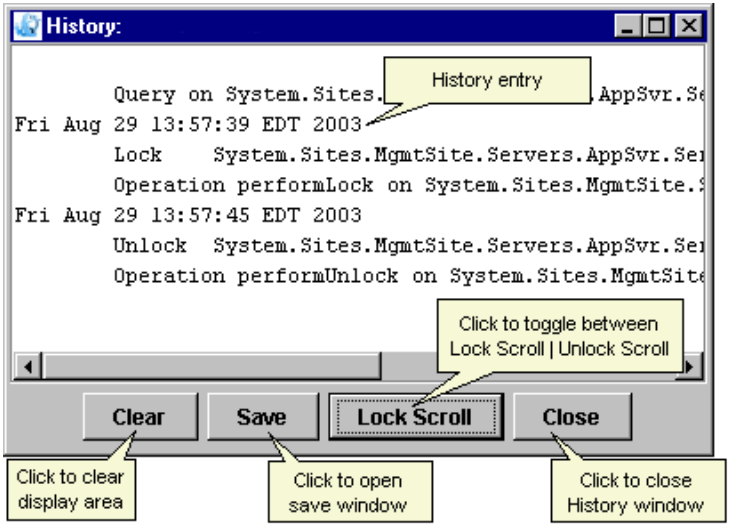
Opening the History window

The History window is available from all levels of the system tree.

1 From the menu bar, select **Tools** > **History**

The History window opens.

Figure 39 History window



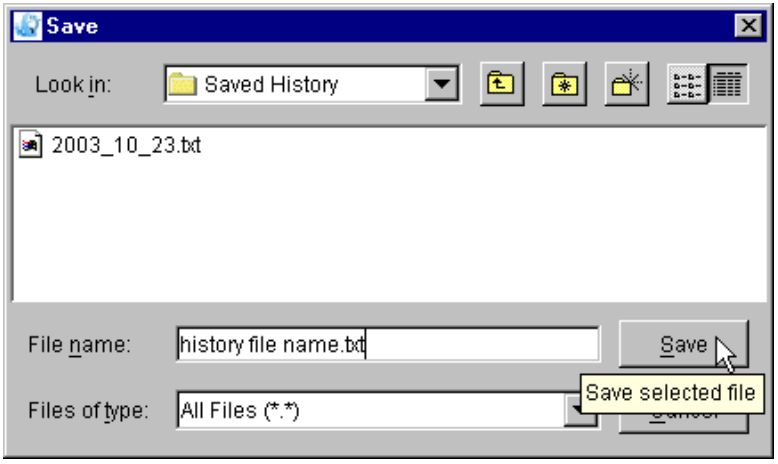
Saving history information

Administrators can save the entries displayed in the History window to a directory on the workstation as a text file.

1 In the History window, click the **Save** button

The Save History dialog box opens.

Figure 40 Save history dialog box



2 Assign a name for the file, adding a file extension for the application you want to read the file (e.g. *.txt, *.doc).

3 Click **Save**

Communications monitor

Administrators can view their XML communications between the System Management Console and the Management Module component. The XML is displayed as text in the Monitor Communications window.

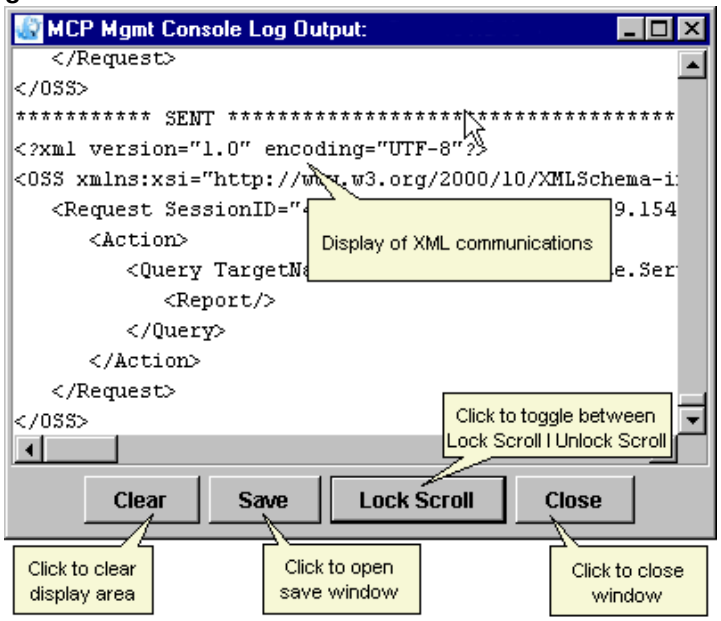
Opening the Monitor Communications window

The Monitor Communications window is available from all levels of the system tree.

1 From the menu bar, select **Tools** > **Monitor Communications**

The Monitor Communications window opens.

Figure 41 Monitor Communications window



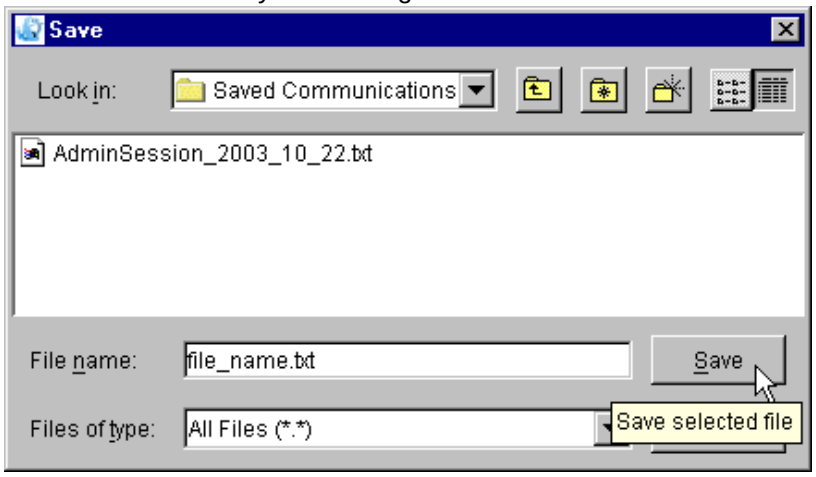
Saving the communications information

The text displayed in the Monitor Communications window can be saved to a text file on the workstation.

1 In the Monitor Communications window click the **Save** button

The Save dialog box opens.

Figure 42 Session History save dialog box.



2 Assign a name for the file, adding a file extension for the application you want to read the file (e.g. *.txt, *.doc).

3 Click **Save**

General Information Area refresh

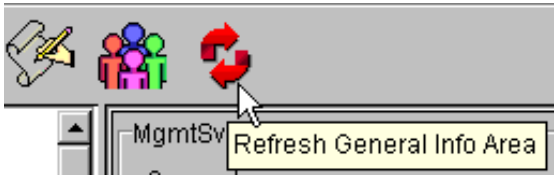
The Refresh General Information Area tool allows administers to update the information displayed in the General Information Area (GIA) of the System Management Console. Refresh is available for all levels of the system tree, with the exception of the logical nodes of Sites, Server, and Components.

In addition to invoking a refresh, the GIA for a selected system node automatically refreshes approximately every 20 seconds.

1 Select System, a site, a server, a component, or service in the system tree.

2 Click the **Refresh** icon on the toolbar

Figure 43 Refreshing the GIA.



Communication between active administrators

The List Active Administrators tool displays the active administrators and allows administrators to communicate with each other. The information displayed about each administrator entered and saved in the database. Refer to *CVoIP Database Module Basics* for information on adding administrators.

Listing active administrators

Use the following procedure to view a list of active administrators.

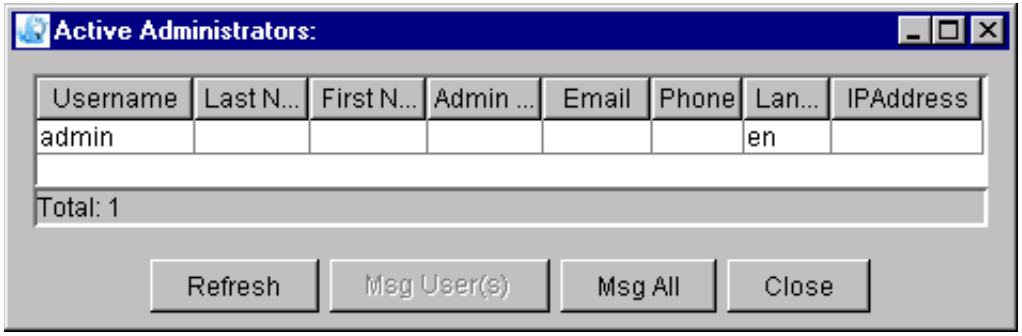
1 From the menu bar, select **Tools** > **List Active Administrators**

Alternatively, click the List Active Administrators icon in the toolbar

Figure 44 List Active Administrators icon on the toolbar..

The Active Administrators window opens. CVoIP only supports the configuration of limited administrator definitions. As a result, not all fields in the Active Administrator window disply information. Administrators need to be identified in the window by either Username or IP address.

Figure 45 Active Administrators window



Sending messages to active administrators

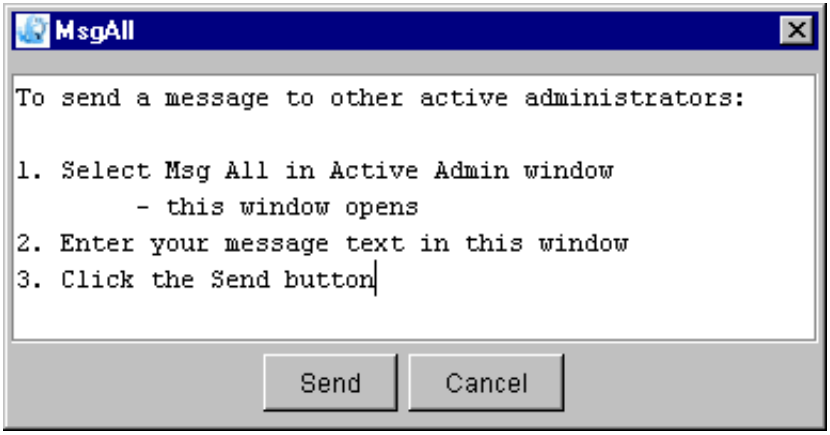
Any administrator can send a text message to a specific administrator or all administrators involved in an active System Management Console session. The message shows up in a popup window on the receiving workstation(s).

1 To send a message to all active administrators, click **Msg All** (message all) button.

The MsgAll (message all) window opens

2 Enter the message in the window

Figure 46 Message All (MsgAll) window



3 Click **Send**.

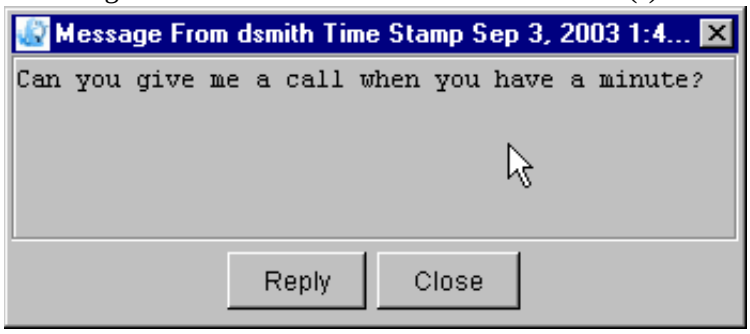
The message is sent to all the active administrators.

4 To send a message to a specific administrator(s), select the administrator(s) from the Active Administrators window, and click **Msg User**(s).

The MsgUsers text window opens.

5 Enter the message in the window, and click **Send**.

The message is sent to the selected active administrator(s).



Administrators receiving the message can respond to the message sender from the popup message window.

Launching the database administration interface

Administrators launch the login dialog box for the Oracle Enterprise Manager (OEM) from the System Management Console. The administrator requires the appropriate privileges to log into the database management application. In addition, the OEM requires the installation of the Jinitiator plug-in to run on the workstations.

For information on managing the database and installing the required OEM plug-ins, refer to *MCS 5100CVoIP Database Module Basics.*

1 Select the database component (imssipdb) in the system tree.

2 From the menu bar, select **Administration** > **Database Administration**

The Confirm IPAddress dialog box opens.

3 Confirm the database IP address, and click **OK**.

The OEM login dialog box opens.

Troubleshooting

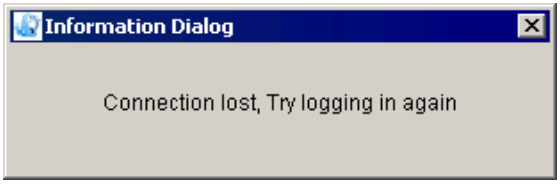
The following procedures describe troubleshooting and resolving some known System Management Console issues:

- System Management Console connection is lost
- System Management Console fails to uninstall properly
- Font problems in System Management Console

System Management Console connection is lost

When the connection between the Management Module and System Management Console is lost, the following dialog box appears on the administrator's workstation screen followed by a login prompt.

Figure 47 Connection lost dialog box



The lost connection may be a network or connection related problem, or an indication that the SysMgr component 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 SysMgr or it's hosting server, administrators can manually failover the Management Module operations to the secondary Management Module. Once the secondary Management Module is operational, a System Management Console connection can be re-established.

For more information on the failover procedure, refer to *MCS 5100CVoIP Management Module Basics*.

System Management Console fails to uninstall properly

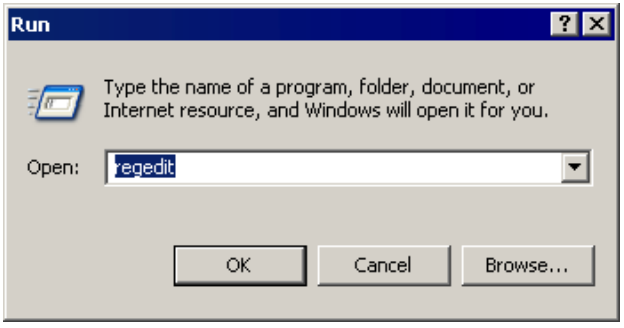
On some systems, the uninstaller does not remove itself properly from the registry. The behavior of this problem is the MCP Console uninstaller reports a successful uninstall, but with the next MCP Console install, the installer application continues to prompt the user to uninstall the MCP Console application. To resolve this problem, the old MCP Console needs to completely removed from the system. The following procedure describes how to completely remove the old MCP Console.

1. Remove the MCP System Management Console folder from the workstation registry if it exits.

   a. In Windows, select **Start** > **Run**

      The Run dialog box opens.

Figure 48 Windows Run dialog box



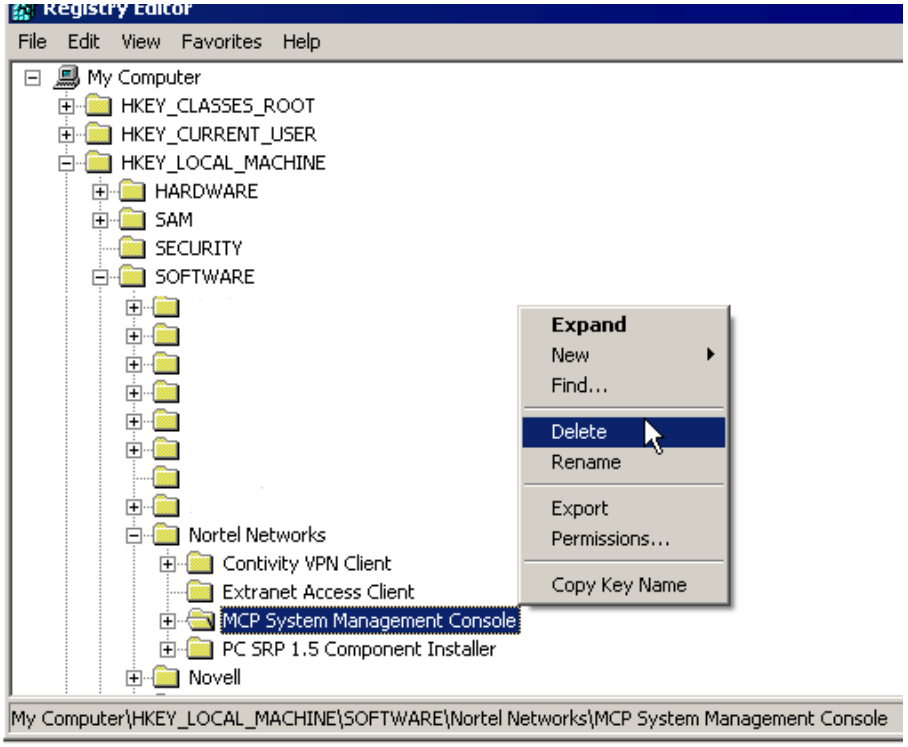
   b. Enter **regedit** and click **OK**.

      The Registry Editor dialog box opens.

   c. Expand the registry tree to view the folder **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Nortel Networks**

   d. Check for a **MCP System Management Console** folder. Delete the folder if it exists.

Figure 49 Registry tree with a MCP System Management Console folder



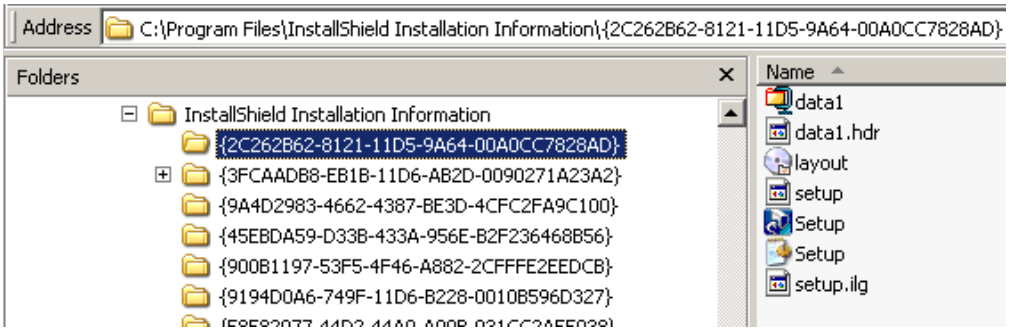
e Close the Registry Editor

2 Remove the MCP System Management Console related folder from the Installation Information folder

a Using Windows Explorer, navigate to the folder **C:\Program Files\ InstallShield Installation Information**

On some systems the folder may be defined as hidden. Use the search functionality to find the folder, or show all hidden files.

Figure 50 InstallShield Installation Information folder



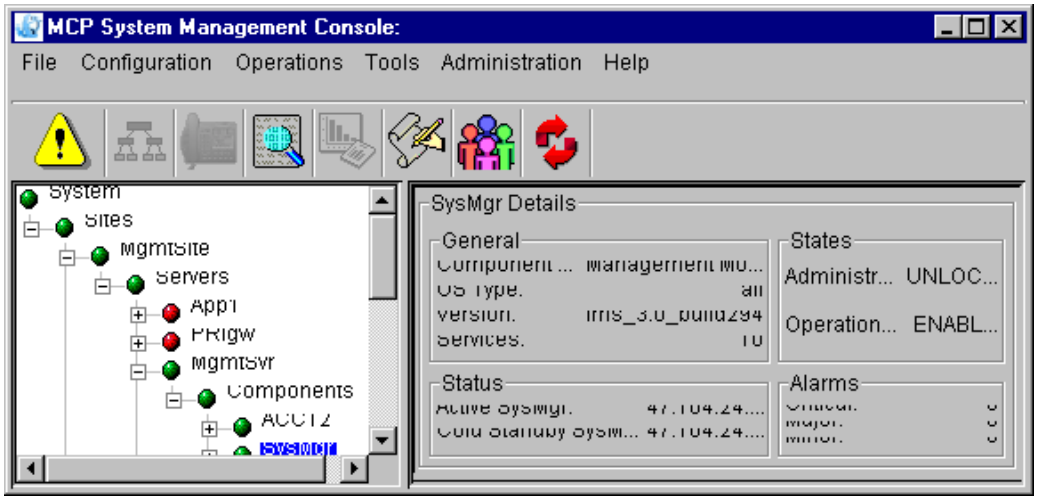
b Delete the MCP System Management Console related folder named **{2C262B62-8121-11D5-9A64-00A0CC7828AD}**

3 Install the updated System Management Console software. With the deletion of the previous installation information, the process will be the same as a first time installation. See the procedure Installing the System Management Console for the first time for more information.

Font problems in System Management Console

The Java Runtime Environment (JRE) used by the 3.0 System Management Console may have conflicts with Post Script (PS) fonts installed on the workstation. The conflict results in spacing problems with the text displayed in the System Management Console GUI. The text generates an extra space, cutting off part of the text underneath. See the following figure for a representation of the problem.

Figure 51 Example of spacing problem generated by PS fonts



To resolve this problem, PS fonts on the workstation need to be removed from the WINNT directory. PS fonts have the file extentions .PFB and .PFM.

1. On the workstation, navigate to the font folder.

   C:\WINNT\Fonts

2. Identify and remove font files with the extensions .PFM or .PFB

3. Restart the System Management Console. If the System Management Console still displays the problem, double check the WINNT\Fonts directory for font files with the .PFM or .PFB extension.