



# Release Notes for Cisco Media Gateway Controller Node Manager Release 2.3

---

February 8, 2007

## Contents

- [Introduction, page 1](#)
- [Software Release History, page 2](#)
- [System Requirements, page 8](#)
- [Supported Network Elements, page 8](#)
- [Installation Procedure Checklist, page 9](#)
- [Upgrade Procedure Checklist, page 9](#)
- [Patch Procedure, page 10](#)
- [Hints and Tips, page 11](#)
- [Configuring the CEMF Software for Maximum Performance, page 13](#)
- [Configuring Raw Filesystems in ObjectStore, page 13](#)
- [Troubleshooting, page 14](#)

## Introduction

The Cisco Media Gateway Controller (MGC) Node Manager (Cisco MNM) is an element management system (EMS) for the Cisco Media Gateway Controller Node, a call control node based on the Cisco PGW 2200 Softswitch. Cisco MNM provides basic management of the Cisco Media Gateway Controller Node devices including fault, configuration, performance and security.

Cisco MNM 2.3(2) is built on version 3.2 of the Cisco Element Management Framework (CEMF) software package. This release adds support for Cisco MGC host call control software Release 9.3(2) and provides backward-compatibility across older versions of the software, including the 7.4(11), 7.4(12), and 9.x releases.



---

Corporate Headquarters:  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

These release notes describe the features and caveats for Cisco MNM. Please read this entire document prior to using Cisco MNM as it contains pertinent information about installing, configuring, and using the software. This document provides up-to-date information about the current release of the Cisco MNM from Cisco Systems, Inc.

For more information on the Cisco MNM software, please visit Cisco's Web site at:

<http://www.cisco.com> > Products and Services > Network Management > Cisco Media Gateway Controller Node Manager.



Note

The Cisco PGW 2200 PSTN Gateway has been renamed as the Cisco PGW 2200 Softswitch. Older names of this product are the Cisco VSC 3000 and Cisco SC 2200. Some documents may still use the older names.

## Software Release History

### Release 2.3(2)

Release 2.3(2) supports Cisco MGC Release 9.3(2) software.

Cisco MNM 2.3(2) adds support for managing the features new in Cisco MGC Release 9.3(2), as shown in [Table 1](#). Enhancement identification numbers are listed where applicable.

**Table 1** *New Features for Software Release 2.3(2)*

Enhancement Identifier	Description
CSCdx05581	Configurable ISUP timer: Only flow-through provisioning is supported; this property does not appear in the Map Viewer.
CSCdx05899	Dual CLI interworking with Voice over IP network, both signaling path and call control: A new property is added to Trunk Group and Signaling components.
CSCdx21438	Performance measurements added for OVL-GROUP, STATE-GROUP, TCAP-GROUP, SCCP-GROUP, and CALL-GROUP
CSCdx53946	BAMS CICS performance measurements added (average number of defined CICS during the measurement period and average number of available CICS during the measurement period).
CSCdx77415	Because the Cisco PGW no longer supports rtrv-eqpt and set-eqpt-state, these fields are removed from the Advance Diagnostics dialog box and the equipment State attribute is removed from hostCard component properties.
CSCdx81140	New Dial Plan properties and measurements
CSCdx81205	H.323 features (new properties and performance measurements)
CSCdx89243	Incoming traps were previously logged in the mgcTrapProcessor.log file along with possibly distracting Cisco EMF log messages. For easier viewing, incoming traps are now logged separately in trapLog.log.
CSCdy10887	Raise an informational alarm after the completion of Cisco PGW discovery.
CSCdy11911	SIP to SIP calling (new performance measurement)

**Table 1** *New Features for Software Release 2.3(2) (continued)*

Enhancement Identifier	Description
CSCdy16650	NCH billing: Support for changed format of trunk group name in BAMS measurement file.
CSCdy26219	Flow-through provisioning: The PTC can manually initiate discovery of the Cisco PGW configuration.
CSCdz40390	Discover, store, and display additional HSI parameters, and upload them to PTC for flow-through provisioning.
CSCuk35423	Instructions for installation of the CiscoView security module, necessary for launch of CiscoView, are added.
CSCuk36212	Support for HSI diagnostics.
	Launch VSPT in appropriate mode based on user privileges.

## Caveats Resolved in Release 2.3(2)

The following caveats were resolved in this release:

**Table 2** *Resolved in Release 2.3(2)*

DDTS Number	Description
CSCdy01369	The Cisco MGC host controller crashes when the Cisco SC2200 is down.
CSCuk35098	mgeTrapProcessor fails to start.
CSCdy59812	A note was added to the User's Guide explaining that details of DPC properties appear on the Signaling Path Properties Details tab.
CSCdw25644	Performance polling did not support secondary standby state; this has been corrected.
CSCuk38672	Cisco MNM mistakenly generates continuous internal alarms against the second Ethernet interfaces on the Cisco MGC host.

## Release 2.3(1)

### Release 2.3(1) Patch 3 Information

The following caveats were resolved in Release 2.3(1) Patch 3:

**Table 3** *Resolved in Release 2.3(1) Patch 3*

DDTS Number	Description
CSCdy01369	The Cisco MGC host controller crashes when the Cisco SC2200 is down.

## Release 2.3(1) Patch 2 Information

The following caveats were resolved in Release 2.3(1) Patch 2:

*Table 4 Resolved in Release 2.3(1) Patch 2*

DDTS Number	Description
CSCdy62462	PTC not able to delete nailed trunks.

## Release 2.3(1) Patch 1 Information

The following caveats were resolved in Release 2.3(1) Patch 1:

*Table 5 Resolved in Release 2.3(1) Patch 1*

DDTS Number	Description
CSCuk36274 ST	MNM in haterras configuration overloads. hostController was updated to only listen to the events that it is interested in.
CSCuk36446 ST	MNM Eldora object does not recognize link up trap. The trap OID was incorrectly mapped for SNMPv1 trap and it is corrected.
CSCuk36488 ST	MNM incorrectly maps some traps from BAMS fixed trap mapping rules for BAMS to account for all severities.
CSCuk36453 ST	MNM trap forwarding script needs to restart trapmanager after clearing all the destination information. The script is fixed and now it restarts the Trap Manager.
CSCuk35190 ST	MNM does not provide full info about HSI traps. The alarm description is enhanced and now it displays the before and after states for state transition alarms.
CSCdx65605	Unreachable alarm does not get cleared.
CSCdx66311	SLT Chassis does not recover from Unreachable state.

## Release 2.3(1) Information

The following caveats were resolved in Release 2.3(1):

*Table 6 Resolved in Release 2.3(1)*

DDTS Number	Description
CSCdx78754	mgcController crashes when HSI is configured with a MGC hostname.
CSCuk35098	CMNM 2.3 mgcTrapProcessor fails to start.
CSCdx65289	Provisioning through Northbound, error, could not fork process.
CSCdx81252	Change naming convention for Embedded SLT and proxy.
CSCdx70380	Unable to collect trunkgroup performance data from BAMS P2.
CSCdx74987	cemf install show:Package deype shows Manager on client install.
CSCdw67888	NF: Cisco MNM support for Circuit Reservation.

**Table 6** *Resolved in Release 2.3(1)*

DDTS Number	Description
CSCdw70210	NF: Route Advance and Redirection on Cause Code.
CSCdw85016	NF: Cisco MNM help support for multiple documents.
CSCdw87816	SLT (Eldora) Support for Cisco MNM needed.
CSCdx02314	SLT 2651 reload traps not understood at Cisco MNM.
CSCdw24133	Support for CV5.4 in Cisco MNM 2.3(1).
CSCdw54369	NF: Cisco MNM support for HSI.
CSCdx23574	Trap Forwarding feature should be removed from Cisco MNM.
CSCdx30915	Cisco MNM performance threshold for PGP counters for Singtel.
CSCdx34369	Remove TrapLog process.
CSCdx38263	Cisco MNM should discover BAMS node name and use it.
CSCdx53946	NF: Add new performance counters for BAMS.
CSCuk33129	Cisco MNM upgrade procedure warns about installing all EMs.
CSCuk33268	When exporting seed file without no name given, nothing happens.
CSCdw57290	NF: Cisco MNM support of Cat6509.
CSCdw54321	NF: INAP-Based Pre-Paid Card Service.

## Release 2.1(2)

The following caveats were resolved in Release 2.1(2):

**Table 7** *Resolved in Release 2.1(2) Patch Level 01*

DDTS Number	Description
CSCdv61281	NF: Country Code Prefix Per Trunk Group Capability.
CSCdw15883	Change MGC Product Name References.
CSCdw21473	Need flow-through interface to support taking resource OOS.
CSCdw31812	Flow through provisioning and upload support needed for GTD parameters.
CSCdw61830	Discovery of ELDORA SLTs core dumps Cisco MNM.
CSCdx04478	Cisco MNM does not support some BAMS performance counters.
CSCdx36796	Cisco MNM does not support flow-thru provisioning for all ISDNPRI prop.
CSCdx44222	Upload of nailed trunk information fails.
CSCdx53946	NF: Add new performance counters for BAMS.
CSCdx65289	Provisioning through Northbound, error, could not fork process.
CSCdx70380	Unable to collect trunkgroup performance data from BAMS P2.
CSCuk32750	Cisco MNM does not retrieve pfce measurements from BAMS 3.09.

*Table 7 Resolved in Release 2.1(2) Patch Level 01 (continued)*

DDTS Number	Description
CSCuk32751	CMNM shows BAMS informational trap every 15 minutes.
CSCuk32926	Cisco MNM generates core and crashes randomly.

## Release 2.1(1)

- The Backup/Restore feature has been removed. This feature is now supported in VSPT.
- Cisco MGX support has been removed. Cisco MGX is now supported in the Cisco MGM Element Manager.
- Online documentation added.
- Cisco MNM has been enhanced to display performance data for SS7Path.
- A new dialog box has been created for Dial Plan properties.
- Added upgrade option to provide ability to upgrade from Cisco MNM 1.5 to Cisco MNM 2.x.

The following caveats were resolved:

*Table 8 Resolved in Release 2.1(1)*

DDTS Number	Description
CSCdr30073	Need to get PM data from failed VSC after a switch over.
CSCdr30073	CMNM need to get performance data from failed VSC after a switch over.
CSCds30084	CMNM need to handle the case when user deploys more than two MGC hosts in a MGC node.
CSCds57400	VSC performance counter units are undefined.
CSCdt09317	Output of the tool to retrieve admin state has misleading info.
CSCdt11172	Performance data for most of CAS measurement group missing.
CSCdt14890	Discovery of Network through seed file is not complete.
CSCdt28893	VSCs state does not appear correctly in the viewer.
CSCdt28931	Rambler does not show peer port information on c7Ip links.
CSCdt37692	Cannot handle v1 cold start trap from VSC.
CSCdt40336	cmnmversion command does not display the correct information in Release 2.0.
CSCdt40353	Release Notes do not mention upgrade procedure for CMNM 2.0.
CSCdt56464	Ramblers diagnostic tools do not respond if invalid uid/pwd.
CSCdt60865	CMNM does not mask out the password during deployment.
CSCdt68946	The navigation menu for the administration dialog should be removed.
CSCdt92769	Status check for admin states gives invalid information.
CSCdt92778	Error with MGC Host Diagnostics status check for linksets.
CSCdt93960	Import from seed file does not discover signalling.

**Table 8** *Resolved in Release 2.1(1) (continued)*

DDTS Number	Description
CSCdu01430	Cleared event in event browser has wrong text.
CSCdu01987	Reboot operation for SLT requires that SLT be deployed with a userid.
CSCdu06927	Some warning messages appear in the log file.
CSCdu33193	BAMS does not get associated with a MGC Node.
CSCdv04298	BAMS node does not get discovered when deployed using seedfile.
CSCdv05092	BAMS doing auto-discovery every 1 hour instead of every 6 hours.
CSCdv05146	Unable to launch Xterm application on BAMS phase 3.
CSCdv05182	MML output is messed up.
CSCdv05411	BAMS nodes get reparented incorrectly.
CSCdv08718	BAMS node does not get deployed while deploying BAMS phase 2.
CSCdv08810	trkGrp properties missing in 9.1.5.
CSCdv21607	Installation script stops after backing up DB.
CSCdv22701	Install: The CEMF_PATCH_LEVEL variable was getting set.
CSCdv22720	Install: CMNM packages do not display in cemf show cmd.
CSCdv22720	CMNM EMs are now displayed with the cemf show command.
CSCdv27591	Manually transitioning VSC from hung discovery state to active state.
CSCdv35277	All SLT interfaces are shown as unreachable.
CSCdv38256	Install: Remove mgxEM from CSCOCmnmm install.
CSCdv38256	The mgxEM has been removed from CMNM.
CSCdv39487	Process status diagnostic tool doesnt work on BAMS 3.04.
CSCdv39570	Cisco MGX 8260 support has been removed.
CSCdv44635	ST. CMNM cant reboot the MGC host(userdoc).
CSCdv47874	Cannot upload/flow through provision some nas path properties.
CSCdv73019	Unable to retrieve node properties for BAMS P2.
CSCdv76921	Change chassis snmp community string not propagated to child.
CSCdv77983	SLT device unreachable alarm not cleared.
CSCdv82497	Install: update required CEMF patch version from 1 to 4.
CSCdv88044	CMNM fails to bring up the trunkgroup property screen.
CSCdv88124	CMNM fails to get operational status of linkset component.
CSCCuk23874	CMNM. Status of C7IPlink misses first letter.
CSCCuk25971	NMS. CMNM does not find VSPT Release 2.1.
CSCCuk26527	ST. CMNM fails to get a large dialplan.
CSCCuk27716	ST. CMNM cant reboot the MGC host.

# System Requirements

The following is the minimum hardware and software you need to install and run Cisco MNM:

- Sun Ultra 60 workstation with 2 CPUs (440 MHz or faster)
- Sun Solaris 8 operating system
  - April 2001 release recommended
  - Open Windows with the Common Desktop Environment (CDE)
- 2.0 GB of RAM (or greater)
- 9 GB SCSI drives properly configured. The database drives should be configured as RAW devices and connected to a separate SCSI controller for maximum performance.
- The tmpfs file system must be mounted to /tmp for maximum performance.
- ObjectStore (Cisco Element Management Framework (CEMF) database program) should be configured to use raw file systems



**Note**

Detailed system requirements are documented in Chapter 2 of the *Cisco Media Gateway Controller Node Manager User's Guide*. Review this chapter prior to installing or configuring the software.



**Note**

Installing drives greater than 9 GB does *not* result in performance gains. The main bottleneck of the CEMF application is hard disk input/output (i/o) speed, not capacity. Maximum performance is achieved using many drives of lower capacity instead of a few, larger capacity drives.

# Supported Network Elements

The following network elements have been tested and verified to work with this release 2.3(2) of the Cisco MNM.



**Note**

All other releases of Network Element Software have not been tested and are not supported with this release.

- PGW 2200:  
7.4(11), 7.4(12), 9.14(T), 9.1(5), 9.2(2), 9.3(1), and 9.3(2)
- Billing and Measurement Server (BAMS):  
2.63, 2.64, 2.65, 2.67i, 2.68, 3.08, 3.10, and 3.12
- H.323 Signaling Interface (HSI)  
2.21 (backward compatible with 2.20)
- Catalyst 5500 or 6500:  
5.x or higher
- Catalyst 2900XL:  
Cisco IOS Release 12.x



- SLT:  
Cisco 2611 or 2651 router running Cisco IOS Release 12.1(x), 12.2(x)  
Cisco 2611XM router running Cisco IOS Release 12.2(11)T2
- Integrated SLT  
Cisco AS5350 or AS5400 access server running Cisco IOS Release 12.2(10.6)T
- Cisco EMF: Cisco MNM 2.3(2) has been tested and verified with CEMF 3.2 patch 3 and CEMF 3.2 Patch 4.

## Installation Procedure Checklist

Before installing the software, read Chapter 2, *Installing CMNM*, of the *Cisco MGC Node Manager User's Guide*. If you are setting up a client/server architecture, then the CEMF and Cisco MNM software must be installed on both the client and server workstations. The Cisco MNM installation software determines whether the client or manager software should be installed.

- Verify that the minimum hardware requirements pertaining to your site have been met
- Ensure that the computer is in DNS
  - Ensure that the computer is using DNS  
The computer must have a valid entry in DNS.
  - If the computer is not using DNS, disable Name Resolution completely (that is, there should be no `/etc/resolv.conf` file).
- Verify that the CEMF software has been installed and is running (the CEMF software must be running for the Cisco MNM software to be installed.)



### Note

---

Refer to the “Installing CMNM” section in the “Cisco Media Gateway Controller Node Manager Users Guide” for detailed instruction on how to mount the CD-ROM.

---

- Step 1** Become the root user.
- Step 2** Place Cisco MNM CD in the CD-ROM drive.
- Step 3** Change to the `/cdrom/cdrom0` directory
- Step 4** Execute the command: `./installCSCOcmnm`.
- Step 5** Follow the on-screen prompts.
- Step 6** Eject the CD-ROM when the installation is complete.

## Upgrade Procedure Checklist

The Cisco MNM upgrade process enables you to easily upgrade from Cisco MNM Release 1.5. Refer to the “Upgrading from CMNM Release 1.5” section of the “Cisco Media Gateway Controller Node Manager Users Guide” for detailed instructions on how to mount the CD-ROM.

- Step 1** Become the root user.

- Step 2 Place Cisco MNM CD in the CD-ROM drive.
- Step 3 Change to the `/cdrom/cdrom0` directory.
- Step 4 Execute the command `./installCSCOcmnm -upgrade`.
- Step 5 Follow the on-screen prompts.
- Step 6 Eject the CD-ROM when the installation is complete.

## Patch Procedure

The Cisco MNM patch process is cumulative. Downloading and installing the latest patch installs all previous patches. The patch process automatically determines which portions of the Cisco MGC Node Manager need to be patched. In order for you to install a patch, the base Cisco MGC Node Manager software must be installed. Use the following steps to install the desired patch.

- 
- Step 1 Verify that the base Cisco MGC Node Manager software is installed.
  - Step 2 Become the root user.
  - Step 3 Create a temporary installation directory `/opt/cmnm_tmp_install`.
  - Step 4 Download the patched software:
    - a. Go to [www.cisco.com](http://www.cisco.com).
    - b. Log in.
    - c. Navigate to *Technical Support > Software Center > Products and Downloads > Voice Software*. On this page find and click on *Cisco Media Gateway Controller Node Manager*. You go to the patch download page.
    - d. Download the desired patch to the temporary installation directory.
  - Step 5 Extract the patched software. For example, you can use:
 

```
zcat CSCOcmmnPatch_0x.tar.Z | tar xvf -
```
  - Step 6 Execute the command: `./patchCSCOcmnm`
  - Step 7 Follow the on-screen prompts.
- 

## Known Issues and Operational Recommendations

This section contains information about known issues and the corresponding workarounds.



### Note

For more information about Cisco IOS issues and workarounds, see the Cisco IOS release notes for your platform.

## Cisco MNM Checks for Available Disk Space For Installation

During installation, Cisco MNM detects how much disk space is available for installation. If the system does not have enough available disk space, you are prompted whether you want to continue the installation routine. If you enter 'N' to stop the Cisco MNM installation, the installation continues.

The workaround is to ensure that enough free disk space is available before Cisco MNM is installed. The amount of disk space required is detailed in the Cisco MNM installation guide.

## Cisco MNM Cannot Discover an Interface or IP Address for BAMS

Sometimes Cisco MNM reports that it cannot discover an interface or IP address for BAMS. This might be caused by the mib2agt getting into a *strange* state. You can restart the mib2agt by stopping the current process. The new process mib2agt is restarted automatically.

```
ps -ef | grep mib2agt
kill -9 <PID>
```

## Using the VNC Viewer to Access Cisco MNM Remotely

X terminal remote access to Cisco MNM has been tested with Reflection X. If you use the AT&T Virtual Network Computing Viewer to access Cisco MNM remotely, you may encounter a display problem when you launch the Cisco MGC Host Toolbar, caused by the current Cisco MNM address translation process.

### To display the Cisco MGC Toolbar launched from Cisco MNM:

In the VNC Viewer window before launching Cisco MNM, set the display by doing one of the following (depending on which shell you are using):

If you are using “sh” or “bash”, run this command:

```
export DISPLAY=10.1.1.1:n.0
```

If you are using “csh”, run this command:

```
setenv DISPLAY 10.1.1.1:n.0
```

where *10.1.1.1* is the IP address of the VNC host (usually the Cisco MNM presentation server) and *n.0* is the port ID that matches the instance of the VNC server you are logging into.

You may then launch Cisco MNM normally and PGW tools will be properly displayed.

## Hints and Tips

### Initial Cisco MNM Configuration

Cisco MNM is initially configured with one user:

```
id: admin
password: admin
```

## Sample Network Seed File

A sample network seed file is located at: <CEMF Directory>/samples/seedfile.txt. To access the <CEMF Directory>, enter the following command:

Manager:

```
pkgparam CSCOcemfm BASEDIR
```

Client:

```
pkgparam CSCOcemfc BASEDIR
```

## Installing CEMF/Cisco MNM on a Server

If you have installed CEMF/Cisco MNM on a server and need to change the IP address/hostname, you must make the changes shown in the following procedure:



Note

---

The following example uses the hostname CMNM and the IP address 10.1.1.1.

---

**Step 1** #cd <CEMF Directory>/bin

**Step 2** #./cemf stop

**Step 3** Edit /var/adm/Atlantech/system/info to reflect the following hostname and ip address:

```
MGRHOSTNAME=rambler
MGRIPADDRESS=10.1.1.1
COREHOSTNAME=rambler
```

**Step 4** Edit <CEMF Directory>/config/env/avCore.sh to reflect the hostname in the lines below, and save the file.

```
MgrSystemManager=rambler1270; export MgrSystemManager
PortAllocator=rambler1270; export PortAllocator
transRouter=rambler1271; export transRouter;
```

**Step 5** Edit /var/sadm/pkg/CSCOcemfm/pkginfo to reflect the following values:

```
MGRIPADDRESS=10.1.1.1
MGRHOSTNAME=10.1.1.1
COREHOSTNAME=10.1.1.1
LOCALHOSTNAME=10.1.1.1
```

**Step 6** You will also need to make these same changes for each Element Manager. To do so, edit the following files:

```
/var/sadm/pkg/hostEM/pkginfo
/var/sadm/pkg/mgcEM/pkginfo
/var/sadm/pkg/mgxEM/pkginfo
```

**Step 7** Rename <CEMF Directory>/ODI/OS5.1/ostore/<hostname>\_server\_parameter to reflect the new hostname.



Note

---

You must obtain a new CEMF license. For information on obtaining a new CEMF license, refer to “CEMF Licensing” in the “Troubleshooting” section.

---

Step 8 <CEMF Direcory>/bin/cemf start

---

## Configuring the CEMF Software for Maximum Performance

The following are guidelines for installing CEMF:

- Use the primary drive for the Solaris operating system and the ObjectStore transaction log.
- The second drive should contain the CEMF software (that is, /opt/cemf).
- Configure the ObjectStore database for Raw FileSystems. The remaining hard drives should contain the RAW FileSystem partitions for the CEMF database (preferably on a separate SCSI controller).

Mount the tmpfs file system to /tmp so the ObjectStore cache files can be kept in memory. ObjectStore is the database program included with CEMF. Keeping the cache files in memory provides for an enormous performance boost for CEMF. Here is how the tmpfs line should read in the /etc/vfstab file (the blank areas between the keywords are spaces):

```
swap - /tmp tmpfs - yes -
```

## Configuring Raw Filesystems in ObjectStore

By default, the CEMF database system (ObjectStore) is configured to use typical cooked file systems (that is, filesystems with readable directory entries) for the database. However, database performance is maximized when ObjectStore is configured to use Raw file systems. To achieve maximum performance, the hard drives containing the Raw file systems should be on a separate SCSI controller (not on the same controller as the primary operating system drive). The following should be noted:

- Partition the hard drives when you install the Solaris operating system.
- Type the command, **/bin/pkgparam CSCOcemfm BASEDIR** to get the installation directory for the CEMF software.
- All Raw partitions must be exactly the same size (in MB). ObjectStore does not use partitions of different sizes.
- The Raw partition names (that is, **/dev/rdisk/c0t1d0s3**) must be available before starting the configuration session.
- Determine the name of the machine (for example, cemfserver).
- Adding, modifying, and/or deleting Raw File systems resets the ObjectStore database and destroys any existing data there.

Complete the following steps to start the ObjectStore and CEMF processes:

- 
- Step 1** Log in to the system as the root user.
- Step 2** Using the following command, stop the current CEMF processes:  
**/etc/init.d/cemf stop**
- Step 3** Shut down ObjectStore:  
**/etc/rc2.d/S80ostore4 stop**
- Step 4** Shut down the AV license manager:  
**/etc/rc2.d/S98avlm stop**

- Step 5** Start a CEMF shell:  
`/etc/rc2.d/S99cemf shell`
- Step 6** Change to the CEMF installation directory:  
`/opt/<INSTALL_DIR>`
- Step 7** Change the directory to `./ODI/OS5.1/ostore/etc` (under `/opt/<INSTALL_DIR>`).
- Step 8** Edit the hostname server parameter file (`<hostname>_server_parameters`) with the following modifications:
- Put a comment character `#` at the beginning of the Log File line. This places the transaction log in the Raw partition and improves performance.
  - Add an entry for each Raw Partition ObjectStore will use. Each line must begin with `PartitionX:` (where X is a number, starting with zero and incrementing by one).



**Note** Don't forget the colon character.

- Each line must have the word `PARTITION` as the second element.
- Each line must have the Raw partition listed as the last element (use the `rdsk` partition identifier).
- Example:

```
unix-shell#> cd /opt/CSCOcemf/ODI/OS5.1/ostore/etc
unix-shell#> cat cemfserver_server_parameters

#Log File: /opt/transact.log
Partition0: PARTITION /dev/rdsk/c2t9d0s0
Partition1: PARTITION /dev/rdsk/c2t10d0s0
Partition2: PARTITION /dev/rdsk/c2t12d0s0
Partition3: PARTITION /dev/rdsk/c2t13d0s0

unix-shell#>
```

- Step 9** Change directory to `<CEMF_INSTALL>/ODI/OS5.1/ostore/lib`. For example, `/opt/CSCOcemf/ODI/OS5.1/ostore/lib`.
- Step 10** Run the command `./osservice -i` to reinitialize ObjectStore. Answer **yes** when prompted to reinitialize the database.
- Step 11** Run the command `/etc/init.d/cemf reset` to reset the CEMF database. Answer **yes** when prompted.
- Step 12** Run the command `/etc/init.d/cemf start` to start the ObjectStore and CEMF processes.  
 ObjectStore is now using RAW databases.

## Troubleshooting

### Viewing Core Files Generated by CEMF and Cisco MNM

Use the `/opt/cemf/bin/listCores` command to view all core files generated by CEMF and Cisco MNM.

## CEMF Licensing

If you are having problems with CEMF licensing, you might need to stop and restart the license manager daemon. To do so, execute the following commands:

```
#> /etc/rc2.d/S98alvm stop
#> /etc/rc2.d/S98alvm start
```



Note

---

The CEMF licenses are fixed for a particular machine. You cannot copy the license file from one machine to another. If you want to install the CEMF software on another machine, you must contact Cisco TAC and ask for a new license. You will need the hostname and hostid of the new machine.

---

## Viewing the Most Recently Changed Log Files

Cisco MNM log files are stored in <CEMF Directory>/logs. You can view the most recently changed log file with **ls -lt** command.

## Interesting Cisco MNM Log Files

Some interesting Cisco MNM log files are:

- hostController.log [MGC Host]
- mgcController.log [MGC Node]
- trapLog.log Incoming traps are logged here, to separate them from CEMF log messages collected in mgcTrapProcessor.log.

## Error Messages That Are Safe to Ignore

Most of the entries in the Cisco MNM log files are created by the CEMF platform and are of limited value. The following error messages are safe to ignore:

- SNMP and MIB parsing errors (which display when an EM controller starts):
  - SNMP : ERROR mib.cc:1283 Mib Object is already on the tree for .
  - SNMP : ERROR mibDependencyMgr.cc:191 mibDependencyMgr.cc:196 Mib . not defined
  - SNMP : ERROR mibParser.y:359 EXPORTS are currently ignored (;, line 8)
  - SNMP : WARN mibParser.y:1154 Name and number form OIDs are not properly implemented ().
- Database warning (which display when an EM controller is first installed):
  - general : WARN Creating Database /opt/AV3/db/mgcController.db
- General errors (which display when the EM controller starts up):
  - general : ERROR Unable to get event channel ID for channel ''
  - general : ERROR EventChannelManager : Failed to find location for event channel
  - general : WARN OGManager::OGManager - Unable to get deleteEventChannel from .ini file
  - general : ERROR OGManager::processGroupClass - invalid class id

- general : ERROR EventChannelManager : Failed to find location for event channel ERROR OGManager::processGroupClass - invalid class id
- general : ERROR OGChangeEventHandler::process - could not find drep!
- general : ERROR IdAllocatorOS : Deprecated constructor called
- Task : WARN PerfPollTask::createGroupsResult : group . already exists.
- mgcController : WARN Controller::initialiseController Controller is configured NOT to auto populate tech tree on autodiscover
- Other misc errors:
  - general : WARN CommsBuffer::serialize - resizing buffer size
  - general : ERROR PersistentAttributeStore::PersistentAttributeStore() nameInit = 'xxx. is longer than 16 characters. All Objectstore segment comments will be truncated to use the first 16 characters.

## Resetting the User Password

If you forget your password, you can reset the CEMF user IDs and passwords. The following command removes all passwords, and resets the admin user ID's password to *admin*.

```
<CEMF Directory>/bin/cemf shell
<CEMF Directory>/bin/partitioningTool -r
```

## Backing Up and Restoring the CEMF/Cisco MNM Databases

The following command backs-up the CEMF/Cisco MNM databases. By default the backup files are placed in */opt/AVBackup*.

```
/opt/CSC0cemf/bin/cemf stop
/opt/CSC0cemf/bin/cemf backup
/opt/CSC0cemf/bin/cemf start
```

The following command will restore a CEMF/Cisco MNM database.

```
/opt/CSC0cemf/bin/cemf stop
/opt/CSC0cemf/bin/cemf restore -t mm-dd-yyyy
/opt/CSC0cemf/bin/cemf start
```

For more information on backing up and restoring CEMF/Cisco MNM Databases refer to the “Cisco EMF Database Backup and Restore Procedures” section of the *Installing, Licensing, and Configuring Cisco EMF Manual*.

## Forcing an Uninstall of an Element Manager

The CEMF daemons must be running for the Element Managers (EMs) to uninstall. There are two ways to force an uninstall of an EM; both cause loss of all CEMF/Cisco MNM data. Before running these commands, it is recommended that you back up your databases.

The *uninstallCSC0cmnm* script can be invoked with an undocumented option to force the removal of all or one EM. From a command line, as root, type the command:

```
/opt/CSC0cemf/uninstall/uninstallCSC0cmnm -force [-em <EM>]
```



You can specify only one EM to remove or all EMs by omitting that parameter. The list of EMs includes hostEM, mgcEM, andmgxEM.

Example:

```
/opt/CSCOcemf/uninstall/uninstallCSCOcmnm -force -em mgxEM -em mgcEM
```

After you run this command, the CEMF databases are corrupted. To correct this problem, reset the CEMF databases by running the following command. You must do this before using CEMF again, even using CEMF to reinstall Cisco MNM.

```
/opt/CSCOcemf/bin/cef stop
/opt/CSCOcemf/bin/cef reset
/opt/CSCOcemf/bin/cef start
```

After you have successfully reset the database and restarted CEMF, you must reinstall Cisco MNM. If you want to restore a CEMF/Cisco MNM database after you have reinstalled Cisco MNM, refer to “Backing up and restoring the CEMF/CMNM Databases” in the preceding section.

If the above method doesn't remove the EMs, then you can try another method. When the EMs are installed, Solaris package information is placed in subdirectories of /var/sadm/pkg. The subdirectory is the name of the package, as specified above (that is, hostEMm, mgcEMm, and so on.). As the root user, complete the following steps for each EM that you want to remove.

```
/opt/CSCOcemf/bin/cef stop
touch /var/sadm/pkg/<EM>/install/.avload
pkgrm <EM>
/opt/CSCOcemf/bin/cef reset
/opt/CSCOcemf/bin/cef start
```

Example:

```
/opt/CSCOcemf/bin/cef stop
touch /var/sadm/pkg/mgcEMm/install/.avload
pkgrm mgcEMm
/opt/CSCOcemf/bin/cef reset
/opt/CSCOcemf/bin/cef start
```

To restore a CEMF/Cisco MNM database after you have reinstalled Cisco MNM, refer to the preceding “Backing Up and Restoring the CEMF/CMNM Databases”.

## Managing Network Devices Over a Slow Link

If you are managing network devices over a slow link (T1 or slower), you might need to alter SNMP parameters used by Cisco MNM for SNMP Get Requests. You can change these parameters for any existing objects by accessing the States dialog. You can also change these parameters in the Advanced tab of the Seed File Deployment dialog.

The default number of SNMP retries is 2. You might need to increase this value when the Cisco MNM workstation is connected to network devices over a slow link.

The default SNMP timeout value is 5000 milliseconds (5 seconds). You may need to increase this value when the Cisco MNM workstation is connected to network devices over a slow link.

## Maximizing Logfile Output

By default Cisco MNM logs only warning and error messages. If you want to turn on debug messages in all log files, complete the following steps, as the root user:

- 
- Step 1 **cd <CEMF Direcory>/bin**
- Step 2 **./cemf stop**
- Step 3 **cd <CEMF Direcory>/config/init**
- Step 4 Edit loggercommon.include and add or change the following line:  
**loggingLevelMask = 12**
- Step 5 **cd <CEMF Direcory>/bin**
- Step 6 **./cemf start**
- Step 7 To set the logging level back to warning, add or change the following line:  
**loggingLevelMask = 10**
- 

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems  
Attn: Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

---

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)