



Cisco Media Gateway Controller Node Manager Installation Guide, Version 2.6(1)

December, 2005

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-9109-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0406R)

Cisco Media Gateway Controller Node Manager Installation Guide, Version 2.6(1)
Copyright © 2005, Cisco Systems, Inc.
All rights reserved.



Preface	v
Audience	v
Conventions	v
Product Documentation	vi
Obtaining Documentation	vi
Cisco.com	vi
Product Documentation DVD	vii
Ordering Documentation	vii
Documentation Feedback	viii
Cisco Product Security Overview	viii
Reporting Security Problems in Cisco Products	viii
Obtaining Technical Assistance	ix
Cisco Technical Support & Documentation Website	ix
Submitting a Service Request	x
Definitions of Service Request Severity	x
Obtaining Additional Publications and Information	x

CHAPTER 1

Installation Overview and Planning	1-1
Installation Overview	1-1
Who Should Install Cisco MGC Node Manager?	1-1
Determine Your Hardware Requirements	1-2
Supported Configurations	1-3
Hardware Requirements	1-4
Disk Drives and Database Storage	1-4
Installation Checklist	1-5

CHAPTER 2

Installing Cisco MGC Node Manager	2-1
Performing a New Installation of the Cisco MNM	2-1
Task 1: Gather Installation Software and Required Information	2-1
Installation Software	2-1
Required Information	2-2
Task 2: Ensure That Network Devices Have the Correct Software	2-3
Task 3: Plan and Execute Hard Drive Partitioning	2-5
Task 4: Ensure That the Sun Solaris 8 Operating System Is Installed	2-5

- Task 5: Obtain a Cisco EMF License 2-5
- Task 6: Make System Modifications 2-5
 - Setting Up IP and Remote User Access Information 2-6
- Task 7: Install CiscoView 5.4 2-6
- Task 8: Install Cisco EMF 3.2 2-7
 - Installing Cisco EMF Patches 2-7
 - Installing the Cisco EMF SSH Add-On Package 2-8
 - Starting Cisco EMF 2-8
- Task 9: Install Cisco MGC Node Manager 2.6(1) and Verify the Installation 2-9
 - Installing Cisco MGC Node Manager 2-9
 - Verifying the Installation 2-10
 - Verifying Element Managers 2-10
 - Verifying the Installation of CiscoView 5.4 2-11
 - Starting Cisco MGC Node Manager 2-12
 - Getting Started with Secure Communications on Cisco MGC Node Manager 2-13
- Task 10. Install the CiscoView Security Module 2-14
- Task 11: Set Up the X Terminal Workstations for Remote Access 2-15
 - Creating an XDMCP Connection 2-15
 - Creating a Workstation Connection 2-15
 - Fixing the Insufficient Colors Problem 2-16
- Task 12. Synchronize Time 2-16
- Task 13: Configure Network Devices to Forward Alarms 2-16
- Upgrading from Previous Cisco MGC Node Manager Versions 2-16
 - Backing Up Your Databases 2-18
- Uninstalling the Cisco MGC Node Manager Software 2-18
 - Verifying Uninstallation of Cisco MGC Node Manager 2-18
- Displaying Current CMNM Packages 2-19
- Viewing Help for CMNM Install Scripts 2-19
- Uninstalling Cisco EMF 2-19
- Troubleshooting Common Installation Problems 2-20



Preface

This installation guide provides the information you need to install, configure, and use the Cisco Media Gateway Controller Node Manager (Cisco MGC Node Manager). It also contains reference information that might be needed by administrators, service technicians, and users.

Audience

This document is designed for:

- System administrators who install and configure Cisco MGC Node Manager
- Network Operations Center (NOC) personnel who use Cisco MGC Node Manager to monitor the network and respond to events and alarms

This document describes Cisco MGC Node Manager in the context of the Cisco Element Management Framework (Cisco EMF).

Cisco MGC Node Manager enhances some capabilities of Cisco EMF. Your product ships with Cisco MGC Node Manager and Cisco EMF documentation; you need to be familiar with both in order to be proficient with Cisco MGC Node Manager.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

Table 1**Product Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco MGC Node Manager, 2.6(1)</i>	<ul style="list-style-type: none"> On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/ps5539/index.html
<i>Installation Guide for Cisco MGC Node Manager, 2.6(1)</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/ps5539/index.html
<i>User Guide for Cisco Media Gateway Controller Node Manager, Version 2.6(1)</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/ps5539/index.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Instructions for ordering documentation using the Ordering tool are at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Installation Overview and Planning

This chapter provides the overview and planning information you need to carry out a successful installation of the Cisco Media Gateway Controller Node Manager Version 2.6(1) (Cisco MGC Node Manager). Specific procedures for installing the Cisco MGC Node Manager are provided in [Chapter 2](#).



Note

In previous releases the Voice Services Provisioning Tool (VSPT) was packaged together and known as Cisco MGC Node Manager Provisioning Tool.

The chapter contains the following topics:

- [Installation Overview, page 1-1](#)
- [Determine Your Hardware Requirements, page 1-2](#)
- [Installation Checklist, page 1-5](#)

Installation Overview

Successful network management using Cisco MGC Node Manager begins with a well-planned and carefully executed installation. Network element management involves many interdependent factors, including:

- The correct hardware for your environment
- The correct software release and patch levels on the managed devices
- The correct installation of Cisco Element Manager Framework, the foundation software for Cisco MGC Node Manager
- Performing installation tasks in the required order, so that prerequisites are in place when needed

To organize the installation process, use the [“Installation Checklist” section on page 1-5](#) to plan and carry out your installation. Begin by reading it over to understand the major tasks in a successful installation, and check off each task as completed.

Who Should Install Cisco MGC Node Manager?

Installing Cisco MGC Node Manager involves tasks such as setting up hard drives and checking and modifying system files, which are best performed by an experienced system administrator with good knowledge of UNIX and Solaris.

Determine Your Hardware Requirements

The hardware you need and the way you install Cisco MGC Node Manager depend on the size of the network you are managing and the amount of data you collect. This section is designed to help you determine your hardware requirements and software configuration.

Cisco EMF and Cisco MGC Node Manager each comprise server and client software:

- The server software handles network management, including management of the databases that contain network information and store alarm and performance data. The server software also handles the GUI applications with which users interact when the Cisco MGC Node Manager is installed on a standalone server.
- The client software handles the GUI applications with which users interact.

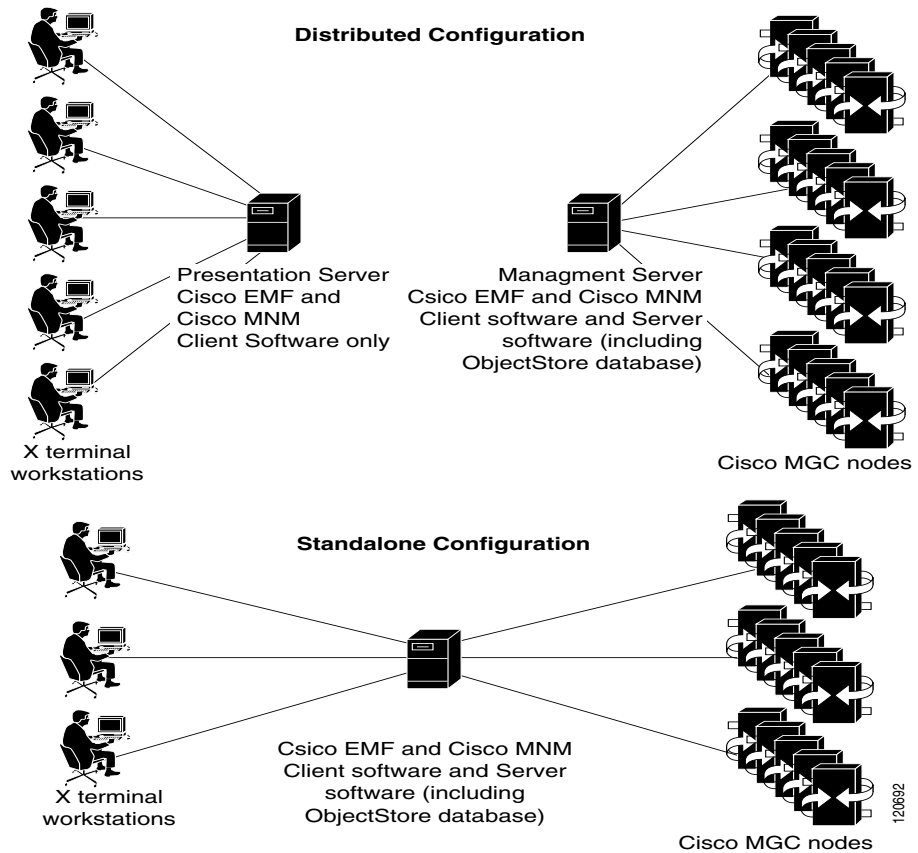
The Cisco EMF and Cisco MGC Node Manager software runs on a separate machine or on machines other than the Cisco MGC host. In a small network, such as a lab, server and client software might reside on a single machine (a standalone configuration). In larger networks, the software is installed on two (or more) machines, in this distributed configuration:

- One machine, known as the Management server, contains the server software (including the ObjectStore database management software included with Cisco EMF) and client software
- One machine, known as the Presentation server, contains the client software only. In some large networks, more than one Presentation server may be required.

In either configuration, users typically access Cisco MGC Node Manager from X terminal workstations that run the Client software through a Telnet session. In the distributed configuration, the X terminal workstations connect directly to the Presentation server to run the Client software.

The two configurations are shown in [Figure 1-1](#).

Figure 1-1 Standalone and Distributed Configurations

**Note**

The management server is sometimes called the Database server. The presentation server is sometimes called the client, GUI, or Application server. To avoid confusion, this document uses Management server and Presentation server consistently, and these terms describe the machines in a distributed configuration, not the software that resides on them.

Cisco MGC Node Manager supports ten simultaneous X terminal users, depending on your processing resources, network size, and the version of Cisco EMF you are running.

Supported Configurations

These configurations are supported:

- Cisco MGC Node Manager and Cisco VSPT installed together on a network management server. (Recommended)
- Cisco MGC Node Manager installed on a network management server and Cisco VSPT installed on a Cisco PGW host machine.
- Cisco MGC Node Manager installed on a network management server and Cisco VSPT installed on a separate server.

**Note**

Other element managers may be installed on the network management server.

**Caution**

Cisco MGC Node Manager should not be installed on a Cisco PGW 2200 host machine.

Hardware Requirements

The Cisco MGC hardware requirements for various network sizes are described in [Table 1-1](#). In addition, except in a very small network, each operator requires an X terminal workstation.

Table 1-1 Hardware Requirements for Cisco MGC Node Manager Host Machine(s)

Network Element	Small Network 1-3 Operators 1-5 Nodes 24 trap / min	Medium Network ¹ 4-5 Operators 6-10 Nodes 36-42 traps / min		Large Network 6-9 Operators 11-20 Nodes 42-54 traps / min	
		Client	Server	Client	Server
Configuration	1 workstation	Presentation server	Management server	Presentation server ²	Management server
RAM (GB)	2	2	2	2	4
Swap (GB)	4	2	4	2	8
Disk drives (9 GB minimum)	4 ³	1	4	1	4-6
CPU (MHz)	2 x 440-1.05 GB	2 x 440-1.05 GB	2 x 440-1.05 GB	4 x 1.05 GB	4 x 1.05 GB

1. Presentation and Management servers may run co-resident for medium networks when faster Sun CPUs are used or operator loads are light. Add more Presentation servers to increase the number of operators supported.
2. Additional Presentation Servers may be added to maintain good operator response time in large networks with heavy alarm traffic.
3. 2 drive machines will work for smaller networks with less traffic and fewer operators. Response time to operator commands slows down as the network grows and additional operators are added.

**Note**

Disk drive requirements are based on the number of drives. The CEMF host machine requires at least the number of drives indicated in [Table 1-1](#).

These are *recommendations* to aid you in planning. The total amount of disk space required depends on many factors, such as the amount of alarm and performance data collected.

Disk Drives and Database Storage

In a medium to large network, using multiple disk drives to store the databases helps alleviate I/O bottlenecks and improves software performance. If you are using multiple disk drives for database storage, or you expect to generate large database files, use raw partitions, as described in the Cisco Element Management Framework Installation and Administration Guide at: http://www.cisco.com/en/US/products/sw/netmgts/ps829/products_installation_and_configuration_guides_list.html

If you are using cooked file partitions, installing more than one drive for database storage does not yield any performance improvements because the databases cannot span multiple partitions.

Installation Checklist

This Checklist provides a summary of all the tasks required for an initial installation of Cisco MGC Node Manager and the Provisioning Tool. Procedures for completing each task are described in the following chapters.

We recommend that you print out the Installation Checklist to guide you during installation.

Sequence matters unless otherwise noted.

___ Before you begin:

Read the Release Notes, which supplement and, if different, take precedence over information here.

[Determine Your Hardware Requirements](#), as described in this chapter.

___ [Task 1: Gather Installation Software and Required Information](#)

___ [Task 2: Ensure That Network Devices Have the Correct Software](#)

___ [Task 3: Plan and Execute Hard Drive Partitioning](#)

___ [Task 4: Ensure That the Sun Solaris 8 Operating System Is Installed](#)

___ [Task 5: Obtain a Cisco EMF License](#)

___ [Task 6: Make System Modifications](#)

___ [Task 7: Install CiscoView 5.4](#). This task is required only if you want to manage Cisco SLTs or LAN switches from Cisco MGC Node Manager, which uses the CiscoView server as the management interface.

___ [Task 8: Install Cisco EMF 3.2](#) If you want to use SSH for secure communications with SSH-enabled network components, this includes installing the Cisco EMF strong cryptographic add-on.

___ [Task 9: Install Cisco MGC Node Manager 2.6\(1\) and Verify the Installation](#)



Note If you are installing any other element managers to run co-resident with Cisco MGC Node Manager, also install them now.

___ [Task 10. Install the CiscoView Security Module](#) (If you are using CiscoView)

___ [Task 11: Set Up the X Terminal Workstations for Remote Access](#)

___ [Task 12. Synchronize Time](#)

___ [Task 13: Configure Network Devices to Forward Alarms](#). This task, required before Cisco MGC Node Manager can collect alarm information from network devices, is covered in the *Cisco MGC Node Manager 2.6(1) User's Guide*, Chapter 2, "Configuring Network Devices for Management."



Installing Cisco MGC Node Manager

This chapter provides detailed instructions for these installation tasks:

- [Performing a New Installation of the Cisco MNM, page 2-1](#)
- [Upgrading from Previous Cisco MGC Node Manager Versions, page 2-16](#)
- [Uninstalling the Cisco MGC Node Manager Software, page 2-18](#)
- [Uninstalling Cisco EMF, page 2-19](#)
- [Troubleshooting Common Installation Problems, page 2-20](#)

Before you begin

- Read the [Installation Overview, page 1-1](#)
- [Determine Your Hardware Requirements, page 1-2](#)
- Print the [Installation Checklist, page 1-5](#) and use it to guide your installation.

Performing a New Installation of the Cisco MNM

Task 1: Gather Installation Software and Required Information

This section describes the software and information you should have on hand before you begin installation.

Installation Software

Cisco MGC Node Manager and Provisioning Tool Software

Your order of Cisco MGC Node Manager includes this software:

- Cisco MGC Node Manager 2.6(1), including:
 - The Cisco MGC Node Manager element managers that work with Cisco EMF
- Cisco Element Management Framework (Cisco EMF) 3.2. The software includes ObjectStore 5.1 Service Pack 7 and 7.1, which provides database management.

- Go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cemf-sp32-sp1> for the latest Cisco EMF 3.2 software (at least Service Pack 7) and the patch Release Note (an Acrobat PDF file such as *CEMF3.2P7DepRelNote.pdf*). For overall version 3.2 Release Notes, go to http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cemf/3_2sp7/notes/index.htm
- If you want to use SSH for secure communications with SSH-enabled network components, also download the cryptographic add-in package available from the network management download page <http://www.cisco.com/kobayashi/sw-center/sw-netmgmt.shtml> under Cisco Element Management Systems - CEMF Strong Cryptographic Software. Download both the CEMF Crypto Add-on Package Software and the CEMF Crypto Add-on Package Installation Guide. You must have authorization to download cryptographic software; if you do not, you are automatically redirected to an authorization request page.
- Cisco documentation, including:
 - Netscape, for displaying Help for browser-based management
 - Cisco MGC Node Manager User's Guide
 - Cisco Documentation CD
- CiscoView 5.4 (unbundled from the Cisco MGC Node Manager installation). Install CiscoView if you want to manage Cisco SLTs or Cisco LAN switches (Cisco MGC Node Manager will use the CiscoView server as the management interface). CiscoView should be installed *before* installing Cisco EMF and Cisco MGC Node Manager.
- The Cisco MGC Node Manager Provisioning Tool (formerly the Voice Services Provisioning Tool). The Provisioning Tool version must match your version of the Cisco MGC software. If you are managing nodes with Cisco MGC hosts running different software versions, you can install multiple Provisioning Tool versions. Cisco MGC Node Manager automatically launches the correct version for the currently selected host.

For the latest VSPT patch, go to <http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-nm>.

For the Cisco MGC Node Manager Release Notes 2.6.1 , go to http://www.cisco.com/en/US/products/sw/netmgmtsw/ps1912/prod_release_note09186a00802c8ce3.html

X Terminal Software

To access Cisco MGC Node Manager from a remote workstation, you should have Reflection 7.2 or above installed. See the “[Task 11: Set Up the X Terminal Workstations for Remote Access](#)” section on [page 2-15](#) for information about X terminal access.

Solaris 8 Operating System

The machines that will run Cisco MGC Node Manager should have the Sun Solaris 8 operating system with Common Desktop Environment (CDE) 1.3 installed.



Caution

The Solaris Language setting must be English and the Locale setting must be English (C-7 bit ASCII). Other Language and Locale choices are not supported.

Required Information

This chart lists information helpful to have before you begin installation. Complete the chart and have it available as you work through the installation tasks.

Table 2-1 Required Information

Information	Where To Find It	Value
Superuser (su) password and privileges	Your UNIX system administrator	
Host name and host ID of the machine where Cisco EMF will be installed (in a distributed configuration, the Management server)	On the machine, enter hostname at the command prompt. The host name displays. At the command prompt, enter hostid . The host ID displays. This is a hexadecimal string that identifies the system, not the IP address.	Hostname: Host ID:
Host IP address of that machine	At the command prompt, enter host . If there are multiple interfaces, select the IP address of the interface where traps will be forwarded (as specified when you configure devices for network management; refer to the Cisco MGC Node Manager User's Guide at http://www.cisco.com/en/US/products/sw/netmgts/ps1912/products_user_guide_list.html , Chapter 3.	
Product Authorization Key for Cisco EMF, to be used in Task 6	On the Cisco EMF product CD sleeve.	
DNS Domain of the machine where Cisco EMF will be installed (in a distributed configuration, the Management server) if your network uses DNS	Your UNIX system administrator	
IP address of CiscoView server, required when you install Cisco MGC Node Manager		IP address

Task 2: Ensure That Network Devices Have the Correct Software

Cisco MGC Node Manager interacts with other software running on the various components of the Cisco MGC node. A potential cause of network management problems, such as failure to discover a device during deployment, is a mismatch between the software on the device and the version or patch compatible with Cisco MGC Node Manager. The software requirements for these components are described in [Table 2-2](#).

**Caution**

Upgrades are released frequently. To be sure that you have any necessary software patch, check the Web site for the latest bulletins and upgrades.

Table 2-2 Required Software Versions for Cisco MGC Node Devices

External Software	Version	Where To Check for Upgrades
Cisco MGC host software	7.4.12 and 9.x through 9.6(1)	For upgrades to the PGW 2200: Go to the Software Center Voice Software download page at http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml . (You will be asked to log in.) On that page, go to <i>Cisco PGW 2200 Node Components - Cisco Media Gateway Controller</i> and click on the desired version. For installation documentation and release notes: Version 9: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/ Version 7: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/
Cisco SLT IOS SS7 image	12.1(x), 12.2(x)	For upgrades: http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:2600&s=Software_Installation#Software_Features_%26_Versions For installation documentation and release notes: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/slt/index.htm
Cisco LAN Switch code	5.x or higher	For upgrades: http://www.cisco.com/public/sw-center/sw-lan.shtml
BAMS	2.63, 2.64, 2.65, 2.67i, 2.68, 3.08, 3.10, 3.12, 3.13	For installation documentation and release notes: http://www.cisco.com/en/US/products/sw/voicesw/ps522/prod_technical_documentation.html
HSI server	2.21 (backward compatible with 2.20)	For installation documentation: http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_user_guide_book09186a0080116d4d.html
Cisco ITP IOS SS7 image	12.2(4)	For configuration documentation: http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_ios_releases_home.html

Task 3: Plan and Execute Hard Drive Partitioning

By default, the Cisco EMF software is installed with the ObjectStore database configured for standard UNIX cooked partitions (partitions with readable directory structures). However, we recommend using raw partitions (partitions without a readable directory structure) for the database drives for larger networks because they offer these advantages over cooked partitions:

- The capability of having databases over 2 GB in size
- The ability to store database files across multiple drives

Refer to the *Cisco Element Management Framework Installation and Configuration Guide* for a description of raw versus cooked partitions and for instructions for partitioning your hard drives.

Task 4: Ensure That the Sun Solaris 8 Operating System Is Installed

Cisco MGC Node Manager machines should have the Sun Solaris 8 operating system with CDE 1.3 installed. The operating system installation script is provided by the hardware manufacturer.

If the Sun Solaris 8 operating system is not already installed, install it according to instructions provided by the manufacturer.

Install the latest J2SE Solaris 8 patch cluster, which can be found at the following URL:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

When the Solaris operating system is installed, go to [Task 3: Plan and Execute Hard Drive Partitioning](#).

**Note**

Please check that Solaris 8 is installed on your Sun hardware. Sun hardware is typically shipped with Solaris 2.7.

Task 5: Obtain a Cisco EMF License

You need a valid license key file available on the system to start Cisco EMF. In a distributed configuration, the license key is required on the Management server.

Refer to the *Cisco EMF Installation and Configuration Guide* at:

http://www.cisco.com/en/US/products/sw/netmgts/ps829/products_installation_and_configuration_guide_book09186a00801a8e04.html

Task 6: Make System Modifications

Two kinds of system modifications are necessary after you have installed the Solaris operating system and set up disk drives:

- Setting up IP and remote user access information, described below
- Checking and, if needed, configuring DNS. Refer the *Cisco EMF Installation and Configuration Guide* at:
http://www.cisco.com/en/US/products/sw/netmgts/ps829/products_installation_and_configuration_guide_book09186a00801a8e04.html

Setting Up IP and Remote User Access Information

After you have installed Solaris and added all hard drives, you will need to edit some files on the Management server that contain data for IP networking and remote user access.

Table 2-3 IP Networking and Remote User Access Files

File	Modification
/etc/defaultrouter	Add the host name and IP address of the default gateway router that provides network access between remote users, network devices, and the standalone system or the Management server.
/etc/default/login	Add a # symbol at the front of the line that says <code>CONSOLE = /dev/console</code> to comment out the line. If you do not comment out this line, users will not be able to login to the machine remotely.
/etc/default/login	Add the login accounts for all users that will be accessing the server by Telnet.
/etc/hosts	Add the Presentation server's host information.

Task 7: Install CiscoView 5.4

CiscoView is a graphical device management tool based on the Simple Network Management Protocol (SNMP) that provides real-time views of networked Cisco devices. Cisco MGC Node Manager uses CiscoView to configure and monitor the Cisco SLT and the LAN switch (Cisco Catalyst 2900, 5500, and 6509) devices through a CiscoView server.

CiscoView is optional; install it only if you want to manage the Cisco SLT or LAN switches from Cisco MGC Node Manager.

You install CiscoView *before* installing Cisco MGC Node Manager 2.6(1) so that you can identify the CiscoView server IP address that must be entered when you install Cisco MGC Node Manager. CiscoView may be installed locally on the Cisco MGC Node Manager workstation, or on a remote server.

Step 1 Install CiscoView 5.4 from the Cisco MGC Node Manager fourth CD. For CiscoView installation details, refer to the *CiscoView 5.4 Installation and Setup Guide* at http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_installation_guide_book09186a00800e19f6.html.

Step 2 Write down the CiscoView server IP address, which will be needed in Task 9 when you install Cisco MGC Node Manager.



Note CiscoView must use the default port number, 1741. Do not modify this port number during installation.



Note If you are using CiscoView, also make sure to install the CiscoView security module, after installing Cisco MGC Node Manager. See the “[Task 10. Install the CiscoView Security Module](#)” section on page 2-14.

About Client Workstation Software

Client workstations must have Java 1.3 and Netscape 4.76 installed to use CiscoView as a client. (Other browsers may work but have not been verified.) Netscape 4.76 is installed with Cisco EMF. The correct version of Java 1.3 is packaged with CiscoView. When you launch the CiscoView server the first time, you will be prompted to download and install the Java 1.3.1 version bundled with the plugin-131-sparc.tar CiscoView server. Follow the instructions displayed to download and install this plugin.

To use the CiscoView server, we also recommend that you install the latest J2EE Solaris patch cluster which can be found at the following URL:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

Task 8: Install Cisco EMF 3.2

For basic installation, follow the procedure described in Chapter 2 of the *Cisco EMF Installation and Configuration Guide* at:

http://www.cisco.com/en/US/products/sw/netmgsw/ps829/products_installation_and_configuration_guide_chapter09186a00801a8e14.html

For a management server, choose **Server Installation**. For a presentation server (a client), choose **Remote Client Installation**. You do not need a license on a client machine.

After installing the base 3.2 version, go on to “[Installing Cisco EMF Patches](#)” section on page 2-7. If you are using SSH for secure communications with SSH-enabled network components, continue with Installing SSH. Finally, start the Cisco EMF Server, as described in “[Starting Cisco EMF](#)” section on page 2-8.

Installing Cisco EMF Patches

Cisco MGC Node Manager requires Cisco EMF Service Pack 7 and 7.1. Refer to the Release Notes to check on any additional patches required.

To install Service Pack 7 and 7.1, follow these steps:

-
- Step 1** Determine your current Cisco EMF version and patch level:
cemf install -show
 - Step 2** Go to the following URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cemf-sp32-sp1>
 - Step 3** Download CEMF 3.2 Service Pack 7 software, CEMF3.2P7.tar.Z, to a directory on your hard drive.
 - Step 4** Download and read the CEMF 3.2 Service Pack 7 Release Note, CEMF3.2P7DepRelNote.pdf.
 - Step 5** Download CEMF 3.2 Service Pack 7.1 software, CEMF3.2P71.tar.Z, to a directory on your hard drive.

- Step 6** Download and read the CEMF 3.2 Service Pack 7.1 Release Note, CEMF3.2P71DepRelNote.pdf.
- Step 7** Follow the patch installation instructions in the Release Note and in the *Cisco EMF Installation and Configuration Guide* at the following location:
- http://www.cisco.com/en/US/products/sw/netmgtsw/ps829/products_installation_and_configuration_guide_book09186a00801a8e04.html
-

Installing the Cisco EMF SSH Add-On Package

To enable SSH support on Cisco MGC Node Manager, you install the CEMF strong cryptographic add-on package.



Note

We recommend installing SSH on Cisco MGC Node Manager and Cisco VSPT before installing it on the Cisco PGW, so that you can use the element managers to monitor the installation process on the PGW and other managed components.

- Step 1** Download the CEMF Crypto Add-on Package Software and the CEMF Crypto Add-on Package Installation Guide available from the network management download page <http://www.cisco.com/kobayashi/sw-center/sw-netgmt.shtml> under Cisco Element Management Systems - CEMF Strong Cryptographic Software. You must have authorization to download cryptographic software; if you do not, you are automatically redirected to an authorization request page.
- Step 2** Follow the installation instructions in the CEMF Crypto Add-on Package Installation Guide.



Note

Make sure the entry of SSH exists in the `/etc/services` (on the machine where the MNM is installed).



Caution

Using # character in the `/etc/motd` banner may cause problems in the SSH connectivity as these #’s interfere in the expect scripts used in the MNM. In case you face problem using SSH with CEMF Crypto Add-on package installed and the SSH entry in the `/etc/services` file, please try removing your motd banner.

Starting Cisco EMF

Start Cisco EMF as described in the following procedure:

- Step 1** Log in to the system where you installed Cisco EMF, and enter `su - root` to become the root user.
- Step 2** Change the working directory to CEMF bin by entering:
- ```
cd <CEMF_ROOT>/bin
```
- Where `<CEMF_ROOT>` is the directory where Cisco EMF is installed.
- Step 3** If the Cisco EMF background processes are not already running, enter:
- ```
./celf start
```



Note Depending on your server, it may take 10-30 minutes for the Cisco EMF startup processes to complete, with relatively longer startup if your database is new or has been reset.

Task 9: Install Cisco MGC Node Manager 2.6(1) and Verify the Installation

Follow these instructions to install Cisco MGC Node Manager. If you are upgrading from Version 1.5 or 2.x, see the “[Upgrading from Previous Cisco MGC Node Manager Versions](#)” section on page 2-16.

Identify any necessary patches by checking the location given in the “[Installation Software](#)” section on page 2-1.



Note You must install the Cisco MGC Node Manager software as **root**.

Follow the procedure below to install Cisco MGC Node Manager on a standalone system or on both machines (Management server and Presentation server) in a distributed configuration. The Cisco MGC Node Manager installation process automatically detects if the Cisco EMF complete software is installed, or only the Cisco EMF Client, and then installs the correct Cisco MGC Node Manager component.



Note If you are installing another element manager to run co-resident with Cisco MGC Node Manager, this is also the point in the installation sequence at which it should be installed. See the Release Notes for Co-Residence (of Cisco MGC Node Manager and another EMS) at http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/prod_release_notes_list.html.

Installing Cisco MGC Node Manager

- Step 1** Make sure that Cisco EMF is running.
- Step 2** Type `cd <CEMF_ROOT>/bin`, and enter the following command to verify that Cisco EMF is running:
- ```
>./cemf query
```
- Cisco EMF should display the following message:
- ```
CEMF Manager 3.2 initialized
```
- Step 3** If you are not already logged in as root, change the user to root user by entering `su - root`.
- Step 4** Verify that the Volume Management daemon is running:
- Enter the command `ps -ef | grep vold`. If the daemon is running, you see the following output:
- ```
root 363 1 0 May 23 ? 0:01 /usr/sbin/vold
```
- If the daemon is running, go on to Step 5. If the daemon is not running, start the daemon using the following command:
- ```
/etc/init.d/volmgt start
```
- Verify that the Volume Management daemon is running with the command provided above. If it is still not running, contact your system administrator.

Step 5 Place the Cisco MGC Node Manager installation media into the CD-ROM drive.

Step 6 Enter `cd /cdrom/cscocmnm`.

Step 7 Enter `./cmninstall`

The Install Package opens and displays the following options:

- ```
1) CMNM V.2.5.2 Package
q) Quit
```

Existing installations of any of the installation software are detected and are listed as “Already Installed”.




---

**Note** To upgrade to the next version of MGC Node Manager, enter `./cmninstall -u`

---

**Step 8** Enter `1` to install Cisco MGC Node Manager 2.6(1).

The installation process begins. During installation, you are asked for various kinds of input, summarized here:

- CiscoView Server IP address—Enter the IP address of the CiscoView server installed in Task 7. If you are not using CiscoView, just press **Enter**.
- Logfile directory location—Press **Enter** to accept the default location `/var/tmp` or type another location and press **Enter**.
- Logfile name—Press **Enter** to accept the default name `CSCOcmnm.log`, or type another name and press **Enter**.

After checking that disk space is sufficient, the Install Package asks if you want to continue with the installation.

**Step 9** Enter `y` to proceed with installation. The process typically takes from 15-40 minutes depending on your system.

When installation is complete, this message appears:

```
Everything appears to be installed correctly.
```

Go on to verify the installation.




---

**Note** If installation is not successful, check the installation log which by default is `/var/tmp/installCSCOcmnm.log`.

---

## Verifying the Installation

Verify that Cisco MGC Node Manager and CiscoView are installed properly before starting Cisco MGC Node Manager.

## Verifying Element Managers

---

**Step 1** Verify that the Cisco MGC Node Manager Package is installed using the following command:

**pkginfo CSCOcmmn**

The following message should appear:

```
application CSCOcmmn Cisco MGC-Node Manager(cmmn)2.6
```

- Step 2** Verify that the Cisco MGC Node Manager Element Managers have been installed. Run the following script to display the installed Cisco MGC Node Manager Element Managers and compare this with the list in the table below.

```
Cisco EMF Basedir/bin/cmmnversion -verbose
```

```
CSCOcmmn Tool Versions
```

```

 Patch Build Build
 Name Version Level Num Type

CSCOcmmn 2.6.1(1) 00 110204 DEV
CSCOcmev 2.6.1
CSCOcmlp 2.6.1 00
CSCOcelfm 3.2 Patch: 170007-06
 Patch: 190701-05

```

```
CSCOcmmn Element Manager Versions
```

```

 Patch Build Build
 Name Version Level Num Type

hostEMm 2.6.1 00 110204 DEV
mgcEMm 2.6.1 00 110204 DEV

```

**Note**

Specific information displayed from running this script varies according to the cmmn release and patch you are using.

**Table 2-4 Element Managers**

|        |                                                                                  |
|--------|----------------------------------------------------------------------------------|
| mgcEM  | Common Element Manager for Cisco MGC node devices                                |
| hostEM | Element Manager for Cisco MGC host signaling, trunking, and dial plan components |

**Note**

If you suspect problems in installation, check the installation log file (which by default is `/var/tmp/installCSCOcmmn.log`) to determine specifics.

## Verifying the Installation of CiscoView 5.4

Verify the installation of CiscoView 5.4 by entering the following command:

```
./cmmnupdateCVip -s
```

- If the package is installed, you see the following:

```
Current Ciscoview IP Address: 10.10.10.10
```

where 10.10.10.10 is the server IP address.

- If the package is not installed, you see the following:

```
ERROR: information for "CSCOcmcv" was not found
```

CiscoView is designed to work with CiscoWorks 2000. When installing CiscoView packages outside this environment, certain functions are not supported. The following CiscoView buttons do not work in the Cisco MGC Node Manager environment:

- Telnet
- CCO connection
- Preferences
- About
- Help


**Note**

When running xdsu, the following exception is generated and can be ignored:

```
ERROR: exception occurred while examining Integration Utility configuration:
com.cisco.nm.nmim.nmic.IntgUtilCheckConfig
```

### Changing the IP Address of the CiscoView Server If Needed

When you install Cisco MGC Node Manager, you fill in the IP address of the CiscoView server. If you need to change the IP address of the CiscoView server after Cisco MGC Node Manager is installed, enter the following command from the Cisco EMF base directory:

```
/cmmupdateCVip -i <new CiscoView IP address>
```

Information similar to the following is displayed:

```
cmm CiscoView Server IP Addresses changed
From: <old IP address>
To : <new IP address>
```

### Starting Cisco MGC Node Manager

- 
- Step 1** Have Cisco EMF running.
  - Step 2** Log in with your user ID.
  - Step 3** Change directory to the Cisco EMF directory. For example:  
**cd /opt/cemf/bin**


**Note**

An X-server must be running, and the DISPLAY environment variable must be properly configured. Use one of the following commands, depending on which shell you are using, to set the x-display variable.

In “csh” or “tcsh”: **setenv DISPLAY <hostname>:0**

In “sh” or “ksh”: **DISPLAY=<hostname>:0;export \$DISPLAY**

- 
- Step 4** Enter:  
**./cemf session**

**Step 5** When prompted, enter your login name and password:



**Note**

The default Cisco MGC Node Manager login and password are **admin**. Use the login and password configured for your system.

Refer to the Cisco MGC Node Manager User's Guide at <http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/>; Chapter 3, "Getting Started with Cisco MGC Node Manager" for help on navigation and basic operations.

If you are using SSH for secure communications with SSH-enabled network devices, go on to the next section, [Getting Started with Secure Communications on Cisco MGC Node Manager, page 2-13](#).

## Getting Started with Secure Communications on Cisco MGC Node Manager

This section describes how to enable secure communications on network devices managed with Cisco MGC Node Manager.

**Before you begin:** You must have installed the Cisco EMF strong cryptographic add-on package in Task 8 and you must know the security policy for the elements you are enabling. (Secure communications are enabled on the network elements directly, not using Cisco MGC Node Manager. See the component SSH installation documentation, such as

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mgcfm/> for the Cisco PGW 2200 Release 9.6(1).) You do not need to know the specific SSH version; Cisco MGC Node Manager automatically negotiates the correct SSH version, SSH 2 if available or SSH 1.x..

Do you have existing (already deployed in Cisco MGC Node Manager) network elements that are now SSH-enabled? See "[To Update Existing SSH-Enabled Network Elements](#)" section on page 2-13.

Do you want to deploy new network elements that are SSH-enabled? See "[To Deploy New SSH-Enabled Elements](#)" section on page 2-13.

### To Update Existing SSH-Enabled Network Elements

Use this procedure to set SSH as the security policy for network elements that are already deployed and have SSH enabled.

- 
- Step 1** In the Map Viewer, select the SSH-enabled element you want to update.
  - Step 2** Right-click and choose **Tools > Accounts**. The Accounts dialog box appears.
  - Step 3** For Security Policy, select **SSH**. (**None** is the default.)
  - Step 4** Click **Save**.
  - Step 5** Repeat the above steps for the remaining SSH-enabled elements.
- 

### To Deploy New SSH-Enabled Elements

Use this procedure to deploy new elements that have been SSH-enabled.

- 
- Step 1** In the Deployment Wizard template, for Security Policy select **SSH**. Enter other information as usual.

**Step 2** Click **Finish**.

Cisco MGC Node Manager discovers the element using the appropriate SSH protocol. Non-SNMP communication with the element will now use SSH secure utilities.

**To Identify SSH-Enabled Elements**

You can identify whether an element uses SSH by checking the Security Policy in its Accounts dialog box.

**Task 10. Install the CiscoView Security Module**

If you are using CiscoView, the CiscoView Security Module must be installed on the CiscoView server after CiscoView and Cisco MGC Node Manager have been installed.

**Step 1** Determine the IP address Cisco MGC Node Manager is using for the CiscoView server. For example, if Cisco EMF is installed in /opt/cemf, enter:

```
- /opt/cemf/bin/cmmupdateCVip -showip
```



**Note** An IP address of "0.0.0.0" is the local workstation.



**Note** If the address is not correct, see [“Changing the IP Address of the CiscoView Server If Needed” section on page 2-12](#) for how to change it.

**Step 2** Locate the CSCOCvsec.pkg that is shipped with the Cisco MGC Node Manager software and resides in the ciscoviewsecurity directory:

```
- cd ciscoviewsecurity
```

If the CiscoView server is not installed on Cisco EMF server, go on to Step 3. If the CiscoView server is installed on the Cisco EMF server, skip to Step 4.

**Step 3** Use ftp to copy the CSCOCvsec package to the CiscoView server using the CiscoView server IP address you determined with the cmmupdateCVip command.

```
- ftp cvserverIPAddress
```

```
cd /tmp
```

```
binary
```

```
put CSCOCvsec.pkg /tmp/CSCOCvsec.pkg
```

Telnet (or SSH) to the CiscoView server:

```
- telnet cvserver
```

You are now ready to install the package.

**Step 4** Change user to “root” user, (if not already “root”):

```
- su - root
```

**Step 5** Install the package:

```
- /usr/sbin/pkgadd -d /tmp/CSCOcvsec.pkg
```

**Note**

If you uninstall and reinstall Cisco MGC Node Manager, you must reinstall the security package.

## Task 11: Set Up the X Terminal Workstations for Remote Access

You can access Cisco MGC Node Manager remotely from a workstation or PC. Cisco MGC Node Manager has been tested with the Reflection 7.20 X server software package.

### Creating an XDMCP Connection

For Reflection software to display Cisco MGC Node Manager correctly, Reflection software must be run in XDMCP mode. For host name, use the name of the Presentation server (in a distributed configuration) or of the standalone system.

- 
- Step 1** Start Reflection.
- Step 2** From the Connection menu, select **New XDMCP Connection**.
- Step 3** From the Method pull-down menu, select **Broadcast** or **Direct**, and continue with one of the following set of steps:
- For Broadcast method:
- Click **Connect**.
  - Select the appropriate XDMCP computer. If you do not know which computer to select, contact your system administrator.
- For Direct method:
- In the Host Name field, enter the host name of an XDMCP computer.
  - Click **Connect**.

An X terminal window opens on the host machine. Start Cisco MGC Node Manager in the usual manner, as described in the [“Starting Cisco MGC Node Manager”](#) section on page 2-12.

**Note**

If the Cisco EMF Launchpad displays but appears to be inactive, check for a message box behind the Launchpad reporting that there are insufficient colors available for Cisco EMF Manager. You can safely ignore the message (and close the message box), or remedy the problem as described in the next section.

### Creating a Workstation Connection

Use the following procedure to connect to Cisco MGC Node Manager from a remote UNIX workstation:

- 
- Step 1** Open an X-terminal window.
- Step 2** Use Telnet to connect to the Cisco MGC Node Manager host.

**Step 3** Enter the following command to change to the Cisco MGC Node Manager directory:

```
#cd /opt/cemf/bin
```

**Step 4** Enter the following command to launch Cisco MGC Node Manager:

```
#!/cemf session
```

---

## Fixing the Insufficient Colors Problem

To fix the “... insufficient colors available for Cisco EMF Manager” problem, refer to the procedure in “Configuring Reflection X Version 7.20 to Support Cisco EMF Color Usage” in the *Cisco EMF Installation and Configuration Guide* at:

[http://www.cisco.com/en/US/products/sw/netmgtsw/ps829/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps829/products_installation_and_configuration_guides_list.html)

## Task 12. Synchronize Time

After installing Cisco MGC Node Manager, you should synchronize the time configured for the Cisco MGC, Cisco MGC Node Manager, and the Billing and Measurement Server (BAMS). To ensure that Cisco MGC Node Manager records are correct, these components should all be configured to Greenwich Mean Time (GMT). Refer to the *Cisco Media Gateway Controller Software Release 9 Software Installation Guide* and the *Billing and Measurement Server User's Guide* for your BAMS server for information about setting the time for these components.

## Task 13: Configure Network Devices to Forward Alarms

A final task in readying Cisco MGC Node Manager for network management is to configure the devices in the network so that they send alarm information to Cisco MGC Node Manager. For details, refer to Chapter 3 in the *Cisco MGC Node Manager User's Guide* at

[http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products_user_guide_list.html).



### Note

Migration from Cisco MGC Node Manager Release 1.5 to Cisco MGC Node Manager Release 2.6(1) is not supported. Performance and alarm data cannot be migrated to Cisco MGC Node Manager Release 2.6(1). The only recommended alternative is to create a seed file, which can be used for manual discovery.

---

# Upgrading from Previous Cisco MGC Node Manager Versions

If you are upgrading from a previous version of Cisco MGC Node Manager, the installation upgrade option installs Cisco MGC Node Manager Version 2.6(1) and leaves your data intact (for example, network data and user access settings). You do not need to uninstall your previous version before upgrading.



### Note

Cisco MGC Node Manager 1.5 uses Cisco EMF 3.1. Cisco MGC Node Manager 2.6(1) and previous 2.x versions use Cisco EMF 3.2.

---

Although the upgrade option preserves your data, we recommend that you perform a backup before upgrading, as described in the “Uninstalling the Cisco MGC Node Manager Software” section on page 2-18.

Perform the following steps to upgrade from a previous Cisco MGC Node Manager version:

- 
- Step 1** Check the “Installation Checklist” section on page 1-5 to identify any other tasks needed for the upgrade.
- Step 2** Have Cisco EMF and Cisco MGC Node Manager running. Change to the <cemf\_root>/bin directory and enter **./cemf query** to check the current version.
- Step 3** If you are not already logged in as root, change user to root user by enter the following command  
**su - root**
- Step 4** Verify that the Volume Management daemon is running:  
Enter the command **ps -ef | grep vold**. If the daemon is running, you see the following output:  
**root 363 1 0 May 23 ? 0:01 /usr/sbin/vold**  
If the daemon is running, go on to Step 5. If the daemon is not running, start the daemon using the following command:  
**/etc/init.d/volmgt start**  
Verify that the Volume Management daemon is running with the command provided above. If it is still not running, contact your system administrator.
- Step 5** Place the Cisco MGC Node Manager installation CD into the CD-ROM drive and enter **cd /cdrom/cscocmmn**.
- Step 6** Back up your database (see the “Uninstalling the Cisco MGC Node Manager Software” section on page 2-18).
- Step 7** Start Cisco MGC Node Manager and in the Map Viewer remove the MGX objects in the MGX-8260-View (refer to the Cisco MGC Node Manager User’s Guide, Chapter 5, “Modifying or Deleting Deployed Objects” at [http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products_user_guide_list.html)).
- Step 8** Close Cisco MGC Node Manager.
- Step 9** Install CEMF 3.2 Patch 6 and any later patches specified in the Release Notes.
- Step 10** Enter either of the following commands:  
**cmnminstall -u**  
Or  
**cmnminstall -upgrade**  
The installation begins. During installation, you are asked for various kinds of input, summarized here:
- Logfile directory location—Press **Enter** to accept the default location /var/tmp or type another location and press **Enter**.
  - Logfile name—Press **Enter** to accept the default name CSCOcmmn.log, or type another name and press **Enter**.
- Step 11** When the installation is complete, verify it according to the instructions in the “Verifying the Installation” section on page 2-10.
- Step 12** After the upgrade completes, start Cisco MGC Node Manager and do the rediscover the following objects:
- All BAMS objects, using the Map Viewer BAMS-View

- All HSI objects, using the Map Viewer HSI-View

**Note**

During the upgrade process, you may see error messages caused by Cisco EMF trying to create controllers that already exist. These messages may safely be ignored.

## Backing Up Your Databases

If you are upgrading from Cisco MGC Node Manager 1.5, you must back up your databases. If you are upgrading from Cisco MGC Node Manager 2.x, the upgrade process retains your databases, but it is nonetheless good practice to back up your databases before upgrading. For more details, see the *Cisco EMF Installation and Configuration Guide*.

# Uninstalling the Cisco MGC Node Manager Software

Cisco EMF must be running to uninstall Cisco MGC Node Manager. Use the following procedure to uninstall the Cisco MGC Node Manager software:

- 
- Step 1** If Cisco MGC Node Manager is open, close it. Do not stop Cisco EMF.
- Step 2** Enter either of the following commands:
- ```
cmnminstall -r
```
- Or
- ```
cmnminstall -remove
```
- Information similar to the following will be displayed:
- ```
-----
                Cisco MNM Uninstallation
                Wed Dec 15 09:56:16 AM
-----
```
- Step 3** When prompted, verify that you want to uninstall Cisco MGC Node Manager. The following message is displayed:
- ```
Have your databases been backed up [y/n]: [n] y
```
- Step 4** Enter **y**. You cannot uninstall Cisco MGC Node Manager unless you answer **y**.
- Step 5** When prompted, enter the log file directory location and the logfile name. The following message is displayed:
- ```
Continue with CSCOcmmn uninstall [y,n,?] y
```
- Step 6** Enter **y**, and Cisco MGC Node Manager is uninstalled.
-

Verifying Uninstallation of Cisco MGC Node Manager

After uninstalling Cisco MGC Node Manager, you should verify the uninstallation. Use the following procedure to verify that the Cisco MGC Node Manager package is not installed:

Step 1 Enter `pkginfo CSCOCmnm`.

The following message should appear:

```
ERROR: information for "CSCOCmnm" was not found
```

Step 2 Enter `pkginfo | grep EM` to verify that no Cisco MGC Node Manager Element Managers are installed.

The following message should appear:

```
ERROR: information for "CSCOCmncv" was not found
```

```
Cisco MGC Node Manager is uninstalled.
```

Displaying Current CMNM Packages

For displaying the current CMNM Packages, do the following:

Step 1 Login as "root":

Step 2 Enter either `cmnminstall -s` or `cmnminstall -show`.

This command displays all the current CMNM Packages.

Viewing Help for CMNM Install Scripts

For viewing the help content for the current CMNM Packages, do the following:

Step 1 Login as "root":

Step 2 Enter either `cmnminstall -h` or `cmnminstall -help`.

This command displays all the current CMNM Packages.

Uninstalling Cisco EMF

You must uninstall Cisco MGC Node Manager before uninstalling Cisco EMF. When Cisco EMF is deinstalled, all Cisco EMF processes are automatically stopped. If ObjectStore was installed as part of the Cisco EMF installation, it is removed during uninstallation. If ObjectStore was installed as a separate package before the Cisco EMF installation, ObjectStore still remains installed after Cisco EMF is deinstalled.

Use the following procedure to uninstall Cisco EMF:

-
- Step 1** As a superuser (**su**), log in to the machine where Cisco EMF is installed.
- Step 2** Ensure that Cisco MGC Node Manager has been deinstalled.
- Step 3** At the command line prompt, enter the following command to change to the Cisco EMF bin directory:
cd /opt/<CEMF_ROOT>/bin
- Step 4** At the command line prompt, enter:
./cemfinstall -remove
- Step 5** Choose an option from the menu.
- For more details, see the *Cisco Element Management Framework Installation and Configuration Guide* at http://www.cisco.com/en/US/products/sw/netmgtsw/ps829/products_installation_and_configuration_guides_list.html.
-

Troubleshooting Common Installation Problems

Carefully following the “[Installation Checklist](#)” section on page 1-5, will avoid most installation pitfalls. If a problem does occur, check this section for troubleshooting guidelines.

Related Topics

Cisco MGC Node Manager User’s Guide, Appendix C, “Troubleshooting Cisco MGC Node Manager”.
“[Problems Installing an Element Manager on Cisco EMF](#)” in the *Cisco Element Management Framework Installation and Configuration Guide*.

Troubleshooting Installation Problems

Problem	Suggested Steps
You get the message, “Cannot connect to session” when you try to start a Cisco MGC Node Manager session.	<p>Make sure that Cisco EMF is running.</p> <ul style="list-style-type: none"> • If Cisco EMF is not running, start it; then retry starting Cisco MGC Node Manager. • If Cisco EMF is running, check to see if the IP address or host name of the Cisco MGC Node Manager server has changed since Cisco MGC Node Manager was installed. If so, follow the steps described for the next problem.
You get the message, “System IP address does not match databased address” when you try to start Cisco EMF.	<p>This may be caused by a change in the IP address or host name of the Cisco MGC Node Manager server after Cisco MGC Node Manager was installed. To correct the problem:</p> <ol style="list-style-type: none"> 1. Stop Cisco EMF: <code>/opt/cemf/bin/cemf stop</code> 2. If needed, update the IP address in Cisco EMF: <code>/opt/cemf/bin/cemf updateIP -m</code> You are prompted for the new IP address. Enter the new IP address. 3. If needed, update the host name in Cisco EMF: <code>/opt/cemf/bin/cemf updateName -m</code> You are prompted for the new host name. Enter the new name. 4. Restart Cisco EMF. <code>/opt/cemf/bin/cemf start</code> <p>Note If the Management server address or name has changed in a distributed configuration, make the necessary changes on both the Management server and the Presentation server. If the Presentation server address or name has changed, make the changes on the Presentation server only.</p>
Password problems	Reset the password.

Problem	Suggested Steps
License challenges	Verify that: <ul style="list-style-type: none"> • The license file has a .lic extension • The license file is present in the /opt/CSCOcemf/license directory. • The license has not expired. If it has, get a new license at http://cco.cisco.com/kobayashi/sw-center/sw-registration.shtml. For instructions, see Task 4: Ensure That the Sun Solaris 8 Operating System Is Installed, page 2-5. • The license is a multi-user license. • The license file was not issued for a different machine. The license is machine-specific; you cannot move a license file from one machine to another but must get a new license for your current machine.
Uninstallation problem	Make sure you are uninstalling in the correct sequence. Before uninstalling Cisco EMF, you must uninstall Cisco MGC Node Manager. Before uninstalling Cisco MGC Node Manager, make sure that Cisco EMF is running.



C

- CEMF SSH add-in download [2-2](#)
- CEMF SSH add-on
 - installing [2-8](#)
- CEMF strong cryptographic download [2-2](#)
- changing
 - hostname of Cisco MNM server [2-21](#)
 - IP address of Cisco MNM server [2-21](#)
- checklist
 - for installation [1-5](#)
- Cisco EMF
 - license [2-5](#)
 - patches [2-7](#)
- Cisco MNM
 - problems starting [2-21](#)
- CiscoView [2-11](#)
- CiscoView security module [2-14](#)
- CiscoWorks 2000 [2-12](#)
- Client server
 - see Presentation server [1-3](#)
- Client software [1-2](#)
- configurations
 - of Cisco MNM [1-2](#)
- Cooked partitions [1-5](#)
- crypto for CEMF [2-2](#)

D

- database storage [1-4](#)
- deploy network elements for SSH [2-13](#)
- distributed Cisco MNM configuration [1-2](#)

G

- getting started
 - with SSH on Cisco MGC Node Manager [2-13](#)
- GMT [2-16](#)

H

- hard drive
 - partitioning [2-5](#)
- hardware
 - required [1-2](#)

I

- identifying
 - SSH-enabled elements in Cisco MGC Node Manager [2-14](#)
- information
 - required for installation [2-2](#)
- installation
 - overview [1-1](#)
 - troubleshooting [2-20](#)
- installing SSH on CEMF [2-8](#)
- IP address
 - of Cisco MNM server [2-21](#)
- IP information
 - setting up [2-6](#)

L

- Language
 - on Solaris [2-2](#)

LAN switch [2-6](#)

license

for Cisco EMF [2-5](#)

license challenges

troubleshooting [2-22](#)

Locale

on Solaris [2-2](#)

M

Management server [1-2](#)

multiple disk drives [1-4](#)

O

ObjectStore software [1-2](#)

operating system [2-2](#)

overview

of installation [1-1](#)

P

partitioning

hard drive [2-5](#)

patches

for Cisco EMF [2-7](#)

for network device software [2-4](#)

Planning and Installation Checklist [1-5](#)

Presentation server [1-2](#)

R

Raw partitions [2-5](#)

remote user access

setting up [2-6](#)

required hardware [1-2](#)

required information [2-2](#)

required software [2-1](#)

for network devices [2-3](#)

S

security enhancements

installing on CEMF [2-8](#)

security module, CiscoView [2-14](#)

Server software [1-2](#)

setting up

IP and remote user access information [2-6](#)

software

client [1-2](#)

required [2-1](#)

required on managed network devices [2-3](#)

server [1-2](#)

software requirements [2-5](#)

Solaris 2.6 [2-2](#)

Solaris Language [2-2](#)

Solaris Locale [2-2](#)

SSH [2-15](#)

installing on CEMF [2-8](#)

SSH download for CEMF [2-2](#)

SSH-enabled elements

identifying in Cisco MGC Node Manager [2-14](#)

SSH for CEMF

installing [2-8](#)

SSH on Cisco MGC Node Manager

getting started [2-13](#)

standalone Cisco MNM configuration [1-2](#)

starting Cisco MNM

problems with [2-21](#)

strong crypto for CEMF [2-2](#)

installing [2-8](#)

T

troubleshooting

installation [2-20](#)

U

update network elements for SSH [2-13](#)

X

XDMCP connection [2-15](#)

X terminal

software [2-2](#)

