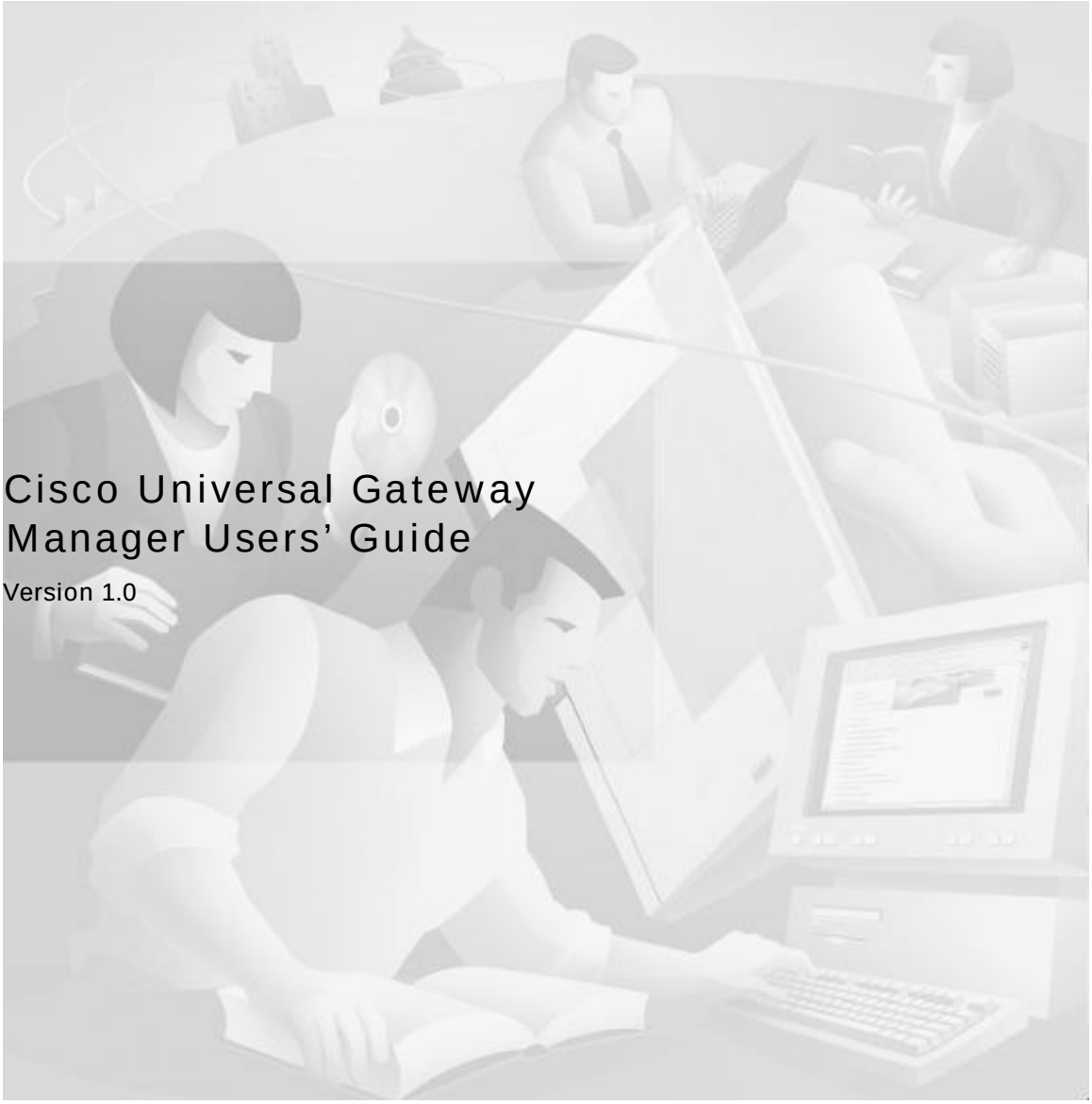


Cisco Universal Gateway Manager Users' Guide

Version 1.0

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

Customer Order Number: DOC-7812208=
Text Part Number: 78-12208-01

CONTENTS

Preface

Purpose

This document describes how to plan, install, and operate the Cisco Universal Gateway Manager (Cisco UGM) Version 1.0.

Audience

The primary audience for this guide consists of network administrators who use Cisco UGM to manage the access servers in system networks.

Scope

This document describes Cisco UGM in the context of the Cisco Element Management Framework (Cisco EMF).

Cisco UGM enhances some capabilities of Cisco EMF. Your product ships with Cisco UGM and Cisco EMF documentation, which are necessary to be proficient with Cisco UGM.

Related Documents

- *Cisco Universal Gateway Manager Quick Start Guide*
- Cisco Universal Gateway Manager Online Help
- Cisco Universal Gateway Manager Release Note
- Cisco Universal Gateway Manager Readme file (on the product CD)
- *Cisco Element Management Framework Installation and Licensing Guide*
- *Cisco Element Management Framework User Guide*

Where to Get the Latest Version of This Guide

The hard copy of this guide is updated at major releases only and does not always contain the latest enhancements occurring between major releases. Cisco provides separate release notes or configuration notes for spares, hardware, and software enhancements occurring between major releases. The online copy of this guide is always current and incorporates the latest enhancements to the product.

You can access the current online copy of this guide on the World Wide Web at:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com.

Conventions Used in This Guide

Convention	Description
bold	Command or keyword that you must enter.
italic	Argument for which you supply a value.
[x]	Optional keyword or argument that you enter.
{x | y | z}	Required keyword or argument that you must enter.
[x {y | z}]	Optional keyword or argument that you enter with a required keyword or argument.
string	Set of characters that you enter. Do not use quotation marks around the character string, or the string will include the quotation marks.
screen	Information that appears on the screen.
^ or Ctrl	Control key—for example, ^D means press the Control and the D keys simultaneously.
< >	Nonprinting characters, such as passwords.
!	Comment line at the beginning of a line of code.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss.

Note Means *reader take note*. Notes contain helpful suggestions or reference to materials not contained in this manual.

Tips Means the information *might help the reader solve a problem*.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

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

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships withyour 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 as an annualsubscription.

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
- 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 408526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to 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:

Attn Document Resource Connection
Cisco Systems, Inc.
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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

An Overview of Cisco Universal Gateway Manager

This chapter contains the following topics:

Overview of Cisco UGM

The Cisco Universal Gateway Manager (Cisco UGM) provides a means to configure and manage fault, performance, and security of the Cisco AS5350, AS5400, AS5800, and AS5850 devices in your network.

- Fault management

  Cisco UGM provides device- and port-specific alarm frequency and severity information. The fault management GUI supports point-and-click alarm acknowledgement and clearing functions, and also enables trap forwarding.

- Configuration of system components

  Cisco UGM provides various configuration services for the managed devices and their components. As objects are configured or modified, the database is automatically updated to reflect the current configuration of the network.

- Performance monitoring

  Cisco UGM collects performance information from each managed device and its components. This information allows you to monitor the network by viewing and graphing performance data associated with an object.

- Security management

  Cisco UGM supports role-based access to its management functions. You can define user groups and assign users to these groups. This function also supports control of administrative state variables for Cisco UGM resources.

Features of Cisco UGM

With Cisco UGM you can perform the following tasks:

- Use the Cisco EMF Map Viewer to graphically view and inventory your managed Cisco AS5350, AS5400, AS5800, and AS5850 devices, and the Ethernet, modem card, DS0, DS1, and DS3 interfaces on those devices.
- Graphically view and generate text reports on system performance.

  See Chapter8, "Managing the Performance of Cisco UGM Devices."

- Forward SNMP traps to multiple devices. Alarm events are generated from two sources: incoming SNMP traps from managed devices and internal alarms generated by Cisco UGM itself.

  See Chapter9, "Managing Faults with Cisco UGM."

- Assign selected user access to Cisco UGM.

  See Chapter7, "Managing Security on Cisco UGM."

- Automatically discover Cisco AS5350, AS5400, AS5800, and AS5850 devices and their ports.

  See Chapter3, "Deploying, Discovering, and Exporting Inventory Data with Cisco UGM."

- Perform single or bulk-mode IOS configuration of similar Cisco AS5350, AS5400, AS5800, and AS5850 devices.

  See Chapter 4, "Configuring Devices with Cisco UGM."

- Perform single or bulk-mode updates of IOS images and modem images to similar devices on the system.

  See Chapter 5, "Managing Images and Scheduling Actions with Cisco UGM."

- Commission or decommission device and card objects.

  A decommissioned object is not managed by Cisco UGM; no alarm events are raised against it, and no performance or presence polling is carried out.

  You can also "commission" or "decommission" devices to prevent them from displaying unnecessary alarm information during configuration and rebooting.

  See "Overview of the Commission/Decommission Function for a Chassis" section on page 9-19 and "Overview of the Commission/Decommission Function for a Card" section on page 9-20.

- Back up, store, and restore IOS configurations for managed devices in the system.

  See "Backing Up Your Database" section on page A-3 and "Restoring Your Database" section on page A-4.

System Architecture for Cisco UGM

The Cisco UGM product consists of two main components:

- Cisco Element Management Framework (EMF) software
- Cisco UGM software which manages these Cisco devices:
  - Cisco AS5350
  - Cisco AS5400
  - Cisco AS5800
  - Cisco AS5850

Each of these devices provides ports through which dial-in users can access the network.

Cisco EMF is a client-server environment supporting various deployment options. The best configuration for you depends on the number of servers, clients, and users in your network.

The Cisco EMF client is the device from which you can employ a remote X-terminal to access either another Cisco EMF client or the Cisco EMF server. You do not need a Cisco EMF client between your client and the Cisco EMF server, but doing so improves performance for large or medium deployments.

Figure1-1 Directly Accessing the Cisco EMF Server

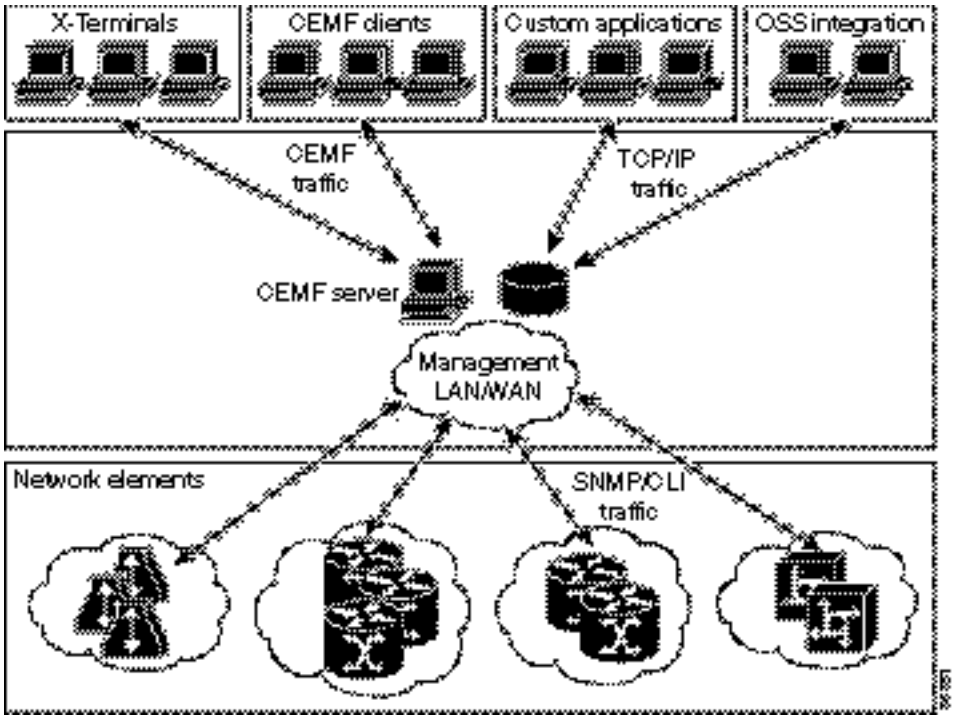
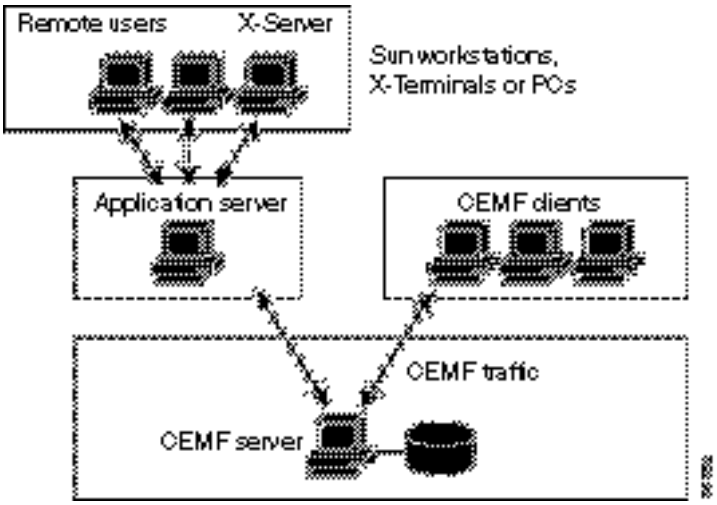


Figure1-2 Accessing the Cisco EMF Server Through a Client



Cisco EMF Server Requirements and Guidelines for Cisco UGM

Cisco UGM runs on the Cisco Element Management Framework (EMF) server or Cisco EMF client. The server requirements for the Cisco EMF server running Cisco UGM are:

- Sun Enterprise 450 with four 250-MHz processors and six 9-GB hard drives

  or
- Sun Ultra 60 with two 360-MHz processors and two 9-GB hard drives
- Solaris 2.6 OS
- 1 GB RAM
- 2 GB swap disk space
- CD–ROM drive
- (Optional) Console to use with the Cisco AS5800 device:
  - Cisco 2511 router (with IOS software image c2500-i-1.120-5.T or IOS software image c2500-i-1.112-18.T)
  - Cisco 2560 router (with IOS software image igs-in-1.111-5)
- 17-inch color monitor
- 24-bit graphics card
- Cisco Element Management Framework (EMF) 3.0 server and client components
- Cisco Universal Gateway Manager

For details on Cisco EMF 3.0 server requirements, refer to the *Cisco Element Management Framework Installation and Licensing Guide*.

Cisco EMF Client Server Requirements and Guidelines for Cisco UGM

Caution Although Cisco UGM supports simultaneous multiple user sessions, you must avoid simultaneously accessing and modifying the configuration of the same device or subcomponent. Doing so will corrupt the data for that stack.

The Cisco EMF client requirements to support Cisco UGM are:

- Sun Ultra 5 with Solaris 2.6 OS installed

  Or

  Sun Ultra 10 with Solaris 2.6 OS installed
- 360-MHz processor
- 256 MB of RAM
- 2 GB swap disk space
- 9 GB hard drive
- CD–ROM drive
- (Optional) Console to use with the Cisco AS5800 device:
  - Cisco 2511 router (with IOS software image c2500-i-1.120-5.T or IOS software image c2500-i-1.112-18.T)
  - Cisco 2560 router (with IOS software image igs-in-1.111-5)
- 17-inch color monitor
- 24-bit graphics card
- Cisco EMF 3.0 client component
- Cisco Universal Gateway Manager
- Ethernet connectivity to the Cisco EMF server running Cisco UGM

For details on Cisco EMF 3.0 client requirements, see the *Cisco Element Management Framework Installation and Licensing Guide.*

Cisco UGM Hardware Installation Considerations

- Provision at least one trunk card.
- T1 and E1 trunk cards cannot coexist in the same device.
- Cisco AS5350 device:
  - Install cards in slots 1 through 3.
  - Slot 0 is reserved.
  - You cannot install more than two T1 or E1 cards in the device.
- Cisco AS5400 device:
  - Install cards in slots 1 through 7.
  - Slot 0 is reserved.
  - You cannot install CT3 and 8PRI cards in the device.
- Cisco AS5800 device:
  - Install trunk cards only in slots 0 through 5.
  - Install modem and 3NP108 cards in slots 0 through 11.
  - Slots 12 and 13 are reserved.
  - You cannot install CT3 and 12PRI cards in the same device.
- Cisco AS5850 device:
  - Install cards in slots 0 through 5 and 8 through 13.
  - Slots 6 and 7 are reserved.
  - You cannot install CT3 and 12PRI cards in the same device.

Installing and Deinstalling the Software

This chapter describes how to install the required network components for the Cisco Universal Gateway Manager (Cisco UGM), and contains the following topics:

Overview of Installing Cisco UGM

To install Cisco UGM, you must first install Cisco EMF which is a separate software package with its own installation procedure. To install Cisco EMF and Cisco UGM, follow these steps:

1. Make sure that you satisfy the requirements described in the "Cisco EMF Server Requirements and Guidelines for Cisco UGM" section on page1-6, and the "Cisco EMF Client Server Requirements and Guidelines for Cisco UGM" section on page1-7.
2. Obtain a Cisco EMF license.
   See the "Obtaining a Cisco EMF License" section on page2-3, and also refer to the *Cisco Element Management Framework Installation and Licensing Guide.*
3. Plan the hard drive partitions and swap space.
   See the "Obtaining a Cisco EMF License" section on page2-3, and "Setting Up Cooked Partitions for Cisco EMF (Default)" section on page2-5.
4. Find out the host name and host ID.
5. Install the Sun Microsystems Solaris 2.6 Operating System and patches.
6. If you are planning to operate Cisco UGM with CiscoView:
   a. Install the Netscape browser on your system.
   b. Install CiscoView, Release 5.0. or 5.1. (This is the release supported by Cisco UGM).
7. Install the Cisco EMF software.
   See the "Overview of Installing Cisco EMF" section on page2-7, and also refer to the *Cisco Element Management Framework Installation and Licensing Guide.*
8. Install Cisco EMF patches (if necessary).
   See the Release Notes that shipped with your Cisco UGM software.

9. Install the Cisco UGM software.
   See the "Overview of Installing Cisco UGM" section on page2-12.
10. Install Cisco UGM patches (if necessary).
    See the Release Notes that shipped with your Cisco UGM software.

Obtaining a Cisco EMF License

You need a valid license key available on the system to start the Cisco EMF server. If you do not have a license key, you can install the software, but you cannot start CiscoEMF.

To update the Cisco EMF license currently in use, for example if you wish to extend an evaluation license or convert an evaluation system to a proper installation with a permanent license, refer to the *Cisco Element Management Framework Installation and Licensing Guide.*

Step 1 If you are a registered Cisco.com user, go to the Cisco Software Registration site at: http://cco.cisco.com/kobayashi/sw-center/sw-registration.shtml

Or

If you are not a registered Cisco.com user, go to the Cisco Software Registration site at:
http://cco.cisco.com/public/sw-center/sw-registration.shtml

Step 2 Click **Cisco Element Management Framework**.

Step 3 In the **Contact Information** section**,** fill all required fields (denoted by an asterisk).

Note Because the permanent license key is returned to you by e-mail as an attached file, you must provide your correct e-mail address.

Step 4 In the **Version** number field, select the version of the Cisco EMF product that you want a license for.

Step 5 If it was not automatically filled in for you when you filled in the Contact Information, enter the Product Authorization Key (PAK) number.

The PAK number is provided on the CiscoEMF product CD sleeve.

Step 6 Specify the hostname of the server where the CiscoEMF product is installed.

You can obtain the hostname of the server by entering **hostname** at the command line prompt.

Step 7 Specify the host ID (a hexadecimal string that identifies the system—not the IP address) of the server where the Cisco EMF product is installed.

You can obtain the host ID of the server by entering the **hostid** command.

Step 8 Enter the answers to the questions at the end of the form and click **Enter Form**.

Overview of Partitioning the Hard Disk

To partition the server hard drive that Cisco UGM is installed on, follow these guidelines:

Table2-1 Partitioning the Cisco UGM Server Hard Disk

Partition	Size
/	250 MB
<swap>	2 GB on server; 1 GB on client
/var	513 MB
/usr	2 GB
/opt	2 GB
/backup	
/scratch	Remainder of disk

To increase system performance, create the ObjectStore transaction log (default/opt/transact.log) and ObjectStore database (default/opt/cemf/db) on separate disks.

Viewing the Disk Space

Enter the following command:

```
host_name# df -k
```

The available disk space appears as blocks or KB.

Setting Up Cooked Partitions for Cisco EMF (Default)

By following this procedure, you can improve your system performance.

Note Do not install databases on the same drive as the Cisco EMF software.

Step 1 Move cache files to a separate drive (not partition).

Step 2 On a separate drive, add a partition and copy that partition to **/ostart_cache**.

Step 3 Create the file localhost.sh in the following directory:

<CEMF Directory>/config/env/**localhost.sh**

Step 4 Enter:

OS_CACHE_DIR=/ostore_cache ; export OS_CACHE_DIR

OS_COMMSEG_DIR=/ostore_cache ; export OS_COMMSEG_DIR

Step 5 Place the transaction log on a different drive from the installation, cache, and database files.

Setting Up Raw Partitions for Cisco EMF

By following this procedure, you can improve your system performance.

Note Do not install raw partitions on the same drive as the Cisco EMF software.

Step 1 Move the cache files to a separate drive (not partition).

Step 2 On a separate drive, add a partition and copy that partition to **/ostart_cache**.

Step 3 Create the file localhost.sh in the following directory:
<CEMF Directory>/config/env/**localhost.sh**

Step 4 Enter:

OS_CACHE_DIR=/ostore_cache ; export OS_CACHE_DIR

OS_COMMSEG_DIR=/ostore_cache ; export OS_COMMSEG_DIR

Step 5 Make sure that the transaction log is in the raw partition, and the server parameter file does not have an entry for the transaction log.

Note The server parameter file is located in <CEMF directory>/ODI/OS5.1/ostore/etc/*hostname*_server_parameter (where *hostname* is the workstation's hostname).

Overview of Installing Cisco EMF

You can enter the cemfinstall command with optional parameters to install and deinstall Cisco EMF.

Note You must log in as superuser (su) to use cemfinstall.

Table2-2 cemfinstall Command Parameters

Parameter	Description
	When you don't specify any parameters, the installation menu appears.
-choice <choice>	Select the <choice> menu option. For example, by entering cemfinstall -c 3, you select the third menu option.
-dir {<directory>]	Displays the location of the packages.
-echoonly	Does not run (only echoes) the commands.
-help	Displays Help.
-remove	Removes an existing installation.
-show	Shows all packages installed by cemfinstall.
-yestoall	Answer Yes to all cemfinstall script questions.

Installing the Cisco EMF Server Image

Step 1 Log in as superuser (**su**) to the workstation where you want to install Cisco EMF.

Step 2 Insert the CiscoEMF product CD into the CD-ROM drive.

Step 3 Change to the CD-ROM drive and enter:

```
host# cd /cdrom/cdrom0
```

Step 4 To start the CiscoEMF installation script, enter:

```
host# ./cemfinstall
```

Step 5 Select option **1** to install the server image.

The server processes and a local client are installed on a server workstation.

Step 6 Specify a directory for the installation files. The default location is /opt/cemf.

Step 7 If the default location is acceptable, press **Enter**.

Or

If the default is not acceptable:

a. Enter **n**.

b. Enter a directory path.

c. Press **Enter** to verify your choice or to repeat the sequence described in a. through c.

Step 8 Enter the directory to be used for backing up and restoring data. The default directory /opt/Backup appears.

Refer to the *Cisco Element Management Framework User's Guide* for details of the data backup and restore processes.

Step 9 If the server has more than one hostname, the hostname menu appears. Select the correct hostname and press **Enter**.

Or

If the correct hostname is not listed in the menu, enter the hostname and press **Enter**.

Step 10 If the Server Hostname and Server IP Address setup is correct, press **Enter**.

Or

To change these values, enter **n**.

Tips Change these values if your system has multiple network card interfaces.

Step 11 Configure the ObjectStore option for your installation.

Refer to the *Cisco Element Framework Management Installation, Configuration, and Licensing Guide* for details on ObjectStore.

Step 12 To accept the default DNS domain, enter **y**.

Or

To change the default:

a. Enter **n**.

b. Specify the relevant DNS domain and press **Enter**.

Step 13 To use the FlexLM daemon provided with Cisco EMF, enter **y**.

Step 14 If you have a valid license file available on your network, enter the full name and path of the license file.

Note To obtain a license, see the "Obtaining a Cisco EMF License" section on page2-3.

Step 15 To use an existing license, enter **n**.

Step 16 To verify the location of the license file, enter **y**.

Note If you do not have a valid license file you can still continue with the installation by entering n. The installation process continues; however you cannot start the Cisco EMF Server until a valid license key is provided. Enter the <*CEMF_ROOT*>/bin/cemf license command to update the license information.

Step 17 When the installation is complete, leave the /cdrom/cdrom0 directory and enter **eject**.

Step 18 Remove the CiscoEMF product CD from the CD-ROM drive.

Installing the Cisco EMF Client Image

Note If you have already installed the server image on your server, do not install the client image on the same server. (The CiscoEMF server image also contains the client image.)
See the "Installing the Cisco EMF Server Image" section on page2-7.

Follow this procedure to install Cisco EMF on additional client workstations. You can do this in order to relieve the server from some processes or to support additional system users.

See the "Cisco EMF Server Requirements and Guidelines for Cisco UGM" section on page1-6.

Step 1 Log in as superuser (**su**) to the workstation where you want to install Cisco EMF.

Step 2 Insert the CiscoEMF product CD into the CD-ROM drive.

Step 3 Change to the CD-ROM drive and enter:

```
host# cd /cdrom/cdrom0
```

Step 4 To start the CiscoEMF installation script, enter:

```
host# ./cemfinstall
```

Step 5 Select option 2 to install the client processes on a client workstation.

The default location for installing the Cisco EMF client is /opt/cemf.

Step 6 If the default installation location is acceptable, press **Enter**.

Or

If the default is not acceptable:

a. Enter **n.**

b. Enter a directory path.

c. Press **Enter** to verify your choice or to repeat the sequence described in a. through c.

Step 7 Enter and verify the hostname of the system where you want to install the Cisco EMF server image.

Step 8 If the Server Hostname and Server IP Address setup is correct, press **Enter**.

Or

To change these values, enter **n**.

Tips Change these values if your system has multiple network card interfaces.

Step 9 When the installation is complete, leave the /cdrom/cdrom0 directory and enter **eject**.

Step 10 Remove the CiscoEMF product CD from the CD-ROM drive.

Installing Cisco EMF Patches

You may have to install one or more patches for Cisco EMF. Refer to the Release Notes that shipped with Cisco UGM for the exact patch version and location from where you can download the patch.

Tips All Cisco EMF patches are also located on Cisco.com.

Step 1 Go to the following website:

http://www.cisco.com/cgi-bin/tablebuild.pl/cemf

Step 2 Download the appropriate CEMF patch to a directory on your hard drive.

Step 3 From the same directory, enter:

./ cemfinstall

Starting Cisco EMF

Step 1 Log in as the **root** user on the system where you want to install the Cisco UGM.

Step 2 Change to the CEMF bin directory by entering:

cd <CEMF_ROOT>/bin

where <CEMF_ROOT> is the directory where Cisco EMF is installed.

Note Run the install script from the directory where the script is located.

Step 3 If the Cisco EMF background process are not already running, enter

./cemf start

Wait 10 to 15 minutes for the Cisco EMF startup processes to complete.

Note Do not start the CiscoEMF GUI session (**./cemf session**) because the Cisco UGM installation will end any running Cisco EMF GUI-based sessions.

See the "Starting a Cisco EMF GUI Session from a Local Workstation" section on page2-17.

Overview of Installing Cisco UGM

After the Cisco EMF server or client image is installed on your systems, install the Cisco UGM on your server and client.

The Cisco EMF run level is lowered (placed offline) at the start of the Cisco UGM installation process and is reset at completion to its former level (placed online).

Caution If Cisco UGM is reinstalled (after the Cisco UGM initial installation), any existing data is lost. Back up any existing data before reinstalling Cisco UGM.
See the "Backing Up Your Database" section on pageA-3.

If Cisco EMF detects any traces of Cisco UGM from a previous installation, this installation ends. Enter the **./removeEMS** command to remove traces of the previous installation.

See the "Overview of Deinstalling Cisco UGM" section on page2-17.

If the installation script does not find the swap space disk partition, you are asked to enter the location of the swap space; if the swap space disk partition is less than 2 GB, the installation ends.

For help in setting up the swap space partition, see the "Overview of Installing Cisco UGM" section on page2-2.

Installing the Cisco UGM Software Image

Note If you are planning to operate Cisco UGM with CiscoView, make sure that the Netscape browser is installed on your system and that you are running CiscoView version 5.0 or 5.1.

Step 1 Check that you are running the correct version of Cisco EMF by entering:

*<CEMFROOT>***/bin/cemf install -show**

Cisco EMF version and patch information appear. Compare this with the release notes shipped with your Cisco UGM product.

Step 2 Start Cisco EMF by entering:

*<CEMFROOT>***/bin/cemf start**

Step 3 Insert the Cisco Universal Gateway Manager CD-ROM.

Step 4 Change to the CD-ROM drive.

Step 5 If you are installing Cisco UGM on the server, enter:

./installEMS

Or

If you are installing Cisco UGM on the client, enter:

./installEMS -c

The installation script checks to see that CiscoEMF version 3.0.4 is installed. If it detects an older version of Cisco EMF, the installation ends.

Step 6 Specify if you will use CiscoView with this Cisco UGM installation:

- If you answer **y** (yes), proceed with Step 7.
- If you answer **n** (no), go to the Note in Step 7.

Step 7 Enter the following information for CiscoView:

```
Enter path where netscape can be found: /opt/cemf/bin/netscape
Using netscape at /opt/cemf/bin/netscape
Use telnet found at /usr/bin/telnet? Press Enter to accept or enter
new location: <Enter>
Using telnet at /usr/bin/telnet
Select on which host CiscoView is installed by using
1) its HostName
2) its IP Address
Enter 1 or 2:2
Enter IP Address: 172.19.50.10
```

Note The HostName specified in this step must exist in the /etc/hosts file of the Unix system.

The Cisco UGM installation takes approximately one hour to complete. This installation time excludes that for the Cisco EMF, which is already installed.

Note If the installation fails, check the log file llinstall.log in the /tmp directory to identify the problem.

Sample Error Messages Generated during Cisco EMF and Cisco UGM Installation

Some environment-specific error messages may be generated when you enter the UNIX **pkgadd** command during the installation process. Even though these messages may not be fatal and may allow installation to continue, Cisco UGM may operate unpredictably. Contact Cisco's TAC (Technical Assistance Center) for assistance in troubleshooting these errors.

```
pkgadd: ERROR: cppath ( ) : unable to stat
</usr/local/src/asm/CEMF_3.0.4-RC2/packages/CSCOcemfm/reloc/config/
genericController/stateMachines/networkStateMachine>

ERROR: attribute verification of </usr/local/cemf/config/
genericController/stateMachines/networkStateMachine> failed
pathname does not exist

pkgadd: ERROR: source path
</usr/local/src/asm/CiscoUGM_1.0/ASMainEM/packages/ASMainEM/reloc/conf
ig/dialogs/ChannelStatistics.ASMainEM.dialog> is corrupt
pathname does not exist
```

Accessing Cisco UGM Remotely

You can access Cisco UGM functions from a workstation or PC remotely.

When you access Cisco UGM remotely, it takes longer to run certain functions than if you are connected to the server. This section contains system settings that can help you optimize Cisco UGM remote access and viewing.

Step 1 From your Windows desktop, choose **Start** > **Programs** > **Reflection** > **Reflection X**.

Step 2 From the toolbar in the X Client Manager window, select **Settings** > **Window Manager**.

- **a.** In the Window Mode field, select **Microsoft Windows Desktop**.
- **b.** In the Default Local Window Manager field, select **Microsoft Windows**.
- **c.** In the Options field, select **Allow Remote Window Manager**.
- **d.** Click **OK**.

Step 3 From the toolbar in the X Client Manager window, choose **Settings** > **Color**.

- **a.** In the Default Visual Type field, select **PseudoColor Emulation**.

b. In the Colormap Preallocation field, select **System Colors**.

c. In the Private field, select **None**.

d. Add the light green color (needed to view status codes) by clicking **Edit** at the bottom of the screen.

e. In the Red (R), Green (G), and Blue (B) fields, change the B and R values to 190 each; the G field remains at 248.

f. Click **Add** and enter **LightGreen** as the description for this new color.

g. Click **OK**.

h. To return to the Reflection X window, click **OK**.

Starting a Cisco EMF GUI Session Remotely

Step 1 From your Windows desktop, choose **Start** > **Programs** > **Reflection** > **Reflection X**.

Step 2 From the X Client Manager left pane, select a telnet mode:

- xdmcpdir.rxc (Direct)—Use this mode if the remote device is on a different subnet from the server.
- xdmcpbrd.rxc (Broadcast)—Use this mode if the remote device is on the same subnet as the server.

Step 3 In the hostname field, enter the server that you want to telnet to, and click **Connect**.

Step 4 Login as **root** (username) with a password provided by your system administrator.

Step 5 Enter the following command:

cd /opt/cemf/bin

Step 6 Start the Cisco EMF client by entering:

./cemf session

Step 7 Log in as an admin level user and enter the password:

admin

Note admin is the system default password. Use the username and password assigned by your system administrator.

The Cisco EMF Launchpad appears, and Cisco UGM starts automatically.

Starting a Cisco EMF GUI Session from a Local Workstation

Step 1 Start Cisco EMF by entering:

./cemf session

Step 2 Log in as an admin-level user and enter the password:

admin

Note admin is the system default password. Use the username and password assigned by your system administrator.

The Cisco EMF Launchpad appears, and Cisco UGM starts automatically.

Overview of Deinstalling Cisco UGM

Cisco UGM and Cisco EMF must both be running when you deinstall Cisco UGM.

If you have difficulty deinstalling the software, see the "Troubleshooting Deinstalling Cisco UGM" section on page2-20.

The Cisco EMF run level is lowered (placed offline) at the start of the Cisco UGM deinstallation process and is reset at completion to its former level (placed online).

Note The ./removeEMS script detects and removes the server image, the client image, or both.

Table2-3 Cisco UGM Deinstallation Command Options

Command Option	Description
-help or **-h**	Displays online Help.
-upgrade or **-u**	Performs an upgrade instead of a removal. To preserve Cisco UGM databases when the system is deinstalled, use this option.
-skipportcheck	Performs a forceful removal without checks. Since the controller does not participate in this forceful removal, Cisco UGM objects are still seen in the Map Viewer. Manually delete the objects to remove them from the Map Viewer and the database. Use this command only if the ./removeEMS command fails.
-noconfirm	Assumes a yes answer to all script prompts.

The Cisco UGM deinstall process takes approximately one hour to complete.

Deinstalling Cisco UGM

Note You must run the deinstall script from the directory where the script is located.

Step 1 Verify that you have exited all CiscoEMF sessions.

Step 2 Insert the Cisco Universal Gateway Manager CD-ROM.

Step 3 Change to the CD-ROM drive and enter:

./removeEMS

This script removes Cisco UGM Version 1.0. You can specify several options with this command.

Tips If the deinstallation fails, check the log file lluninstall.log in the /tmp directory to identify the problem.

See the "Overview of Deinstalling Cisco UGM" section on page2-17 for details.

Overview of Deinstalling Cisco EMF

When CiscoEMF is deinstalled, all Cisco EMF processes are automatically stopped.

If ObjectStore was installed as part of the Cisco EMF installation, it is removed during deinstallation. If ObjectStore was installed as a separate package before the Cisco EMF installation, ObjectStore still remains installed after Cisco EMF is deinstalled.

Note Ensure that you have backed up all databases as the deinstallation removes dynamically created files (for example, log files and databases).
See Chapter2, "Installing and Deinstalling the Software" in this document, and refer to the *Cisco Element Management Framework User Guide*.

Deinstalling Cisco EMF

Caution The order in which components are removed is important. You must deinstall the patches first—in reverse order—by starting with the latest patch. For example, if patches 3, 4 and 5 are installed, you must deinstall patch 5, then patch 4, then patch 3; then deinstall Cisco EMF itself.

Step 1 As a superuser (**su**), log in to the machine where Cisco EMF is installed.

Step 2 Ensure that Cisco UGM has been deinstalled.

Step 3 At the command line prompt, change to the CiscoEMF bin directory, and enter:

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 Licensing Guide*.

Troubleshooting Deinstalling Cisco UGM

You may have difficulty deinstalling Cisco UGM for these reasons:

- Your temporary license ended and you cannot start Cisco EMF.
- Cisco UGM stopped operating.

If either of these conditions exists, deinstall each individual element package.

The names of the server packages are:

- ASMainEMm
- IOSMgrm
- IOSFmgrm
- commonEMm

The names of the client packages are:

- ASMainEMc
- IOSMgrc
- IOSFmgrc
- commonEMc

Step 1 Remove the element package registration from Cisco EMF by entering:

<CEMF_ROOT>/**bin/cemf load -removelock -skipportcheck -remove** *<Pkg Name>*

Step 2 Remove the element package by entering:

/usr/sbin/pkgrm *<Pkg Name>*

Step 3 Remove Cisco EMF by entering:

<CEMF_ROOT>/**bin/cemfinstall -remove**

Deploying, Discovering, and Exporting Inventory Data with Cisco UGM

With Cisco UGM, you can query the network for managed devices. Each device is then queried for subcomponents. When you remove or insert cards that support Online Insertion/Removal (OIR), an OIR trap is sent from the device which then causes Cisco UGM to automatically rediscover device subcomponents.

This chapter contains the following sections:

Overview of Deploying Devices into the Network

In order to set up Cisco UGM to manage network devices, you must first deploy the devices into the network. An object for each device is created automatically when the device is deployed by Cisco UGM. This created object represents a real object in the network and is stored under the Network, Physical, and device-specific (AS5350, AS5400, AS5800, AS5850) views. You can access the device object through the Map Viewer.

Refer to the *Cisco Element Management Framework User Guide.*

In the Cisco EMF Map Viewer, you can deploy these objects:

- A region object (representing the region where the managed devices are located).
- A site object (representing the physical site of the managed devices).

Region and site objects can represent virtual, or actual, regions or sites on the network.

Deploying a Region Object

Step 1 Right-click the physical node and select **Deployment** > **Deploy generic objects**.

Step 2 In the Deployment Wizard dialog box, select the **Region** option and click **Next**.

Step 3 Enter responses to the Deployment Selector Screen and click **Next**.

Step 4 In the Object Details screen, specify a site name.

Step 5 In the Deployment Summary screen, click **Finish** and wait until the deployment process is completed.

For details on creating site objects, refer to the *Cisco Element Management Framework User Guide*.

Deploying a Site Object

Step 1 Right-click the physical node, or, if you created a region object and want your site object to be located under it, right-click that region and select **Deployment > Deploy generic objects**.

Step 2 In the Deployment Wizard dialog box, select the **Site** option and click **Next**.

Step 3 Enter responses to the Deployment Selector Screen and click **Next**.

Step 4 In the Object Details screen, specify a site name.

Step 5 In the Deployment Summary screen, click **Finish** and wait until the deployment process is completed.

For details on creating site objects, refer to the *Cisco Element Management Framework User Guide*.

Overview of Discovery

You can start this application by using one of these methods:

- Click the Discovery icon in the Cisco EMF Launchpad.
- Right-click a selected container object like Site or Region, and select the Deployment > Auto Discovery option from the menu.

Device objects are discovered first, followed by the subcomponent objects. When the subcomponent discovery is in progress, the device object is in the discovering state.

For details on icons, refer to the *Cisco Element Management Framework User Guide*.

The device and subcomponent objects are discovered and located in the region or site from where you initiate discovery.

Caution Do not attempt to discover all network objects in bulk mode. Discover objects by specifying a range of (approximately 30) IP addresses.

If objects are not discovered during the first discovery, the next discovery finds these undiscovered objects. The database retains information about previously discovered objects.

For example, if you specified the IP address range (of devices to be discovered) to be from 171.22.41.65 to 171.22.41.95, and Cisco UGM did not discover devices in the 171.22.41.83 to 88 range, you can initiate discovery to find these devices.

After the initial discovery of devices, discovery is triggered again when:

- A device object is in the errored state for more than a specified time interval, the default being 15 minutes.

  You can modify this time interval in the .ini file located at:

  <CEMFROOT>/config/ASMainCtrl/ASMainCtrlUser.ini

- Cisco UGM receives an Online Insertion and Deletion (OIR) trap (from a device that supports OIR).
- You start discovery by first decommissioning and then commissioning the device as described in the "Overview of the Commission/Decommission Function for a Chassis" section on page9-19.

If the underlying device subcomponents have changed, corresponding changes are made during rediscovery leading to deletion or creation of Cisco EMF objects (representing cards and ports).

For more details, refer to the *Cisco Element Management Framework User Guide.*

About SNMP Tables

Cisco UGM discovers device subcomponents by getting the following SNMP tables:

- ENTITY-MIB.entPhysicalTable
- OLD-CISCO-CHASSIS-MIB.cardTable
- IF-MIB.ifTable
- RFC1407-MIB.dsx3ConfigTable
- RFC1406-MIB.dsx1ConfigTable

- CISCO-POP-MGMT-MIB.cpmDS0UsageTable
- CISCO-MODEM-MGMET-MIB.cmLineStatusTable

Discovering Objects Automatically

Caution Do not attempt to discover all network objects in bulk mode. Discover objects by specifying a range of (approximately 30) IP addresses.

Step 1 From the Map Viewer, select the object (region, site, or device) that you want to discover.

Step 2 To open the Discover Network Devices window, right-click the device and select **Discovery** > **Auto discovery**.

Step 3 Select the drop down list next to Discovery Method and select **SNMP** or **IP and SNMP**.

Step 4 Set the **Hop Count** to the number of subsequent levels of subnets that you want to discover.

Note The maximum number of subnets that you can discover is 16.

Step 5 For IP devices in the **Ping Retries** data entry box, specify the number of times the system should try Internet Control Message Protocol (ICMP) ping to identify whether an active machine is connected to a specified address.

The maximum number of ping retries is 10.

Step 6 Enter a community name in the **New Community** data entry box; then, click **Add**.

Step 7 In the data entry box next to **SNMP Retries**, enter the number of times the system should try to get the RFC1213-MIB.system attribute from a device without receiving a reply before the device is discarded as not being an SNMP device.

The maximum number is 10.

Step 8 In the Physical Location panel, click **Use Physical Path**. If required, select **Get Path** for the correct physical view.

Step 9 In the data entry box next to **SNMP Timeout**, enter the required time. The default is set to 10 seconds.

Step 10 (Optional) You can restrict the IP address range that the system interrogates by double-clicking **Device Interface**.

The Discovery Interface window appears.

Step 11 (Optional) Specify a range of IP addresses (or even a single address) by entering a start address and a stop address. Only IP addresses within the specified address range are discovered.

Step 12 To start the discovery process, select the device from the Device Interfaces list.

Step 13 Click **Start**.

Note You can stop creating and deploying device objects by clicking **Stop**.

When the Network Access Server (NAS) object is discovered, the process is immediately followed by the automatic discovery of NAS components, such as cards and ports. This subcomponent discovery leads to the creation (under the NAS object) of the hierarchy of subcomponent objects.

Overview of Deploying Device Objects Manually

You can deploy Cisco UGM device objects manually by using templates. In addition, you can discover device subcomponents automatically by getting a number of SNMP tables from the NAS. (There is no manual deployment for device subcomponents.)

You can use either of the following templates for each type of managed device in your network:

- Template for AS5*xxx* as Decommissioned—Use this template to deploy a device only; not to discover any of its subcomponents.

Tips This template creates an object in a decommissioned state; Cisco UGM does not process its traps, and performance data is not collected.

- Template for AS5*xxx* with Sub-Chassis Discovery—Use this template to deploy and commission the device and automatically initiate subcomponent discovery.

In the manual deployment mode, you can assign NAS device object names, whereas in auto-discovery mode, Cisco EMF assigns device object names based on the IP address of the device.

The device objects are discovered and located in the region or site from where you manually initiated the deployment.

Deploying Device Objects Manually

Caution When you manually deploy device objects:

Check that the IP address or device name that you specify is not already used in the network of Cisco UGM-managed devices. If a conflict is detected, the manual deployment fails.

Verify that the type of NAS device matches the template that you specify. If you use an AS5*xxx* template to deploy an AS5*yyy* device type, Cisco UGM detects a conflict, and creates the device object in the errored state with no subcomponents. Delete the object and deploy a device object that matches the template.

Step 1 Click a site or region in the left pane until you access the device to be deployed.

Step 2 Right click the device and select: **Deployment > Deploy Access Servers> Deployment Wizard—Templates**. Select the template that you want.

Step 3 Enter the number of objects. If you enter a number greater than 1, repeat Step 4 for each object.

Step 4 Enter the IP address of the device that you want to deploy and click **Forward**.

The device subcomponents are deployed automatically only if you chose a template with subcomponent discovery.

See the "Overview of Deploying Device Objects Manually" section on page3-6.

Overview of Exporting Inventory Data

With Cisco UGM, you can export your system inventory data into a flat text file. By using report-generating software, you can format this data into a report. Exporting files allows you to export data from the database to a UNIX directory; then, you can send the file to an external system through File Transfer Protocol (FTP).

- Schedule only one file (at a time) for inventory data export. If multiple files are scheduled for export at different intervals (hourly, daily, weekly, or monthly) only the last scheduled export saved is active. Any previously specified inventory data exports are ignored.
- Exporting inventory files enables you to get a snapshot of the managed devices' physical view in a flat file. Data output consists of device names and associated attributes.
- Schedule inventory export to occur automatically on an hourly, daily, weekly, or monthly basis. Or you can trigger it immediately.
- Specify the aging time (number of days) and action (delete, move, compress) for the inventory output files.
- Exported inventory objects consist of site, region, device, and subcomponent objects.
- Exported attributes include IP address, shelf, slot, and port numbers for subcomponent objects.

Scheduling Inventory Data Export

By default the inventory data export feature is disabled. Follow these steps to enable this feature:

Step 1 In the Map Viewer, choose **Physical > ASEMSConfig > File Export > File Export Properties**.

Step 2 In the File Export Properties dialog box, click the **Inventory** tab.

Step 3 Select **Scheduled Export**.

Step 4 Enter the location where the exported file will be stored and the delimiter that you want to use.

Step 5 Select the file aging action, duration, and directory where the aged file will be stored.

Step 6 Select the time interval when you want the inventory text file to be created. The export takes place at the beginning of the hour. For example, if the interval is set to hourly, the export takes place at 1:00, 2:00... every day.

Step 7 Click **Save**.

Updating Inventory Data

Inventory data is retrieved during the discovery of network objects. You can update the inventory data by forcing rediscovery of any number of network objects.

Step 1 In the Map Viewer, right-click the device, region, or site where you want to initiate rediscovery.

Step 2 For a site or region, select **ASMainEM > Chassis Commissioning**.

Or

For a single device object, select **Chassis > Chassis Commissioning**.

Step 3 From the object list, select the device or multiple devices that you want to rediscover.

Step 4 Click **Decommission** and wait for the object to transition to the Decommissioned state.

Step 5 Click **Commission** to discover network objects. Wait until the objects transition to the Normal state.

Inventory data has been updated for the selected objects. To export the inventory data, complete the "Exporting Inventory Data Immediately" section on page3-10.

Exporting Inventory Data Immediately

Step 1 In the Map Viewer choose **Physical > ASEMSConfig > File Export > File Export Properties**.

Step 2 In the File Export Properties dialog box, click the **Inventory** tab.

Step 3 Enter the location where the exported file will be stored, and the delimiter that you want to use.

Step 4 Click **Save**.

Step 5 Click **Export Now**.

Exporting a File

Step 1 In the Physical view, select the object for which you want to export inventory data. Right click the object and choose **ASEMSConfig > File Export > Open File Export Properties > Inventory**.

Step 2 In the Export Type field, enter:

- **Scheduled**—Enables scheduled inventory export.
- **None**—Disables scheduled inventory export. Select this option if you plan to immediately export data (see Step 12 in this procedure).

  If you followed this step, skip Step 8 through Step 11.

Step 3 Enter a storage path for the inventory data file.

Step 4 Enter a delimiter to use between fields of data in the report.

The default value of the delimiter is the "|" string.

Step 5 Select an action to be performed when file aging occurs:

- **none**—Disables aging; File Age and Aging Directory fields are ignored.
- **delete**—Deletes the aged file from the disk.
- **move**—Moves the aged file into the aging directory.

- **moveTarCompress**—Compresses the aged file; then, adds it to the FileExport.tar file which, if it does not already exist, is created in the Aging Directory.

Step 6 Enter the maximum size (in KBytes) of a file before the selected aging action is performed. Export then continues in the newly created file.

Step 7 Enter a location where the file is moved to (or moveTarCompressed to) when aging occurs.

- If you enter a non-existent directory path, the directory path is automatically created.
- This location field does not apply to the delete aging action.
- The directory string that you enter must end with a trailing / (forward slash).
- If the Action field is set to moveTarCompress, a tar file named FileExport.tar is created in the Aging Directory to contain aged files.

Step 8 Select the frequency of data export:

- **hourly**
- **daily**
- **weekly**
- **monthly**

Step 9 Select the hour for the export:

- **n/a**—If the Period field was set to an hourly value.
- **0 through 23**—The scheduled hour for the export.

Step 10 Select the scheduled week day for the export:

- **n/a**—If the Period field was set to hourly, daily, or monthly values.
- **Monday through Sunday**—Scheduled week day for the export.

Step 11 Select the scheduled day of the month for the export:

- **n/a**—If the Period field was set to hourly, daily, or monthly values.
- **1 through 31**—Scheduled day of the month for the export.

Step 12 Click **Export Now.**

- Triggers the immediate export of inventory data by using the saved Storage Path and Delimiter.
- Cancels a running inventory export (if any) and begins a new one.

- Generates an Action Report dialog containing results of this action.

Step 13 Click **Save**.

- Saves user-specified data.
- Changes are validated and applied to the system (if valid).
- Generates an Action Report containing results of this action.

See the "Format of Exported Data" section on page3-14.

Example of an Inventory Export File

See the "Format of Exported Data" section on page3-14 for a description of fields in this file.

```
Physical:/Region-1|Region|
Physical:/Region-1/AS5400-1|AS5400Chassis|172.24.217.24|
Physical:/Region-1/AS5400-1/CT3_DFC|CT3Card|0|
Physical:/Region-1/AS5400-1/FastEthernet0_0|FastEthernetPort|
Physical:/Region-1/AS5400-1/FastEthernet0_1|FastEthernetPort|
Physical:/Region-1/AS5400-1/NP108DFC|UPCard|0|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-0|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-1|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-10|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-100|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-101|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-102|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-103|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-104|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-105|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-106|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-107|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-11|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-12|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-13|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-14|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-15|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-16|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-17|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-18|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-19|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-2|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-20|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-21|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-22|UniversalPort|
Physical:/Region-1/AS5400-1/NP108DFC/UnivPort-2-23|UniversalPort|
```

Format of Exported Data

Inventory export data is formatted as follows:

<Device pathName>|<Device Type>|<attribute1>|<attribute2>....

where attributes (if any) are specific to the device or subcomponent.

Table3-1 Inventory Export Data Format

Device Type	Attributes
Site	<State>|<City>
AS5350Chassis	<ipaddress>
AS5400Chassis	<ipaddress>
AS5800Chassis	<ipaddress>
AS5850Chassis	<ipaddress>
ASUPCarrierCard	<shelf#>
ASBundleCarrierCard	<shelf#>
ASRSCCard	<shelf#>
ASDSCCard	<shelf#>
AST1Card	<shelf#>
ASE1Card	<shelf#>
ASCT3Card	<shelf#>
ASModemCard	<shelf#>
ASUPCard	<shelf#>
ASDS1Port	<port#>|<slot#>|<shelf#>
ASE1Port	<port#>|<slot#>|<shelf#>
ASDS3Port	<port#>|<slot#>|<shelf#>

Note If a device or subcomponent is not listed in this table, no attribute information is generated for it; just the pathname and device type appear.

Any unrecognized devices appear as “Unknown” for the device type.

Configuring Devices with Cisco UGM

This chapter contains the following sections. Complete the tasks in this order:

Overview of Configuring Managed Devices

Many users can access Cisco UGM—like all Element Management Systems—on the Cisco EMF platform. You must take precautions to avoid simultaneously accessing and modifying the same network object or any of its components. Establish access schedules for all your users.

Tips

Before testing IOS operations on your Cisco UGM system, save the original configuration file from the device, so that you can retrieve it if necessary.

This table shows configuration actions available for Cisco UGM-managed devices: Cisco AS5350, AS5400, AS5800, and AS5850.

Table 4-1 Configuration Actions and the Devices on Which They Are Supported

	AS5350	AS5400	AS5800	AS5800 with 324 Universal Port Card	AS5850	State Change	Can Be Scheduled
Get Configuration	Yes	Yes	Yes	Yes	Yes	No	No
Send Configuration	Yes	Yes	Yes	Yes	Yes	Yes	No

Task 1: Preparing the Device for Configuration

Changes that you make in the Device Readiness Configuration dialog box are applied only to the selected device object.

Step 1 In **Map View > Physical**, right-click the device object to be configured, and select **Device Readiness Configuration**.

Step 2 Click the **Login** tab. Select an authentication method:

- **Group**—(Default) The device uses the values defined in the Group Authentication method and the Group Authentication Object Name.

  These values are defined in the System Object Settings dialog box (Map View > Physical > AS5*xxxx* > Device Readiness Configuration).

- **Local**—If you select this value, the authentication values that you enter in the following steps are applied to the device.

Step 3 (Optional) Enter the name of the Group Authentication object used by this device.

This field is used only if you selected the **Group** authentication method.

Step 4 Enter a password for administrators to access the system.

Step 5 Enter the username as configured on the device.

Or

This entry must match a username that you selected when building the device configuration file. See the "Task 3: Option 1: Building a Configuration File from a Template" section on page4-5.

Step 6 Enter a password corresponding to the User ID, followed by the login password.

Or

This entry must match a password that you selected when building the device configuration file. See the "Task 3: Option 1: Building a Configuration File from a Template" section on page4-5.

Step 7 Click **OK**.

Step 8 Click the **Trap** tab. Select the interface where SNMP traps currently originate.

Step 9 Select if the traps should be saved to NV Ram.

Step 10 Click **Set Trap Source and Trap Receiver**.

This starts Cisco IOS commands that enable trap forwarding by using the specified input as the source interface and the Cisco UGM server host as the trap destination.

Task 2: Entering IOS Access Parameters

Step 1 In the Physical tree, locate and right-click the device object for which you want to enter access parameters.

Step 2 Select **Configure Device > Perform IOS Operations**.

Step 3 Select the interface through which Cisco IOS commands can access the selected devices.

- **Console**—Enables you to access and configure the selected devices through a connected console even, if the Ethernet address for the selected device is inaccessible.
- **Ethernet**—Enables you to directly access the selected devices through the IP addresses by which the device was discovered during deployment.

  If you selected the Ethernet configuration interface, the IP address of the target device (discovered when the device was deployed) appears.

Step 4 If you selected the Console configuration interface to configure the device, enter the IP address and the port number of the connected console.

Step 5 Select the firmware upgrade method:

- **busyout** (Graceful)—The modem/SPE image is upgraded immediately on idle modem ports. The modem ports with calls are upgraded after the calls are completed.
- **reboot** (Forceful)—The modem/SPE image is upgraded when the device is rebooted.
- **download-maintenance**

Step 6 After you enter the IOS access parameters, save them:

- If you want to apply all the displayed IOS access parameters to your selected devices, click **Save**.

Note If you enter IOS Access Information for multiple devices and click Save, Cisco UGM saves only the Configuration Interface, Console Address, and Firmware Upgrade Option.

Cisco UGM does not save the Ethernet Address and Console Port Number because these attributes are unique for each device.

- If you want to apply only the IOS access parameters that you changed to your selected devices, click **Save File** in the icon bar.
- If you specify IOS access parameters for multiple devices, but other individual devices have unique IOS access parameter values (such as login name or password), select that device only, modify the parameter, and click **Save**.

Task 3: Option 1: Building a Configuration File from a Template

To build a configuration file from a template, complete the following procedures in this order:

1. Selecting Access Parameters (General Tab), page 4-6
2. Selecting Card Parameters (Slots Tab), page 4-6
3. Selecting Interface Parameters (Interface Tab), page 4-7
4. Entering SNMP Information for Traps (SNMP Tab), page 4-7
5. Selecting IOS Core Dump and Logging Parameters (Management Tab), page 4-7
6. Entering Modem and SPE Parameters (Modem/SPE Tab), page 4-9
7. Entering Network Communication Parameters (Other Tab), page 4-9
8. Building and Viewing the Configuration, page 4-10

However, if you wish to use an existing configuration file, see the "Task 3: Option 2: Using an Existing Configuration File" section on page 4-11.

Selecting Access Parameters (General Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx* TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Click the **General** tab.

Step 3 Enter the host name of the device.

Step 4 Select the authentication method for users, accounting, administrative users, the network, and Point-to-Point Protocol (PPP) users if necessary.

Step 5 Enter the authentication key to use with Radius or Terminal Access Controller Access Control System (TACACS) servers.

Step 6 Select the list of Radius or TACACS servers to use for authentication.

Step 7 Enter local user names and passwords.

Selecting Card Parameters (Slots Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx* TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Click the **Slots** tab.

Step 3 Select the type of card installed in each slot.

Step 4 (Optional) Select the framing type used by the controller in this slot.

This field is applicable only if a trunk card occupies the slot.

Step 5 (Optional) Select the controller line code for this slot.

This field is applicable only if a trunk card occupies the slot.

Step 6 (Optional) Select the type of signal used when a channel type is channelized.

This field is applicable only if a trunk card occupies the slot and is configured to be Primary Rate Interface (PRI).

Selecting Interface Parameters (Interface Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx*TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Click the **Interface** tab.

Step 3 Select the ISDN switch type.

Step 4 Enter port IP addresses and masks.

Step 5 Enter loopback IP addresses and masks.

Entering SNMP Information for Traps (SNMP Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx*TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Click the **SNMP** tab.

Step 3 Enter the location and owner of this stack.

Step 4 Enter the SNMP read and write community strings.

Step 5 Enter IP addresses of hosts where traps will be sent.

Selecting IOS Core Dump and Logging Parameters (Management Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx*TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Click the **Management** tab.

Step 3 To enable an IOS core dump to all the hosts on the core dump list, select:

- **Yes**
- **No**

Step 4 (Optional) Select a transfer method to use when sending the IOS core dump file to its destinations:

- **ftp**
- **tftp**

This field is applicable only if you enabled IOS core dump transfer.

Step 5 (Optional) Enter the name of the FTP user that will send the IOS core dump file.

This field is applicable only if you enabled IOS core dump transfer and selected the FTP transfer method.

Step 6 (Optional) Enter a filename for the IOS core dump file being transferred.

The default for this field is hostname-core. This field is applicable only if you enabled IOS core dump transfer.

Step 7 (Optional) Enter a password to use when sending the IOS core dump file through FTP.

This field is applicable only if you enabled IOS core dump transfer and selected the FTP transfer method.

Step 8 (Optional) Enter a list of hosts or IP addresses that will receive the IOS core dump file.

This field is applicable only if you enabled IOS core dump transfer.

Step 9 To enable logging hosts, select:

- **Yes** to enable the device to send syslog to the logging hosts. (This is the default.)
- **No** to disable the transfer of syslog to the logging hosts.

Step 10 Select a logging facility.

Step 11 Select a level of traps to be sent to the logging server.

Step 12 Enter the IP addresses where you want to send logging information.

If the logging hosts are enabled, Cisco UGM sets the Cisco EMF server address as a logging host.

Step 13 Select the time zone in which this device is located.

Step 14 Specify if this device uses daylight savings time.

Step 15 Enter the IP addresses of Network Time Protocol (NTP) servers.

Entering Modem and SPE Parameters (Modem/SPE Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx*TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Select if you want to enable the modem or SPE firmware upgrade in the configuration file.

Step 3 (Optional) Select the modem/SPE firmware upgrade method:

- **busyout** (Graceful)—Upgrades the modem/SPE image immediately on idle modem ports. The modem ports with calls are upgraded after the calls are completed.
- **reboot** (Forceful)—Upgrades the modem/SPE image during the next device reboot.
- **download-maintenance**

This field applies only if you enabled modem or SPE upgrade.

Step 4 Enter the SPE firmware file name that is stored in Flash memory.

Entering Network Communication Parameters (Other Tab)

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx*TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Enter the beginning and ending IP addresses of the local IP address pool.

Step 3 Enter the Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous system number.

Step 4 Enter a list of EIGRP network IP addresses.

Step 5 Enter the Challenge Handshake Authentication Protocol (CHAP) host name for this device.

Step 6 Select if Virtual Private Dialing Network (VPDN) support is enabled for this device.

Step 7 Enter a list of DNS server IP addresses.

Step 8 Enter a list of NetBIOS Name Service (NBNS) server IP addresses.

Step 9 Enter a list of default route IP addresses.

Step 10 Enter a list of IP addresses for name servers.

Building and Viewing the Configuration

Step 1 From the Map Viewer window, select **NAS-File-Repository > AS5*xxx*Chassis > Template > Def5*xxx*TemplateFile > Build Config File from Default AS5*xxx* Template.**

Step 2 Click the **General** tab.

Step 3 Click **Build and View Configuration**.

Cisco UGM saves the new configuration file with a unique file name that includes a randomly generated number.

For example, the new file name is similar to 5400.config-16838 and is automatically imported into the NAS-File-Repository. You can now associate the file with a device as described in the "Task 5: Option 1: Associating a Configuration File with a Device Object" section on page4-12.

Task 3: Option 2: Using an Existing Configuration File

To build a new configuration file, see the "Task 3: Option 1: Building a Configuration File from a Template" section on page 4-5.

When you click Get Configuration in the Performing IOS Operations dialog box, you upload the configuration file from a device to the Cisco UGM server. This is a real time operation that cannot be scheduled to later.

Note The Get Configuration operation retrieves the startup IOS configuration on the target device—not the running IOS configuration on that device.

Cisco UGM does not retrieve configuration statements input to the target device after startup. If the running configuration on the target device is different from its startup configuration and you want to retrieve the running configuration, you must manually save the running configuration as the startup IOS configuration on the target device before following this procedure.

Step 1 From the Map Viewer, select the chassis object whose configuration file you want to upload to the server.

Step 2 Choose **AS5*xxx* > Configure Device > Perform IOS Operations.**

Step 3 Select the device from the list, and click **Get Configuration**.

An Action Report window displays the contents of the configuration file that you uploaded.

Step 4 In the Action Report window, click **Save**.

Step 5 Enter a location to store the file.

Step 6 By using a UNIX editor, make changes to the configuration file that you uploaded.

Step 7 Complete the procedure in "Task 4: Importing a Configuration File into the NAS-File-Repository" section on page 4-12.

Task 4: Importing a Configuration File into the NAS-File-Repository

Step 1 Copy the file that you want to import to a directory on the Cisco EMF server where Cisco UGM is installed.

Step 2 Select **NAS-File-Repository > AS5xxxchassis > Import Files/Images**.

The Deployment Wizard appears.

Step 3 In the Template Choices window, select the Configuration option and click **Forward**.

Note Select the choice that applies to the file you want to import.

Step 4 In the first Object Parameters window, note or enter the name of the configuration file object as it will appear in the Map Viewer.

Step 5 Enter the path, filename, and description of the IOS configuration file to be imported into the NAS-File-Repository.

Step 6 View the summary dialog box. If this information is correct, click **Finish**.

Step 7 When you receive a message indicating that the file was stored successfully, click **Dismiss**.

The user-supplied IOS configuration file is now stored in the appropriate category under the NAS-File-Repository view. Now you can associate the file with a specific device in the network.

Task 5: Option 1: Associating a Configuration File with a Device Object

You must associate a configuration file with a device before you can download it to the device.

If you have already associated the configuration file with a device, see "Task 5: Option 2: Re-associating a Configuration File with a NAS-File-Repository Object" section on page 4-14.

Step 1 In the Cisco UGM tree, locate and right-click the device object with which you want to associate the configuration file.

- **AS5350**
- **AS5400**
- **AS5800**
- **AS5850**

Step 2 Choose **Configure Device > Associate File Repository Object with Device**.

Step 3 Select one or more of these device objects:

- **AS5350**
- **AS5400**
- **AS5800**
- **AS5850**

Note If you select multiple device objects, make sure that they are all of the same type: all Cisco AS5350, AS5400, AS5800, or AS5850 devices.

Step 4 Select one of these device objects:

- **AS5350Chassis**
- **AS5400Chassis**
- **AS5800Chassis**
- **AS5850Chassis**

Step 5 Select **Configuration** as the type of file to download to the selected device. This is an IOS configuration file with prespecified parameters.

Note You cannot associate the same configuration file with multiple devices in the same operation.

Step 6 View the downloaded file objects and select the version of the configuration file that you want to apply.

When you select the imported file version, the Selected File Repository Object, Description, and Original File Path fields are updated to show the attributes of the selected file.

Step 7 Click **Save Association**.

The corresponding field in the Device Associated With panel is updated to reflect the new configuration file association.

Task 5: Option 2: Re-associating a Configuration File with a NAS-File-Repository Object

By re-associating an existing file repository object with a new file, you can download the new configuration to many devices without associating the file with each device.

"Task 5: Option 1: Associating a Configuration File with a Device Object" section on page4-12 shows you how to associate a configuration file with a device.

Step 1 In the Cisco UGM tree under the NAS-File-Repository node, locate and right-click the IOS configuration file object that you want to associate with a new configuration file.

Step 2 Select **Re-associate File Repository Object with New File**.

Existing NAS-File-Repository objects are listed in the left-hand list box.

Step 3 Select the name of the existing NAS-File-Repository object that you want to associate with a new file.

Step 4 Enter a description for the new file.

The original filename and path associated with the selected repository object appears.

Step 5 Enter the path and filename of the new configuration file that you want to store as the NAS-File-Repository object that you selected in Step 3.

Step 6 Click **Save Association**.

The NAS-File-Repository object points to the new or modified file, and the association with the device is updated.

Task 6: Downloading a Configuration File from the Cisco UGM Server to a Device Object

You can download a configuration file from the Cisco UGM server to a managed device by clicking Send Configuration in the Performing IOS Operations dialog box.

- This is a real time operation that cannot be scheduled to run at a future time.
- The target devices must be in the normal state before you can start downloading a file.
- Clicking Send Configuration changes the device state from normal to softwaredownload, and back to normal when the download is complete.
- Clicking Send Configuration reboots the target devices.
- The Send Configuration operation on multiple devices is performed sequentially.

  You can install a configuration file on several managed devices. In order to do this, you must first check that all selected devices are of the same type, and then associate the configuration file with each individual device.

Note You cannot associate the same configuration file with multiple devices with a single command.

Step 1 From the Map Viewer, select the device object which will receive the new configuration file.

Step 2 Choose **AS5xxx > Configure Device > Perform IOS Operations.**

Step 3 Select the devices from the left-side list and click **Send Configuration**.

(Optional) Task 7: Viewing Configuration Files

You can view the text commands in a configuration file that has been stored as an object in the NAS-File-Repository.

Note You cannot view Cisco IOS, SPE, or modem images.

Step 1 Under the NAS-File-Repository node in the Cisco UGM tree, locate and right-click the IOS configuration file object that you want to view.

Step 2 Select **View Configuration File**.

Step 3 Select the name of the existing configuration file object that you want to view.

Step 4 To see the text in the file, Click **View**.

The contents of the configuration file object appear in the Action Result window.

Step 5 After you finish viewing the file, click **Close**.

(Optional) Task 8: Editing Configuration Files

Step 1 Complete the procedure through Step 4 in the "(Optional) Task 7: Viewing Configuration Files" section on page 4-16.

Step 2 By using a UNIX file editor, make any necessary changes to the file you just saved.

Step 3 After viewing the file, click **Save**.

Step 4 Click **Close**.

Step 5 Complete the procedure in the "Task 5: Option 2: Re-associating a Configuration File with a NAS-File-Repository Object" section on page 4-14.

Managing Images and Scheduling Actions with Cisco UGM

This chapter contains the following sections:

Overview of Image Management

Many users can access Cisco UGM—like all Element Management Systems—on the Cisco EMF platform. You must take precautions to avoid simultaneously accessing and modifying the same network object or any of its components.

Note Establish access schedules for all your users.

This table shows image management actions available for Cisco UGM-managed devices Cisco AS5350, AS5400, AS5800, and AS5850:

Table5-1 Image Management Actions and the Devices on Which They Are Supported

	AS5350	AS5400	AS5800	AS5800 with 324 Universal Port Card	AS5850	State Change	Can Be Scheduled
Send IOS Image	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Install Modem Image	N/A	N/A	Yes	N/A	N/A	Yes	Yes
Install SPE Image	Yes	Yes	N/A	Yes	Yes	Yes	Yes

With Cisco UGM, you can install an image file on several managed devices. In order to do this, you must first associate the image file with the devices; then, download the image to the devices.

Note When you complete IOS operations on the devices, do not close the IOS Operations dialog box. After the actions are completed, an Action Report window shows the status of all attempted IOS operations.

Task 1: Preparing the Device for a New Image

Changes that you make are applied only to the selected device.

Step 1 In **Map View > Physical**, right-click the device object that will receive the new image, and select **Device Readiness Configuration**.

Step 2 Click the **Login** tab. Select an authentication method:

- **Group**—(Default) The chassis uses the values defined in the Group Authentication method and the Group Authentication Object Name.

  These values are defined in the System Object Settings dialog box (Map View > Physical > AS5*xxxx* > Device Readiness Configuration).
- **Local**—If you select this value, the device uses authentication values that you enter in Step 3.

Step 3 Enter the Group Authentication Object Name to apply to the device.

Step 4 Enter a password for administrators to access the system.

Step 5 Enter the username as configured on the device.

Step 6 Enter a password corresponding to the User ID, followed by the login password.

Step 7 Click **OK**.

Step 8 Click the **Trap** tab. Select the interface where SNMP traps currently originate.

Step 9 Choose if the traps should be saved to NV Ram.

Step 10 Click **Set Trap Source and Trap Receiver**. This starts Cisco IOS commands that enable trap forwarding by using the specified input as the source interface and the local host as the trap destination.

Task 2: Entering IOS Access Parameters

Step 1 In the Physical tree, locate and right-click the device for which you want to enter access parameters.

Step 2 Select **Configure Device > Perform IOS Operations**.

Step 3 Select the interface through which Cisco IOS commands can access the selected devices.

- **Console**—Enables the administrator to access and configure the selected devices through a connected console.

  Doing so ensures access, even if the Ethernet address for the selected device is inaccessible.

Note If you plan to download an IOS image to a Cisco AS5800 device, select **Console** in this field. In the Cisco AS5800 device, Cisco UGM discovers the router shelf to represent the device, and the controllers are discovered as device subcomponents.

- **Ethernet**—Enables the administrator to directly access the selected devices through the IP addresses found during device deployment.

  If you selected the Ethernet configuration interface, the IP address of the target device (discovered when the device was deployed) appears.

Step 4 If you selected the Console configuration interface to configure the device, enter the IP address and the part number of the connected console.

Step 5 Select the firmware upgrade method:

- **busyout** (Graceful)—The modem/SPE image is upgraded immediately on idle modem ports. The modem ports with calls are upgraded after the calls are completed.
- **reboot** (Forceful)—The modem/SPE image is upgraded when the device is rebooted.
- **download-maintenance**

Step 6 After you have entered the IOS access parameters, save them:

- If you want to apply all the displayed IOS access parameters to your selected devices, click **Save**.
- If you want to apply only the IOS access parameters that you changed in this dialog to your selected devices, click **Save File** in the icon bar.

- If you have specified IOS access parameters for multiple devices, but other individual devices have unique IOS access parameter values (such as login name or password), select that device only, modify the parameter, and click **Save**.

Task 3: Importing an Image File into the NAS-File-Repository

Step 1 Choose **NAS-File-Repository > AS5xxxchassis > Import Files/Images**.

The Deployment Wizard appears.

Step 2 In the Template Choices window, select the option appropriate to the file that you want to import.

- **Store IOS Image File**
- **Store Modem Image File**
- **Store SPE Image File**

Step 3 Click **Forward**.

Step 4 In the first Object Parameters window, note or enter the name of the image file object as it will appear in the Map Viewer.

Step 5 Click **Forward**.

Step 6 Enter the path, filename, and description of the image file you want to import into the NAS-File-Repository.

Step 7 View the summary dialog. If this is correct, click **Finish**.

Step 8 When you receive a message indicating the store operation was successful, click **Dismiss**.

The user-supplied image file is now stored in the appropriate category under the NAS-File-Repository view. Now you can associate it with a specific device in the network.

Task 4: Option 1: Associating an Image with a Chassis Object

You must associate an image file with a device before you can download it to the device.

If you have already associated the image file with a device, see "Task 4: Option 2: Re-associating an Image with a NAS-File-Repository Object" section on page5-7.

Step 1 In the Cisco UGM tree, locate and right-click the device with which you want to associate the image file:

- **AS5350**
- **AS5400**
- **AS5800**
- **AS5850**

Step 2 Choose **Configure Device > Associate File Repository Object with Device**.

Step 3 Select one or more of these device objects:

- **AS5350**
- **AS5400**
- **AS5800**
- **AS5850**

If you select multiple devices, make sure that they are all of the same type: all AS5350, AS5400, AS5800, or AS5850 devices.

Step 4 Select one of these device objects:

- **AS5350Chassis**
- **AS5400Chassis**
- **AS5800Chassis**
- **AS5850Chassis**

Step 5 Select the type of image file that you want to download to the selected device. This is an IOS configuration file with pre-specified parameters.

Step 6 View the imported file objects and select the version of the configuration file that you want to apply.

When you select the imported file version, the Selected File Repository Object, Description, and Original File Path fields are updated to show the attributes of the selected file.

Step 7 Click **Save Association**.

The corresponding field in the Device Associated With panel is updated to reflect the new image file association.

Task 4: Option 2: Re-associating an Image with a NAS-File-Repository Object

By re-associating an existing file repository object with a new file, you can download the new image to many devices without associating the file with each device.

Step 1 In the Cisco UGM tree under the NAS-File-Repository node, locate and right-click the image file object that you want to associate with a new configuration file.

Step 2 Select **Re-associate File Repository Object with New File**.

Existing NAS-File-Repository objects are listed in the left-hand list box.

Step 3 Select the name of the existing NAS-File-Repository object that you want to associate with a new file.

Step 4 Enter a description for the new file.

Cisco UGM displays the original filename and path associated with the selected repository object.

Step 5 Enter the path and filename of the new image file that you want to store as the NAS-File-Repository object that you selected in Step 3.

Step 6 Click **Save Association**.

The NAS-File-Repository object points to the new or modified file, and the association with the device is updated.

Task 5: Option 1: Downloading an IOS Image

You can download the image to a device now, or schedule it for a later date or time. If you chose to schedule the action for a later time, a Scheduled Action object is created under the ScheduledActions view. The target devices appear under the scheduled action object. You can cancel the scheduled action by deleting its object from the ScheduledActions view.

See the "(Optional) Task 6: Viewing or Cancelling Scheduled Actions" section on page5-12.

- The target devices must be in normal state before you can download an IOS image to a device.
- The Install IOS Image operation changes the device state from normal to softwaredownload, and back to normal when the operation is completed.
- The Install IOS Image operation reboots the target devices.
- The Install IOS Image operation on multiple devices is performed sequentially.
- The IOS image that you send to a target device must be smaller than the available Flash space on that device or the transfer will fail.
- More than one IOS image can reside on the device if there is adequate Flash space.

Note If the image installation fails, you must manually reinstall the IOS image on the target device immediately to prevent an unscheduled restart that sends the device into boot mode.

Tips If the Install IOS Image operation was scheduled, but you subsequently deleted the devices from the Viewer Map, the devices are deleted from all Cisco UGM views—including the ScheduledActions view.

Step 1 You can select an image by entering these commands:

show flash

config t

boot system flash *imagename*

Tips *imagename* is the name of the IOS image that you select from Flash memory.

Step 2 From the Map Viewer, select the device object which will receive the new configuration file.

Step 3 Choose **AS5*xxx* > Configure Device > Perform IOS Operations**.

Note If you are installing an IOS image on multiple devices, check that all selected devices are of the same type.

Step 4 Select the devices from the left-side list and click **Install IOS Image**.

Task 5: Option 2: Downloading a Modem Image

You can download the image now or schedule it for a later date or time. If you chose to schedule the action for later, a Scheduled Action object is created under the ScheduledActions view. The target devices are shown under the scheduled action object. You can cancel the scheduled action by deleting the scheduled action object from the ScheduledActions view.

See the “(Optional) Task 6: Viewing or Cancelling Scheduled Actions” section on page5-12.

- The target devices must be in normal state before you can download a modem image.
- The Install Modem Image operation changes the device state from normal to softwaredownload, and back to normal when the operation is completed.
- The Install Modem Image operation does NOT reboot the target devices.
- The Install Modem Image operation on multiple devices is performed sequentially.
- If the operation fails, the old modem image is still valid.
- The modem image that you send to a target device must be smaller than the available Flash space on that device, or the transfer will fail.
- More than one modem image can reside on the device if there is adequate Flash space.
- The modem image that you send to a target device will affect all modems on the device.

Tips If the Install Modem Image operation was scheduled, but you subsequently deleted the devices from the Viewer Map, the device is deleted from all Cisco UGM views—including the ScheduledActions view.

The Install Modem Image button in the Performing IOS Operations dialog downloads the image file from the Cisco UGM server to a managed device.

Step 1 You can select an image by entering these commands:

show flash

spe 2

firmware location flash *imagename*

Tips Where *imagename* is the name of the modem image that you select from Flash memory.

Step 2 From the Map Viewer, select the chassis object which will receive the new modem image file.

Step 3 Choose **AS5xxx > Configure Device > Perform IOS Operations.**

Note If you are installing a modem image on multiple devices, check that all selected devices are of the same type.

Step 4 Select the devices from the left-side list and click **Install Modem Image**.

Task 5: Option 3: Downloading an SPE Image

You can download the image now or schedule it for a later date or time. If you chose to schedule the action for later, a Scheduled Action object is created under the ScheduledActions view. The target devices appear under the scheduled action object. You can cancel the scheduled action by deleting the scheduled action object from the ScheduledActions view.

See the "(Optional) Task 6: Viewing or Cancelling Scheduled Actions" section on page5-12.

- The target devices must be in normal state before you can download SPE images.
- The Install SPE Image operation changes the device state from normal to softwaredownload, and back to normal when the operation is completed.
- The Install SPE Image operation does NOT reboot the target devices.
- The Install SPE Image operation on multiple devices is performed sequentially.
- The SPE image that you send to a target device must be smaller that the available Flash space on that device, or the transfer will fail.
- More than one SPE image can reside on the device if there is adequate Flash space.
- If the operation fails, the old SPE image is still valid.
- The SPE image that you send to a target device will affect all SPEs on the device.

Tips If the Install SPE Image operation was scheduled, but you deleted the devices from the Map Viewer, the device is deleted from all Cisco UGM views—including the ScheduledActions view.

Step 1 You can select an image by entering these commands:

show flash

spe 2

firmware location flash *imagename*

Where *imagename* is the name of the SPE image that you select from Flash memory.

Step 2 From the Map Viewer, select the device object which will receive the new SPE image file.

Step 3 Choose **AS5xxx** > **Configure Device** > **Perform IOS Operations.**

Note If you are installing an SPE image on multiple devices, check that all selected devices are of the same type.

Step 4 Select the devices from the left-side list and click **Install SPE Image**.

(Optional) Task 6: Viewing or Cancelling Scheduled Actions

- A scheduled action object is created under the Scheduled Actions view, and the device on which the action will occur is placed under the scheduled action object as a child.
- You can view the time and type of scheduled action in the Scheduled Action Details dialog box.
- The scheduled action object is automatically deleted after the scheduled action is completed.

Note You cannot change the time at which an action is scheduled. Delete the scheduled action and recreate a new one with a different time.

Tips Deleting the device object from the scheduled action object deletes the device object from all Cisco UGM views.

Step 1 Expand the Scheduled Actions root node in the Map Viewer to view the scheduled but unexecuted image installations.

The scheduled operations are labeled by type (IOS image installation, Modem image installation, or SPE image installation) and a random number.

Step 2 (Optional) To view the time of a scheduled action, right-click and select **Scheduled Action Details**.

Step 3 (Optional) To view the target devices of a scheduled action, expand that action object.

Step 4 (Optional) To cancel a scheduled action, right-click the scheduled action and select **Deployment** > **Delete**.

Configuring the Administrative State of Objects

This chapter contains the following sections:

Overview of Configuring Administrative States

With the Cisco UGM Configure Administrative States option, you can:

- Remove an object (T1, E1, E1 combination card, T3, or T3 combination card) from service for maintenance with a minimum of customer impact (Graceful Shutdown).
- Place the object back in service after maintenance (Accept Traffic).

Note References to E1 and T3 cards also include the E1 combination and T3 combination cards.

- The Object List contains the selected (root) object and its immediate children.
- Initial dialog display fields are blank—not "Unknown." After a Configure Administrative State action has occurred, the fields retain their values until the next action for that object. The dialog fields show information from a previous action.

- All dialog fields are logged (at INFO level); they are not just Progress Information.
- If a Configure Administrative State action is in progress at the time of Cisco UGM termination, the action is not restarted at the time of a Cisco UGM restart. A "Graceful Shutdown interrupted" or "Accept Traffic interrupted" alarm is raised instead. These alarms are visible in the Event Browser and must be manually cleared.

Objects Which Support Administrative State Configuration

The Configure Administrative State function applies to the following objects only:

- T1 and E1 cards
- CT3 cards
- PRI + NextPort combination cards
- CT3 + NextPort combination cards

You can perform Graceful Shutdown and Accept Traffic actions only for the entire card (not individual ports or channels).

Graceful Shutdown and Accept Traffic are not supported for DFC or Carrier cards, the chassis, and DS0 channels.

About the Graceful Shutdown Function

Note When you start this function, make sure that no other configuration activity is in progress for the selected card or for its host chassis.

You can gracefully shut down a selected card object in a normal state (no Graceful Shutdown action is currently in effect).

Graceful Shutdown of an object consists of two steps: busyout and shutdown.

- Busyout causes the NAS to inform the other side of the trunk that an object is out of service.

  Busyout does not terminate existing calls; instead, busyout allows existing calls to be completed and prevents any new calls from being established on the object.

  Busyout phases out all DS0 operation on the card. When no active DS0s remain, the T1, E1, and/or T3 controllers (as applicable) on the card are shut down.

- Shutdown abruptly stops operation of an active or idle object.

Typical state transitions during the processing of a Graceful Shutdown action are:

normal to shuttingDown to locked.

These transitions are visible in the bottom left corner of the Configure Administrative State dialog box.

The Configure Administrative State option and Graceful Shutdown are available only for some Cisco UGM objects.

For details, see the "Objects Which Support Administrative State Configuration" section on page 6-2.

About the Accept Traffic Function

Note When you start this function, make sure that no other configuration activity is in progress for the selected card or for its host chassis.

You can Accept Traffic on a selected card object in the locked state (resulting from a prior Graceful Shutdown action that was previously performed for this object).

By doing so, you can either configure the object to start receiving calls, or undo the effect of a graceful shutdown. The object is now in service.

Accept Traffic activates all T1, E1, and T3 controllers on the card (including those that may have been shut down by means other than the Graceful Shutdown method). Use this Accept Traffic method to activate T1, E1, and T3 controllers that are "down."

Typical state transitions during the processing of an Accept Traffic action are:

locked to acceptingTraffic to normal

These transitions are visible in the bottom left corner of the dialog.

Note The Configure Administrative State option (and Accept Traffic) is available only for some Cisco UGM objects. For details, see the "Objects Which Support Administrative State Configuration" section on page6-2.

About Processing Times for Configuring Administrative States

This section describes p rocessing times associated with Configure Administrative State actions:

- The dialog display fields are updated every 10 seconds.
- After you click Accept Traffic, allow approximately 60 seconds for the card to power up.
- Allow approximately 40 seconds for the T1, E1, and T3 controllers (as applicable) to start after you click Accept Traffic.
- When you click Graceful Shutdown, the number of active DS0s must drop to 0 before the shutdown begins. This processing time is difficult to anticipate.

Note The number of active DS0s drops to 0 if all calls terminate on their own, ports are disconnected, or the card is removed from the chassis.

About the Action Report

- The Configure Administrative State dialog fields are updated every 10 seconds; only the last update for a field is visible in the dialog. However, all display field updates appear in the Action Report.
- The Action Report appears either because an action is complete or was interrupted.

- The maximum number of characters in the report is limited to approximately 500,000.
- The report is always timestamped, even if the report is “full.”

Configuring the Administrative State for a Supported Object

- When you shut down an object, it and all its descendants in the Physical hierarchy (except Universal ports in combination cards) are shut down as well.
- Once initiated, you cannot cancel Graceful Shutdown. It must run to completion.
- You cannot shut down T1, E1, and T3 controllers in loopback mode.
- At a given time, you can perform only one Configure Administrative State action.
- If you perform a Graceful Shutdown action on a Cisco AS5350 or AS5400 device, you cannot enter the Accept Traffic command.

  The reason for this is that the busyout command is followed by removal of power to the card; the card is logically removed from the chassis; an OIR trap is issued. Since the card is removed from Physical View, the Accept Traffic action has no object to act on.

  As a workaround, manually remove or insert the card into the chassis to start discovery, or enter the no busyout <*slot*> IOS command to the device.

Step 1 In the Map Viewer, select an object in the Physical hierarchy.

Step 2 Right-click the object and select **Configure Administrative State**.

Step 3 Click one of these actions:

- **Graceful Shutdown**
- **Accept Traffic**

Managing Security on Cisco UGM

This chapter contains the following sections:

Overview of Managing Security on Cisco UGM

With the Access Manager, you can set up the following levels of administrative access to Cisco UGM managed devices and their subcomponents:

- An Access Specification—A set of services or features that a user or a group of users assigned to this access specification are authorized to run.
- A User Group—A group identified by a name with a set of users and a set of Access Specifications.
- A User—A user with an associated set of access specifications.

- Access Permission—Within an access specification, you can set one of three levels of access permission for each Cisco UGM service:
  - Read-Only
  - Read-Write
  - Read-Write-Admin

  With Read-Write-Admin access, you can create users, user groups, and access specifications, and change certain attributes like IP addresses and so on.

Note When setting up security management, first create the access specifications, then the user groups, and finally the users.

Pre-set Cisco UGM Feature Lists and Access Specifications

You can assign these features and access specifications to levels of Cisco UGM users.

Table7-1 Cisco UGM Pre-set Features

Feature List	Description
UGM_ASMainEM_All_Properties_Dialogs	All properties dialog boxes for access server chassis.
UGM_ASMainEM_CLIShowCommands	All CLI show command dialog boxes.
UGM_ASMainEM_Chassis_And_Card_Commissioning	Card and chassis commissioning dialog boxes.
UGM_ASMainEM_FileExport_Configuration	All file export configuration dialog boxes.
UGM_ASMainEM_Configure_Admin_States	Configure administrative state dialog box.

Table7-1 Cisco UGM Pre-set Features (continued)

Feature List	Description
UGM_ASMainEM_PerformancePolling Config	Performance polling configuration and start/stop dialog boxes.
UGM_ASMainEM_Provision_AccessSe rvers	Manual deployment of access servers dialog boxes.
UGM_ASMainEM_TrapForwarding	All trap forwarding configuration dialog boxes.
UGM_ASMainEMCiscoView	CiscoView application invocation dialog boxes.
UGM_IOSFmgrEMDialogFeatureList	All NAS file repository dialog boxes.
UGM_IOSFmgrEMProvisioningFeature List	File import dialog boxes for the NAS file repository.
UGM_IOSMgrDialogFeatureList	IOS operations and scheduled actions properties dialog boxes.
UGM_commonEMDialogFeatureList	Device readiness, device information, log configuration, group authentication, and telnet dialog boxes.
UGM_commonEMProvisioningFeature List	Deployment of group authentication objects dialog boxes.

Note You can modify these access specifications, or add new ones.

Table7-2 Cisco UGM Pre-set Access Specifications

Access Specification	Permission	Feature Lists
UGM_ASMainEM_All_Features	Read-Write -Admin	UGM_ASMainEM_All_Properties_Dialogs UGM_ASMainEM_CLIShowCommands UGM_ASMainEM_Chassis_And_Card_Commissioning UGM_ASMainEM_FileExport_Configuration UGM_ASMainEM_Configure_Admin_States UGM_ASMainEM_PerformancePollingConfig UGM_ASMainEM_Provision_AccessServers UGM_ASMainEM_TrapForwarding
UGM_ASThirdParty	Read-Write -Admin	UGM_ASMainEMCiscoView
UGM_IOSMgr	Read-Write -Admin	UGM_IOSMgrDialogFeatureList
UGM_IOSFmgrEM	Read-Write -Admin	UGM_IOSFmgrEMDialogFeatureList UGM_IOSFmgrEMProvisioningFeatureList
UGM_commonEM	Read-Write -Admin	UGM_commonEMDialogFeatureList UGM_commonEMProvisioningFeatureList

Table7-3 Cisco UGM Features with Associated Permissions

Feature	Permission
ASEMSEventBrowser	Read
ProvisionASMainEMASMainEM	Read-Write
ProvisionASMainEMcontainer	Read-Write
ASMainEMAS5350ChassisOpenShow5350Service	Read-Write
ASMainEMAS5400ChassisOpenShow5400Service	Read-Write

Table7-3 Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
ASMainEMAS5800ChassisOpenShow5800Service	Read-Write
ASMainEMAS5850ChassisOpenShow5850Service	Read-Write
ASMainEMContainerOpenShow5350Service	Read-Write
ASMainEMContainerOpenShow5400Service	Read-Write
ASMainEMContainerOpenShow5850Service	Read-Write
ASMainEMContainerOpenShow5800Service	Read-Write
ASMainEMASGenericChassisOpenAccessServerChassisService	Read
ASMainEMASGenericChassisOpenCardPropertiesService	Read
ASMainEMASGenericChassisOpenDs1e1propertiesService	Read
ASMainEMASGenericChassisOpenDS3PropertiesService	Read
ASMainEMASGenericChassisOpenEthernetPortService	Read
ASMainEMASGenericChassisOpenChannelStatisticsService	Read
ASMainEMASUPCardOpenModemUniversalPortService	Read
ASMainEMASGenericChassisOpenChassisCommissioningService	Read-Write
ProvisionASMainEMASTrapForward	Read-Write
ASMainEMASCT3CardOpenDS3PropertiesService	Read
ASMainEMASGenericCardOpenCardPropertiesService	Read
ASMainEMASDS1E1OpenChannelStatisticsService	Read
ASMainEMASEMSOpenEMSAboutService	Read
ASMainEMContainerOpenStartStopPerfPollingService	Read-Write
ASMainEMASDS1E1OpenDs1e1propertiesService	Read
ASMainEMASPerPollConfigOpenStartStopPerfPollingService	Read-Write
ASMainEMASPerPollConfigOpenGlobalPerfPollConfigService	Read-Write
ASMainEMASGenericNetworkIfOpenEthernetPortService	Read
ASMainEMASGenericChassisOpenModemUniversalPortService	Read
ASMainEMContainerOpenChassisCommissioningService	Read-Write
ASMainEMASModemCardOpenModemUniversalPortService	Read

Table7-3 Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
ASMainEMAST1E1CardOpenDs1e1propertiesService	Read
ASMainEMASDS3PortOpenDS3PropertiesService	Read
ProvisionASMainEMASTrapForwardHost	Read-Write
ASMainEMASSPEOpenModemUniversalPortService	Read
ASMainEMASGenericShutDownableOpenConfigureAdminStateService	Read-Write
ASMainEMASModemOpenModemUniversalPortService	Read
ASMainEMASFileExportOpenFileExportService	Read-Write
ASMainEMASDS0ChannelOpenChannelStatisticsService	Read
ASMainEMContainerOpenAccessServerChassisService	Read
ASMainEMASUniversalPortOpenModemUniversalPortService	Read-Write
ASMainEMASGenericCardOpenCardCommissioningService	Read-Write
ASMainEMASTrapForwardOpenTrapForwardService	Read-Write
IOSFmgrEMIOSFileVersionDeleteService	Read-Write
IOSFmgrEMIOSFileCategoryOpenObjectConfigService	Read-Write
IOSFmgrEMIOSDeviceTypeOpenObjectConfigService	Read-Write
IOSFmgrEMIOSTemplateCategoryOpenObjectConfigService	Read-Write
IOSFmgrEMIOSFileVersionOpenObjectConfigService	Read-Write
IOSFmgrEMIOSAS5350TemplateVersionOpenObjectConfigService	Read-Write
IOSFmgrEMIOSAS5400TemplateVersionOpenObjectConfigService	Read-Write
IOSFmgrEMIOSAS5800TemplateVersionOpenObjectConfigService	Read-Write
IOSFmgrEMIOSAS5850RSC6TemplateVersionOpenObjectConfigService	Read-Write
IOSFmgrEMIOSAS5850RSC7TemplateVersionOpenObjectConfigService	Read-Write
IOSFmgrEMIOSAS5850RSC6TemplateVersionOpenBuildConfigFileFrom 5850RSCSlot6TemplateService	Read-Write
IOSFmgrEMIOSAS5850RSC7TemplateVersionOpenBuildConfigFileFrom 5850RSCSlot7TemplateService	Read-Write
IOSFmgrEMIOSFileVersionOpenReassociateService	Read-Write

Table7-3 Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
IOSFmgrEMIOSTechObjOpenAssociateService	Read-Write
IOSFmgrEMIOSAS5400TemplateVersionOpenBuildConfigFileFrom5400 TemplateService	Read-Write
IOSFmgrEMIOSAS5350TemplateVersionOpenBuildConfigFileFrom5350 TemplateService	Read-Write
IOSFmgrEMIOSAS5800TemplateVersionOpenBuildConfigFileFrom5800 TemplateService	Read-Write
IOSFmgrEMIOSConfigFileCategoryOpenViewFileService	Read-Write
IOSFmgrEMIOSConfigFileVersionOpenViewFileService	Read-Write
ProvisionIOSFmgrEMNAS-File-Repository	Read-Write
ProvisionIOSFmgrEMIOSFileCategory	Read-Write
ProvisionIOSFmgrEMIOSDeviceType	Read-Write
IOSMgrIOSScheduledActionOpenScheduledActionPropertiesService	Read-Write
IOSMgrIOSManageableOpenIOSOperationsDialogService	Read-Write
IOSMgrContainerOpenScheduledActionPropertiesService	Read-Write
IOSMgrContainerOpenIOSOperationsDialogService	Read-Write
CommonEMContainerOpenDevInfoService	Read-Write
CommonEMCommonIOSDeviceOpenDevInfoService	Read-Write
CommonEMCommonctrlLogOpenLogLevelConfigService	Read-Write
CommonEMContainerOpenDevLoginConfigService	Read-Write
CommonEMCommonIOSDeviceOpenDevLoginConfigService	Read-Write
CommonEMCommonSystemObjectOpenSystemObjectSettingsService	Read-Write
CommonEMCommonGroupAuthOpenGroupAuthConfigService	Read-Write
ProvisioncommonEMcommonEM	Read-Write
CommonEMTelnetService	Read-Write

Creating an Access Specification

Note You can create an access specification without an associated user group or feature lists.

Step 1 Start the Access Manager from the Launchpad.

Step 2 In the Access Manager window, choose **Edit > Create > Access Specification**.

Step 3 Enter an Access Specification name, whether you want to replicate another access specification, features and feature lists, level of access (Read-only, Read-Write, or Read-Write-Admin) a user group to which to assign this Access Specification (blank if this is the first time you are setting up system security).

Creating a User Group

Step 1 In the Access Manager window, choose **Edit > Create > User Group**.

Step 2 Enter a group name, whether you want to replicate another group, users to include in this group (blank if this is the first time you are setting up system security), and access specifications for this group.

Creating Users

Note You can assign a user to more than one user group; however, if you assign several permission levels to the same user, Cisco UGM reads the highest permission level that is assigned to this user and establishes that permission level for the user through all the groups.

Step 1 In the Access Manager window, choose **Edit** > **Create** > **User**.

Step 2 Enter a login name, first name, surname, e-mail address, and whether you want to replicate another user, group membership, password, and user description.

Modifying Users, User Groups, and Access Specifications

Tips Only a system administrator can modify an Access Manager User, User Group, or Access Specification.

You can modify security entities from the Access Manager GUI by selecting the **Edit>Modify** menu option, or by selecting the object on the Access Manager GUI screen and double-clicking it.

Managing the Performance of Cisco UGM Devices

This chapter contains the following sections:

Overview of Performance Management Features

With the performance management function, you can:

- Collect selected performance attributes at specific times.
- Store these sampled performance attributes in the database of the attribute history server.
- Poll performance data continuously and store it in the controller database.
- View performance data by using the Performance Manager.
- Export performance data to a flat file.

Note All collected performance data is stored for at least seven days in the database.

- Devices on which you enable performance polling must be in the normal (commissioned) state.

  Cisco UGM checks that the device state is normal; performance polling is not affected by the state of device subcomponents.

- Polling is turned on or off at the device level. All subcomponents in the device have polling either enabled or disabled along with the host device. Specify polling intervals at the MIB attribute level; the intervals are global.

  For example, if the user specifies that the Active DS0s attribute is to be sampled on all devices every five minutes, all Active DS0s in all the Cisco UGM-managed devices with polling enabled are sampled every five minutes.

Note Cisco UGM can monitor only pre-defined performance attributes. You cannot modify or add attributes.

About Adding Devices to be Polled

- fiveMin, fifteenMin, thirtyMin, sixtyMin polling periods—Device objects added during a polling cycle are polled only when the current cycle is completed. For example, if you start polling a device in the middle of a 15-minute cycle, no attribute of that device is polled in the current cycle; data from the device is polled in the next 15-minute cycle.
- oneDay, sevenDay polling periods—If the number of new devices added (during a polling cycle) is more than half of the current number of devices being polled, the current polling cycle is discontinued, and all devices (including the new ones) are polled in the next new cycle.

  If the number of new devices added (during a polling cycle) is less than half the current number of devices being polled in the current cycle, no attribute of the new devices is polled in the current cycle; data from the new devices is polled in the next polling cycle.

Information on Dialog Tabs

- Ethernet dialog tab refers to the Ethernet, Fast Ethernet, and GigaBit Ethernet ports.
- Modem dialog tab refers to the modem and universal ports.
- DS1 dialog tab refers to the DS1 port, DS1 channel, and E1 port.
- Chassis dialog tab refers to the Cisco AS5350, AS5400, AS5800, and AS5850 devices.
- DS0 dialog tab refers to the DS0 channel.
- DS3 dialog tab refers to the DS3 port.
- Others dialog tab contains attribute information that cannot be displayed by the Performance Manager. In order to view this data, export it to a flat file. See the “Overview of the Performance Data Export File” section on page8-16.

Note Select the Dynamic Update option to continuously refresh the properties data (under these tabs) every 10 seconds.

About Polling Intervals and the Number of Devices Polled

When you select polling intervals for device and subcomponent attributes and the number of devices to be polled, make sure that the peak load of performance polling does not exceed Cisco UGM management limits.

Consider these factors when selecting polling intervals:

- Number of devices being polled simultaneously.
- Number of ports being polled for each device. (This includes Ethernet ports, DS0 channels, DS1 ports and channels, DS3 ports, modem ports, and universal ports.)
- Number of network interfaces with sub-queue for each device.

Note If the polling load in your system exceeds Cisco UGM capacity, the Performance Manager displays frequent "Missed Poll" messages. For an explanation of this message, see the "Missed Poll" section on page A-12.

Selecting Performance Polling Intervals

Default performance polling intervals for the chassis and its subcomponents are:

- Chassis—fifteen minutes
- DS0, DS1, DS3, Modem, Ethernet, Others—none

To select or change the default or current performance polling interval:

Step 1 In the Map view, choose **ASEMSConfig > PerfPollConfig > Open Global Performance Polling Configuration.**

Step 2 Click the tab representing the system element to be polled.

See the "Information on Dialog Tabs" section on page 8-3 for more details.

Step 3 Click one of the polling period choices: **None**, **fiveMin**, **fifteenMin**, **thirtyMin**, **sixtyMin**, **oneDay**, and **sevenDay**.

Step 4 Repeat Steps 2 and 3 until you have completed your polling interval selections.

Step 5 Click **Save** in the menu bar.

Step 6 Start performance polling as described in the "Starting and Stopping Performance Polling for the Chassis and Subcomponents" section on page 8-5.

Starting and Stopping Performance Polling for the Chassis and Subcomponents

Step 1 In the Map view, right-click the device, and choose **Chassis > Start/Stop Performance Polling.**

Or

From the Map View, right-click a site (or other container) icon and select **ASMainEM > Start/Stop Performance Polling**. (Use this method to start or stop performance polling on multiple devices.)

Step 2 Select the **performancePolling - ON** option.

If you want to stop performance polling later, access this dialog box again and select the **performancePolling - OFF** option.

Step 3 Click the **Save** button.

Wait for the Action Report window to appear before leaving this screen.

Overview of Performance Data

With the Performance Manager, you can generate line charts or tables to view device and subcomponent performance for most attributes of managed devices—with the exception of those included in the Others tab.

Tips Some data cannot be viewed online; export it to a flat file; then, view it.

Line Charts and Tables

With line charts and tables, you can view device or card attribute data. Cisco UGM plots data corresponding to attributes selected from a list in the Performance Manager dialog box.

Line charts plot a single attribute at a time, whereas tables can represent several attributes. The colored dots (in line charts) or cells (in tables) represent:

- Green indicates that performance polling for the device has started.
- Yellow indicates that a poll for an attribute was missed.
- Red indicates that performance polling for the device has stopped.

The **View** button on the top navigation bar has a drop-down menu that allows you to enhance line charts by selecting:

- **Values**—Plots the values of the samples collected during the line chart.
- **Points**—Plots the time that the samples were collected during the line chart.

Device and Subcomponent Performance Attributes That You Can View

Table 8-1 Chassis Performance Attributes

Text Field	MIB Attribute Name	Description
Bad Community Uses	SNMPv2-MIB snmpInBadCommunityUses	Indicates the number of SNMP messages delivered to the SNMP host that represented an SNMP operation not allowed by the SNMP community named in the message.
Bad Community Names	SNMPv2-MIB snmpInBadCommunityNames	Indicates the number of SNMP messages delivered to the SNMP host that used an SNMP community name not recognized by the SNMP entity.
ISDN Cfg B-Channels in Use	CISCO-POP-MGMT-MIB cpmISDNCfgBChanInUseForAnalog	Indicates the number of configured ISDN B-channels that are currently occupied by both analog and digital calls.

Table8-1 Chassis Performance Attributes (continued)

Text Field	MIB Attribute Name	Description
Active DS0s	CISCO-POP-MGMT-MIB cmpActiveDS0	Indicates the number of DS0s that are currently in use.
ISDN Calls Rejected	CISCO-POP-MGMT-MIB cpmISDNCallsRejected	Indicates the number of rejected ISDN calls in this managed device.
ISDN Calls Cleared Abnormally	CISCO-POP-MGMT-MIB cpmISDNCallsClearedAbnormally	Indicates the number of connected ISDN calls that were cleared by an event other than: • Transmission by the local end of a normal disconnect message. • Reception by the remote end of a normal disconnect message.
ISDN No Resource	CISCO-POP-MGMT-MIB cpmISDNNoResource	Indicates the number of ISDN calls that were rejected because there was no B-channel available to handle the calls.
Average Busy 5 min	OLD-CISCO-CPU-MIB avgBusy5	Represents the 5-minute exponentially decayed moving average of the CPU busy percentage.
System Modems In Use	CISCO-MODEM-MGMT-MIB cmSystemModemsInUse	Indicates the number of network modems that are in these states: • connected • offHook • loopback • downloadFirmware
System Modems Available	CISCO-MODEM-MGMT-MIB cmSystemModemsAvailable	Indicates the number of network modems that are onHook.
System Modems Unavailable	CISCO-MODEM-MGMT-MIB cmSystemModemsUnavailable	Indicates the number of network modems that cannot accept calls.

Table8-1 Chassis Performance Attributes (continued)

Text Field	MIB Attribute Name	Description
System Modems Offline	CISCO-MODEM-MGMT-MIB cmSystemModemsOffline	Indicates the number of network modems that have been placed offline administratively.
System Modems Dead	CISCO-MODEM-MGMT-MIB cmSystemModemsDead	Indicates the number of network modems in one of these states: • Bad • downloadFirmwareFailed
Call Count	CISCO-MODEM-MGMT-MIB cpmCallCount	Indicates the number of calls that have occupied this DS0.

Table8-2 Performance Attributes for the DS0 Port

Text Field	MIB Attribute Name	Description
Call Count	CISCO-MODEM-MGMT-MIB cpmCallCount	Indicates the number of calls that have occupied this DS0.

Table8-3 Performance Attributes for the DS1 Port

Text Field	MIB Attribute Name	Description
Line Status (from RFC1406dsx1ConfigTable)	RFC1406 dsx1LineStatus	Indicates the line status of the interface, and contains loopback, failure, received alarm, and transmitted alarm information.
Errored Seconds	RFC1406 dsx1CurrentESs	Indicates the number of errored seconds encountered by a DS1 interface in the current fifteen-minute interval.
Severely Errored Seconds	RFC1406 dsx1CurrentSESs	Indicates the number of severely errored seconds encountered by a DS1 interface in the current fifteen-minute interval.

Table8-3 Performance Attributes for the DS1 Port (continued)

Text Field	MIB Attribute Name	Description
Errored Framing Seconds	RFC1406 dsx1CurrentSEFs	Indicates the number of errored framing seconds encountered by a DS1 interface in the current fifteen-minute interval.
Line Code Violations	RFC1406 dsx1CurrentLCVs	Indicates the number of line code violations encountered by a DS1 interface in the current fifteen-minute interval.
Controlled Slip Seconds	RFC1406 dsx1CurrentCSSs	Indicates the number of controlled slip seconds encountered by a DS1 interface in the current fifteen-minute interval.
Path Coding Violations	RFC1406 dsx1CurrentPVCs	Indicates the number of path coding violations encountered by a DS1 interface in the current fifteen-minute interval.
Line Errored Seconds	RFC1406 dsx1CurrentLESs	Indicates the number of line errored seconds encountered by a DS1 interface in the current fifteen-minute interval.
Unavailable Seconds	RFC1406 dsx1CurrentUASs	Indicates the number of unavailable seconds encountered by a DS1 interface in the current fifteen-minute interval.

Table8-4 Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports

Text Field	MIB Attribute Name	Description
In/Out Octets	IF-MIB ifInOctets ifOutOctets	Indicates the number of incoming or outgoing octets handled by the card.
In/Out Errors	IF-MIB ifInErrors ifOutErrors	Indicates the number of incoming or outgoing packet errors for the card since the last restart.

Table8-4 Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports (continued)

Text Field	MIB Attribute Name	Description
In Ucast Pkts	IF-MIB ifInUcastPkts	Indicates the number of packets, delivered by this sublayer to a higher sublayer that was not addressed to a multicast or broadcast address at this sublayer.
In NUcast Pkts	IF-MIB ifInNUcastPkts	Indicates the number of packets, delivered by this sublayer to a higher sublayer, that was addressed to a multicast or broadcast address at this sublayer.
In/Out Discards	IF-MIB ifInDiscards ifOutDiscards	Indicates the number of incoming or outgoing packets discarded since the last restart.
In Unknown Protos	IF-MIB ifInUnknownProtos	• Packet-oriented interfaces—Indicates the number of packets, received by the interface, that were discarded due to an unknown or unsupported protocol. • Character-oriented or fixed-length interfaces that support protocol multiplexing—Indicates the number of transmission units received by the interface that were discarded due to an unknown or unsupported protocol. • If an interface does not support protocol multiplexing, this counter is always 0.

Table8-4 Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports (continued)

Text Field	MIB Attribute Name	Description
Out Ucast Pkts	IF-MIB ifOutUcastPkts	Indicates the number of packets that high-level protocols requested to be transmitted, but were not addressed to a multicast or broadcast address at this sublayer. This number includes packets that were discarded or not sent.
Out NUcast Pkts	IF-MIB ifOutNUcastPkts	Indicates the number of packets that high-level protocols requested to be transmitted, and were addressed to a multicast or broadcast address at this sublayer. This number includes packets that were discarded or not sent.

Table8-5 Performance Attributes for Modem and Universal Ports

Text Field	MIB Attribute Name	Description
Ring No Answers	CISCO-MODEM-MGMT-MIB CmRingNoAnswers	Indicates calls which were ringing, but were unanswered at this modem.

Table8-5 Performance Attributes for Modem and Universal Ports (continued)

Text Field	MIB Attribute Name	Description
Incoming Connection Failures	CISCO-MODEM-MGMT-MIB cmIncomingConnectionFailures	Indicates the number of incoming connection requests that this modem answered but failed to train with the other DCE. This object exists only for modems which have cmManageable to be true.
Incoming Connection Completions	CISCO-MODEM-MGMT-MIB cmIncomingConnectionCompletions	Indicates the number of incoming connection requests that this modem answered and successfully trained with the other DCE. This object exists only for modems which have cmManageable to be true.

Table8-6 Performance Attributes for the DS3 Port

Text Field	MIB Attribute Name	Description
Line Status (from RFC1407dsx3ConfigTable)	RFC1407 dsx3LineStatus	Indicates the line status of the interface, and contains loopback, failure, received alarm, and transmitted alarm information.
P-bit Errored Seconds	RFC1407 dsx3CurrentPESs	Indicates the number of P-bit errored seconds encountered by a DS3 interface in the current fifteen-minute interval.
P-bit Severely Errored Seconds	RFC1407 dsx3CurrentPSESs	Indicates the number of P-bit severely errored seconds encountered by a DS3 interface in the current fifteen-minute interval.
Errored Framing Seconds	RFC1407 dsx3CurrentSEFSs	Indicates the number of severely errored seconds encountered by a DS3 interface in the current fifteen-minute interval.
Line Code Violations	RFC1407 dsx3CurrentLCVs	Indicates the number of line coding violations encountered by a DS3 interface in the current fifteen-minute interval.
Path P-bit Coding Violations	RFC1407 dsx3CurrentPCVs	Indicates the number of P-bit coding violations encountered by a DS3 interface in the current fifteen-minute interval.
Line Errored Seconds	RFC1407 dsx3CurrentLESs	Indicates the number of line errored seconds encountered by a DS3 interface in the current fifteen-minute interval.
Unavailable Seconds	RFC1407 dsx3CurrentUASs	Indicates the number of unavailable seconds encountered by a DS3 interface in the current fifteen-minute interval.

Performance Attributes that You Cannot View

The following attributes cannot be viewed by Performance Manager; the attributes are uncharted data. Export the data to flat files.

Table8-7 Performance Attributes in the Others Tab

Text Field	MIB Attribute Name	Description
Queue Number within the Queue Set	CISCO-QUEUE-MIB cQStatsQNumber	• In FIFO queuing, this value is always 2. • In priority queuing, this value indicates priority: – High=0 – Medium=1 – Normal=2 – Low=3 • In custom queuing, this value is the queue number referenced in the access list. • In weighted fair queuing, this value is the queue number associated with the traffic stream identified.
Number of Messages in the Sub-Queue	CISCO-QUEUE-MIB cQStatsDepth	Indicates the number of messages currently in the subqueue.
Max Number of Messages Permitted in the Sub-Queue	CISCO-QUEUE-MIB cQStatsMaxDepth	Indicates the number of messages permitted in the subqueue.
Number of Messages Discarded from the Queue	CISCO-QUEUE-MIB cQStatsDiscards	Indicates the number of messages discarded from this queue since the restart of performance polling.
ciscoEnvMonSupplyStatusDescr	CISCO-ENVMON-MIB ciscoEnvMonSupplyStatusDescr	Describes the power supply being monitored.

Table8-7 Performance Attributes in the Others Tab (continued)

Memory Pool Name	CISCO-MEMORY-POOL-MIB	Identifies the memory pool.
Memory Pool Free	CISCO-MEMORY-POOL-MIB ciscoMemoryPoolFree	Indicates the number of bytes from the memory pool that are currently unused on the managed device.
Memory Pool Used	CISCO-MEMORY-POOL-MIB ciscoMemoryPoolUsed	Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.
ciscoPingSentPackets	CISCO-PING-MIB ciscoPingSentPackets	Indicates the number of ping packets sent to the target.
ciscoPingReceivedPackets	CISCO-PING-MIB ciscoPingReceivedPackets	Indicates the number of ping packets received from the target.
ciscoPingMinRtt	CISCO-PING-MIB ciscoPingMinRtt	Indicates the minimum round-trip time taken by the packets in this sequence.
ciscoPingAvgRtt	CISCO-PING-MIB ciscoPingAvgRtt	Indicates the average round-trip time taken by the packets in this sequence.
ciscoPingMaxRtt	CISCO-PING-MIB ciscoPingMaxRtt	Indicates the maximum round-trip time taken by the packets in this sequence.
ciscoPingCompleted	CISCO-PING-MIB ciscoPingCompleted	Indicates when all the packets in this sequence have been responded to or have been timed out.

Viewing Performance Data

User-specified polling intervals may sometimes be delayed due to other system processes. If you want to view new attributes or the latest polled data:

- Click **Now**—The latest polled data appears.
- Click **Refresh**—New attribute data or changes to the format appear.

Step 1 To view Performance Manager data, locate and right-click the object whose performance data you want to view, and choose **Tools>PerformanceManager**.

Step 2 In the left-side list box, click the performance data you want to view.

See the “” section on page8-6.

Step 3 (Optional) Modify the Time Period box settings. These settings tell the Performance Manager to display data collected from a starting to ending time and date.

Step 4 Click the **Line Chart** or **Table Display** tab to view your data in the appropriate form.

Step 5 (Optional) If you selected Line Chart, select **Values** or **Points** if required.

See the “Line Charts and Tables” section on page8-6.

Overview of the Performance Data Export File

With Cisco UGM, you can export inventory, performance, and alarm data to ASCII files and send them to an external system by using File Transfer Protocol (FTP).

The interval at which performance data is exported to flat files is tied to the interval at which performance polling takes place. Changing the performance polling interval also changes the data export interval.

For details on changing the performance polling interval, see the “Selecting Performance Polling Intervals” section on page8-4.

Cisco UGM creates a performance data file for each polling interval that you select. You can create six performance data files at any time:

- fiveMin.export
- fifteenMin.export
- thirtyMin.export

- sixtyMin.export
- oneDay.export
- sevenDay.export

Each data file contains performance data for all attributes sampled at that polling interval.

For example, if Line Code Violations and Out NUcast Pkts are sampled every five minutes, the polled data for these attributes is in the fiveMin.export file. However, if the same attributes are polled once a day, the polled data is now in the oneDay.export file.

You can create performance data export files at the device level to include all subcomponent data, or at the port level, consisting of data from a single attribute.

Location of the Performance Data Export Files

All performance data files are saved in the *CEMF_BaseDir* directory on the server.

For a description of performance data files, see the "Overview of the Performance Data Export File" section on page8-16.

The directory path and filename for each device's performance data file is:

CEMF_BaseDir/Physical:_SiteName_AS5xxxDeviceName.PollingInterval.EXPORT

where:

- *CEMF_BaseDir*—Is the base directory input from the Performance tab of the File Export Properties dialog box. (See the "Exporting a File" section on page8-18.)

  You specify this segment of the path.
- *SiteName*—Is the name of the site object under which the performance polled managed device is located. This is automatically generated by Cisco UGM.
- *AS5xxxDeviceName*—Is the hostname or IP Address of the performance polled managed device. This is automatically generated by Cisco UGM.

Example of Performance Data File Location

If the 172.24.217.25 device is located under Physical > Site-1, and /tmp/Oct-3-test is the input directory for file export, this export file under the /tmp/Oct-3-test directory:

```
Physical:_Site-1_172.24.217.25.fifteenMin.EXPORT
```

Exporting a File

Step 1 In the Physical view, select and right-click the object for which you want to export performance data.

Step 2 Choose **ASEMSConfig > File Export > Open File Export Properties > Performance**.

Step 3 In the Export Type field, select **Continuous**.

Step 4 Enter a storage path for the file.

See the "Location of the Performance Data Export Files" section on page8-17.

Step 5 Select an action to be performed when file aging occurs:

- **none**—Disables aging; File Age and Aging Directory fields are ignored.
- **delete**—Deletes the aged file from the disk.
- **move**—Moves the aged file into the aging directory.
- **moveTarCompress**—Compresses the aged file; then adds it to the FileExport.tar file which, if it does not already exist, is created in the Aging Directory.

Step 6 Specify the maximum size (in KBytes) of a file before the selected aging action is performed. Export then continues in the newly created file.

Step 7 Specify where the file should be moved to (or moveTarCompressed to) when aging occurs.

- If you enter a non-existent directory path, it is automatically created.
- This field does not apply to the delete aging action.
- The directory string that you enter must end with a trailing / (forward slash).
- If the Action field is set to moveTarCompress, FileExport.tar is created in the Aging Directory to contain aged files.

Step 8 Click **Save**. An Action Report is generated.

See the “About Action Reports” section on page8-20.

Example: Performance Export Data Format

Performance export data for scalar attributes is formatted as follows:

<DATA-TIME>|<ATTRIBUTE NAME> <Value>

```
2000/09/08-10:43:51 EDT|CISCO-MODEM-MGMT-MIB.cmSystemModemsDead 0
2000/09/08-10:43:51 EDT|CISCO-MODEM-MGMT-MIB.cmSystemModemsOffline 0
2000/09/08-10:43:51 EDT|CISCO-MODEM-MGMT-MIB.cmSystemModemsUnavailable
0
2000/09/08-10:43:51 EDT|CISCO-MODEM-MGMT-MIB.cmSystemModemsAvailable
60
2000/09/08-10:43:51 EDT|CISCO-MODEM-MGMT-MIB.cmSystemModemsInUse 0
.
.
.
Performance export data for table attributes is formatted as follows:
<DATA-TIME>|<TABLE NAME>|<Column-1 Name>|...|<Column-n Name>|<Value of
Column-1>|...|<Value of Column-n>
2000/09/08-10:43:52
EDT|ASMainEMPerfPollmodule.aSGenericNetworkIfIfPartialTable|IF-MIB.ifI
ndex|IF-MIB.ifInErrors|IF-MIB.ifOutErrors|IF-MIB.ifInUcastPkts|IF-MIB.
ifOutUcastPkts|IF-MIB.ifInDiscards|IF-MIB.ifOutDiscards|IF-MIB.ifInNUc
astPkts|IF-MIB.ifOutNUcastPkts|IF-MIB.ifInOctets|IF-MIB.ifOutOctets|IF
-MIB.ifInUnknownProtos
********|1|0|0|0|0|0|0|0|0|0|0|0
********|2|0|0|0|0|0|0|0|0|0|0|0
********|3|0|0|0|0|0|0|0|0|0|0|0
********|4|0|0|0|0|0|0|0|0|0|0|0
********|5|0|0|0|0|0|0|0|0|0|0|0
********|6|0|0|0|0|0|0|0|0|0|0|0
********|7|0|0|0|0|0|0|0|0|0|0|0
********|8|0|0|0|0|0|0|0|0|0|0|0
********|9|0|0|0|0|0|0|0|0|0|0|0
********|10|0|0|0|0|0|0|0|0|0|0|0|0
********|11|0|0|0|0|0|0|0|0|0|0|0|0
********|12|0|0|0|0|0|0|0|0|0|0|0|0
********|13|0|0|0|0|0|0|0|0|0|0|0|0
********|14|0|0|0|0|0|0|0|0|0|0|0|0
.
.
.
```

About Action Reports

File Export Properties dialog fields are updated when you click on Save; only the last update for a field is visible in the dialog. However, all display field updates are written to the Action Report.

The Action Report appears either because the action was processed or was interrupted.

The maximum number of characters in the report is limited to approximately 500,000.

A timestamped termination message is always written to the report, even if the report is "full."

Managing Faults with Cisco UGM

This chapter contains the following sections:

Overview of Fault Management

With the Event Browser in Cisco UGM, you can identify alarm events and take appropriate action to resolve them quickly and efficiently; in addition, you can forward user-specified SNMP traps to any configured remote host, and continuously export all alarm events, as they are raised, to a user-specified text file.

With Cisco UGM, you can decommission and commission chassis and card objects for maintenance.

Monitored Events

All faults detected by Cisco UGM are referred to as alarm events. Faults are generated from these sources:

- Incoming (supported) SNMP traps from managed devices.
- Internal traps generated by Cisco UGM itself.

You can use the Event Browser to view alarm events raised against an object; various filtering criteria are provided by the Query Editor.

Note Only SNMP traps from managed devices are reported by Cisco UGM; traps from any other unsupported device are discarded. Moreover, the set of supported traps is predefined and nonconfigurable, and any unsupported trap is discarded.

.

Table9-1 Traps from Managed Devices

Fault	Attribute	MIB	Source
Link Down or Link Up trap from any DS1, DS3, or Ethernet interface. Raises major and normal alarms respectively.	IfTable: IfIndex, ifType, ifAdminStatus, ifOperStatus	IF-MIB	SNMP trap; Link Down trap is cleared by one or more Link Up traps for the same interface.
Cold Start trap from the device. Raises warning alarm.	ColdStart trap	SNMPv2-MIB	SNMP trap.
Warm Start trap from the device. Raises warning alarm.	WarmStart trap	SNMPv2-MIB	SNMP trap.
Authentication Failure trap from the device. Raises major alarm.	AuthenticationFailure trap	SNMPv2-MIB	SNMP trap.
Card OIR trap from the device. Raises warning alarm and performs discovery on the affected device.	cefcFRUInserted trap cefcFRURemoved trap	CISCO-ENTITY-FRU-CONTROL-MIB	SNMP trap.
Card inserted or removed in the device. Raises normal alarms.	alarmDirectory: entPhysicalContainedIn trap	ENTITY-MIB	Internal.

Table9-1 Traps from Managed Devices (continued)

Fault	Attribute	MIB	Source
Environment Monitoring Traps from the device. Raises critical alarm for the shutdown trap, and major alarm for all the other traps.	EnvMonShutdownNotification trap EnvMonVoltageNotification trap EnvMonTemperatureNotification trap EnvMonFanNotification trap EnvMonRedundantSupplyNotification trap	CISCO-ENVMON-MIB	SNMP trap.
Loss or re-establishment of communication with device[1]. Raises major and normal alarms respectively.	Not applicable		Internal. Communication lost alarm cleared by the communication established alarm.
Device or card commissioned or decommissioned[2]. Raises informational alarm in both cases.	Not applicable		Internal.
Server disk usage above the major threshold. Raises major alarm.	Not applicable		Internal. Cleared when disk usage is below the major threshold.
Server disk usage above the critical threshold. Raises critical alarm.	Not applicable		Internal. Cleared when disk usage is below the critical threshold.

Table 9-1 Traps from Managed Devices (continued)

Fault	Attribute	MIB	Source
Graceful Shutdown operation was interrupted. Raises major alarm.	Not applicable		Internal.
Accept Traffic operation was interrupted. Raises major alarm.	Not applicable		Internal.

1. See the "Overview of Presence Polling and Loss of Communication with a Device" section on page 9-5.
2. See the "Overview of the Commission/Decommission Function for a Chassis" section on page 9-19.

Overview of Presence Polling and Loss of Communication with a Device

You can detect communication loss with a managed device by using presence polling. Loss of communication can occur for various reasons:

- Network delays.
- Problem with the communication link between EMS and the device, but the device may still be operating properly.
- The device is overloaded, resulting in slow or no response.
- The device has a problem and is unable to respond to presence polling.

Presence Polling Retries

When Cisco UGM first detects loss of communication to a managed device, it does not immediately transition the device to the errored state but retries presence polling. Select the number of retries as described in the "Setting Number of Retries Before Loss of Communication" section on page 9-7.

Presence Polling Intervals

Presence polling uses an interval specified in the "Setting Presence Polling Intervals for Devices in Normal and Errored States" section on page 9-6. If all the communication attempts prove unsuccessful, the device transitions to the errored state. An internal alarm event (communicationLost) with a Major severity level is raised against the affected device.

The default presence polling intervals are:

- 900 seconds during the normal state
- 915 seconds during the errored state

Duration of Communication Loss

When communication is re-established, the device returns to a normal state, and an internal alarm event (communicationEstablished) with a Normal severity level is raised against the affected device.

If communication is restored after the duration specified in the "Setting Loss of Communication Duration" section on page 9-8, Cisco UGM discovers the device's subcomponents to detect any card inventory changes that may have occurred during the loss of communication.

If communication is restored within the specified duration, Cisco UGM transitions the device to the normal state.

Setting Presence Polling Intervals for Devices in Normal and Errored States

Step 1 In Map View, choose **ASEMSConfig > EMS > Settings**.

Step 2 Enter the interval at which a device should be polled in the normal state.

The interval should be an integer value that is 300 or larger (representing seconds). The default is 900 seconds.

Note This value depends on the total number of managed devices in your network. You may need to change this value a few times in order to determine the optimum setting for your network.

Step 3 Enter the interval at which a device should be polled in the errored state.

The interval should be an integer value that is 300 or larger (representing seconds). The default is 915 seconds.

Note This value depends on the total number of managed devices in your network.

Do not enter the same value as for devices in the normal state. A different value avoids overlapping polling intervals for normal and errored states.

Step 4 Click **Apply**.

Setting Number of Retries Before Loss of Communication

When Cisco UGM first detects loss of communication to a managed device, it does not immediately transition the device to the errored state, but retries presence polling by using the polling interval specified in the "Setting Presence Polling Intervals for Devices in Normal and Errored States" section on page9-6 . If these communication attempts are unsuccessful, the device transitions to the errored state.

Step 1 In Map View, select **ASEMSConfig > EMS > Settings.**

Step 2 Enter the number of times Cisco UGM tries to re-establish connectivity before transitioning the device into the errored state.

The number entered should be an integer value that is 0 or larger. A value of 0 disables retries; the default is 1.

Note A large value causes a delay before loss of communication with a device is detected.

Step 3 Click **Apply**.

Setting Loss of Communication Duration

Step 1 In Map View, choose **ASEMSConfig > EMS > Settings.**

Step 2 Enter a time interval for which communication must be lost in order to start discovery.

The interval should be an integer value that is 15 or larger (representing minutes). The default is 15 minutes.

Note A large value results in card inventory changes that are not detected.

If communication is restored after this interval, Cisco UGM initiates discovery of the device's subcomponents to detect any card inventory changes that may have occurred during the loss of communication.

If communication is restored within this interval, Cisco UGM transitions the device to the normal state.

Step 3 Click **Apply**.

Overview of the Event Browser

You can start the Event Browser from the Launchpad or from the pop-up menu for the individual object within Map Viewer.

With the Event Browser, you can perform these tasks:

- Query (filter) events
- Sort events
- Acknowledge events
- Clear events
- Start services on events

You can see all events—regardless of your access privilege. In the Event Browser window, you can check the Ack (acknowledge) box next to an event to communicate to other users that you are planning to deal with that particular event. When you resolve the event, click the Clear box so that other users are informed of this.

Note Only the most severe alarm event against an object appears next to its icon within Map Viewer.

You can view additional alarm details by using the Event browser. For more information, refer to the *Cisco Element Management Framework User's Guide*.

Using the Event Browser

Step 1 In the Map Viewer, note the color coding of status dots to represent the occurrence of alarm events against the objects.

See the "Overview of Alarm Events" section on page9-10 for an explanation of the colors.

Step 2 Right-click the object whose list of alarm events you want to view and choose **Tools>OpenEventBrowser**.

Using the Query Editor

If you do not want to view all events in the system, set up a query by using the Query Editor to view only specific events.

The criteria that you use to specify a query are on individual tabs. The Event Browser is updated with only those events that match the query criteria. A progress bar indicates that Cisco UGM is querying events and the window is being updated.

Caution Any changes that you make to a query are not stored when you exit the Event Browser.

If you have specified different queries, you can open more than one Event Browser session at a time.

For details about the Query Editor refer to the *Cisco Element Manager Framework User's Guide*.

To access the Query Editor from the Event Browser, choose **Edit > Query Setup**.

Overview of Alarm Events

In the Map Viewer tree, you can see raised alarm events by the presence of colored dots next to tree objects in the left pane and by colored annotations against the object icons in the right pane.

The dots are color coded to reflect the following severity levels (highest to lowest): critical, major, minor, informational, and normal.

The defined color coding is:

- Red = Critical
- Orange = Major
- Yellow = Minor
- Cyan = Warning

- White = Informational
- Green = Normal (no events)

A device or card object can be in either commissioned or decommissioned state within Cisco UGM.

If an object is in a commissioned state, alarm events against that object are propagated to the physical tree in the Map Viewer and appear in the parent objects to the region level.

For decommissioned objects, alarm events are not propagated up to the physical tree in the Map Viewer.

For details on commissioning and decommissioning objects, see the "Overview of the Commission/Decommission Function for a Chassis" section on page 9-19.

The following table describes Cisco UGM alarm events, their severity, explanation, and recovery procedures.

Table 9-2 Cisco UGM Alarm Events

Alarm Event	Alarm Severity	Explanation
ciscoColdStart	Warning	You started the device object from a power-off state. **Note** Clear this event manually.
ciscoWarmStart	Warning	You restarted the device object from an on state. **Note** Clear this event manually.
ciscoLinkDown	Major	A DS1 or Ethernet interface is down.
ciscoLinkUp	Normal	A DS1 or Ethernet interface is up.
ciscoAuthenticationFailure	Major	The device received an SNMP message that was improperly authenticated.
cardInserted	Warning	You inserted a new card in the device; Cisco UGM initiates discovery on the device.

Table9-2 Cisco UGM Alarm Events (continued)

Alarm Event	Alarm Severity	Explanation
cardRemoved	Warning	You removed a card from the device; Cisco UGM initiates discovery on the device.
Card inserted in slot	Informational	You inserted a new card in the device; Cisco UGM completes discovery on the device.
Card removed in slot	Informational	You removed a card from the device; Cisco UGM completes discovery on the device.
envMonShutdown	Critical	A critical environmental condition is detected and a device shutdown is imminent.
envMonVoltage	Major	A voltage threshold was exceeded on the device.
envMonTemperature	Major	A temperature threshold was exceeded on the device.
envMonFan	Major	The fan on the device has failed.
envMonRedundantSupply	Major	The power supply on the device has failed.
communicationLost	Major	Cisco UGM lost SNMP connectivity with the device.
communicationEstablished	Normal	Cisco UGM established SNMP connectivity with the device.
entityDecommisioned	Informational	Device or card object has been decommissioned.
entityCommissioned	Informational	Device or card object has been commissioned.
fileSysAboveMajor	Major	Server disk usage is over the user-defined major threshold[1].
fileSysAboveCritical	Critical	Server disk usage is over the user-defined critical threshold[2].

Table9-2 Cisco UGM Alarm Events (continued)

Alarm Event	Alarm Severity	Explanation
fileSysBelowMajor	Normal	Server disk usage is below the user-defined major threshold.
fileSysBelowCritical	Normal	Server disk usage is below the user-defined critical threshold.
gracefulShutdownInterrupted	Major	During a Graceful Shutdown operation, loss of communication with the device occurred or it was decommissioned. **Note** Clear this event manually.
acceptTrafficInterrupted	Major	During an Accept Traffic operation, loss of communication with the device occurred or it was decommissioned. **Note** Clear this event manually.

1. For details on changing this threshold, see the "Example: Sample Configuration File for Fault Management" section on page9-24.
2. For details on changing this threshold, see the "Example: Sample Configuration File for Fault Management" section on page9-24.

Clearing Alarm Events

If you manually clear an alarm event for an object in the Event Browser, that object appears in the Map Viewer with an alarm notification reflecting the next highest alarm present for that object. This change in alarm severity appears in the Map Viewer, even if the fault condition has not actually been corrected.

Cisco UGM does not generate all alarm events again, even if the alarm conditions are still present; therefore, be cautious in clearing alarm events.

Step 1 In the Map Viewer, note the color coding of status dots to represent the occurrence of alarm events against the objects.

See the "Overview of Alarm Events" section on page9-10.

Step 2 Right-click the object whose list of alarm events you want to view and choose **Tools>OpenEventBrowser**.

You can acknowledge and clear individual alarm events by clicking the appropriate box next to each event.

Overview of Trap Forwarding

- Cisco UGM monitors UDP port 162 for all SNMPv1 and v2c traps sent from all managed devices configured to send traps to it, and then forwards them to the specified host destinations.
- Cisco UGM forwards SNMP v1 and v2 traps to multiple remote hosts, but SNMP v2 traps are forwarded as SNMP v1 traps.
- For each remote host, configure a list of trap specifiers that identify specific SNMP traps (consisting of Enterprise ID, Generic ID, and Specific ID).
- Cisco UGM maintains a list of host destinations that you define. Also define specific SNMP traps for each host destination.
- Enter a wildcard (*****) for any field of a trap specifier.
- Add new remote hosts or new trap specifiers by using the Trap Forwarding Deployment Wizard.
- Update existing remote hosts or trap specifier fields by using the Trap Forwarding Properties Dialog.
- Delete existing remote hosts or trap specifiers from the Map Viewer.
- Click Accept Saved Setting (in the Trap Forwarding Properties Dialog box) for trap forwarding changes to take effect.

Specifying New Trap Forwarding Hosts

By using the Trap Forwarding Deployment Wizard, you can:

- Specify host destinations and traps to be forwarded.
- Deploy host destinations and traps.

Note The default is no trap forwarding.

Step 1 Choose **ASEMSConfig > TrapForwarding > Deploy Trap Forwarding Hosts**.

Step 2 Follow the instructions provided by the Deployment wizard.

Step 3 In the Map viewer window, choose **ASEMSConfig > Trap Forwarding > Trap Forwarding Properties**.

Step 4 To enable trap forwarding, click **Accept Saved Setting**.

Specifying New Trap Specifiers for a Trap Forwarding Host

Step 1 From the Map Viewer, open **ASEMSConfig**.

Step 2 Expand the Trap Forwarding tree by clicking on the + (plus) sign.

Step 3 Open the Trap Specifiers Deployment Wizard.

Step 4 Right-click the host destination for which you wish to add a new trap specifier and select **Deploy Trap Specifiers**.

Step 5 Follow the instructions provided by the Deployment wizard.

Step 6 In the Map Viewer, choose **ASEMSConfig > Trap Forwarding > Trap Forwarding Properties**.

Step 7 To update trap forwarding, click **Accept Saved Setting**.

The trap forwarding action triggered reflects any changes made (and saved) i n this dialog box. Any previously specified trap forwarding action is replaced.

Changing Previously Specified Trap Forwarding Data

Step 1 In the Map Viewer, choose **ASEMSConfig > Trap Forwarding > Trap Forwarding Properties**.

Step 2 Enter your changes.

Step 3 Click the Save icon from the dialog toolbar, or choose **File > Save**.

Step 4 To update trap forwarding, click **Accept Saved Setting**.

The trap forwarding action triggered reflects any changes made (and saved) in this dialog. Any previously specified trap forwarding action is replaced.

Removing Previously Specified Trap Forwarding Data

Step 1 From the Map Viewer, open **ASEMSConfig**.

Step 2 Expand the Trap Forwarding tree by clicking the + (plus) sign.

Step 3 Expand any listed host destination by clicking the + (plus) sign.

Step 4 Right-click the object to be deleted (a host destination, or a specific trap specifier for a given host destination) and choose **Deployment > Delete Objects**.

Step 5 In the Map Viewer, choose **ASEMSConfig > Trap Forwarding > Trap Forwarding Properties**.

Step 6 To update trap forwarding, click **Accept Saved Setting**.

The trap forwarding action triggered reflects any changes made (and saved) i n this dialog. Any previously specified trap forwarding action is replaced.

Tips To deactivate or disable all trap forwarding, you must delete all host destinations and click **Accept Saved Setting**.

To resume trap forwarding, re-enter the host destinations.

See the “Specifying New Trap Forwarding Hosts” section on page9-14.

Example: Cisco UGM Trap Mapping Tables

Table9-3 Cisco AS5350 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Severity	Color
ciscoColdStart	1.3.6.1.4.1.9.1.313	0	0	warning	Cyan
ciscoWarmStart	1.3.6.1.4.1.9.1.313	1	0	warning	Cyan
ciscoLinkDown	1.3.6.1.4.1.9.1.313	2	0	major	Orange
ciscoLinkUp	1.3.6.1.4.1.9.1.313	3	0	normal	Green
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.313	4	0	major	Orange

Table9-4 Cisco AS5400 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Severity	Color
ciscoColdStart	1.3.6.1.4.1.9.1.274	0	0	warning	Cyan
ciscoWarmStart	1.3.6.1.4.1.9.1.274	1	0	warning	Cyan
ciscoLinkDown	1.3.6.1.4.1.9.1.274	2	0	major	Orange
ciscoLinkUp	1.3.6.1.4.1.9.1.274	3	0	normal	Green
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.274	4	0	major	Orange

Table9-5 Cisco AS5800 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Severity	Color
ciscoColdStart	1.3.6.1.4.1.9.1.188	0	0	warning	Cyan
ciscoWarmStart	1.3.6.1.4.1.9.1.188	1	0	warning	Cyan

Table9-5 Cisco AS5800 Trap Mapping (continued)

Class Mapping	Enterprise	Generic ID	Specific ID	Severity	Color
ciscoLinkDown	1.3.6.1.4.1.9.1.188	2	0	major	Orange
ciscoLinkUp	1.3.6.1.4.1.9.1.188	3	0	normal	Green
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.188	4	0	major	Orange

Table9-6 Cisco AS5850 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Severity	Color
ciscoColdStart	1.3.6.1.4.1.9.1.308	0	0	warning	Cyan
ciscoWarmStart	1.3.6.1.4.1.9.1.308	1	0	warning	Cyan
ciscoLinkDown	1.3.6.1.4.1.9.1.308	2	0	major	Orange
ciscoLinkUp	1.3.6.1.4.1.9.1.308	3	0	normal	Green
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.308	4	0	major	Orange

Overview of the Commission/Decommission Function for a Chassis

About Commissioning a Chassis

Commission a device to return it to a normal (commissioned) state within the EMS.

When you commission a device, Cisco UGM starts discovery on the device to resolve any card inventory changes that may have occurred while it was in the decommissioned state. When discovery is completed, the device returns to the normal or errored state depending on whether commissioning was successful.

Note When a device is commissioned, all its subcomponents (cards and ports) also transition into the commissioned state.

About Decommissioning a Chassis

With Cisco UGM, you can decommission a device from any state. You can decommission a device due to one of these causes:

- The device was manually deployed.
- You decommissioned the device to suspend reporting alarm events when the device was rebooted or undergoing maintenance.

When you decommission a device, no actual changes are made to the device, which still sends traps to Cisco UGM. However, the resulting alarm events are not reported and do not initiate any actions or status changes. Presence and performance polling are also suspended, and Cisco UGM does not allow any configuration changes or software and firmware image downloads for the device.

Note When a chassis is decommissioned, all its subcomponents (cards and ports) also transition into the decommissioned state.

Overview of the Commission/Decommission Function for a Card

About Commissioning a Card

Commission a card to return it to a normal (commissioned) state within the system.

When you commission a card, Cisco UGM reconciles its status with that of the actual card on the device. When this is completed, the card returns to either the normal or errored state. If the card was removed from the device, the corresponding card object is deleted.

Note When a parent device is commissioned, all its subcomponents (cards and ports) also transition into the commissioned state. Likewise, when a card is commissioned, all its ports are also commissioned.

About Decommissioning a Card

You can decommission a card from any state due to one of these causes:

- The parent device containing the card was decommissioned.
- You decommissioned the card to suspend reporting alarm events when the card was rebooted or undergoing maintenance.

When you decommission a card, no actual changes are made to the card, which still sends traps to Cisco UGM. However, the resulting alarm events are not reported and do not initiate any actions or status changes.

When a parent device is decommissioned, all its subcomponents (cards and ports) also transition into the decommissioned state. Likewise, when a card is decommissioned, all its ports are also decommissioned.

Commissioning and Decommissioning a Device or Card

Step 1 Right-click the device or card object that you want to commission or decommission.

Step 2 Choose **AS5***xxx* **object> Chassis > Chassis Commissioning.**

or

Choose **Card object > Card Commissioning.**

Step 3 Click **Commission** or **Decommission**.

Tips Decommissioned devices appear as shaded icons in the right-hand pane of the MapViewer.

Overview of Exporting Alarm Events

With Cisco UGM, you can capture and export all alarm data to an ASCII text file; this file can then be examined locally by an external system or retrieved by an external system by using File Transfer Protocol (FTP). The external system is responsible for parsing the contents of this file.

Exporting SNMP traps consists of capturing traps from managed devices and writing them to a text file.

Note You cannot forward internally generated Cisco UGM alarm events cannot be forwarded through SNMP; you can export these alarm events by writing them to the ASCII text file.

You can access the Alarm File Export function to schedule alarm data export, specify where the exported data is to be stored, how and when the file ages, and also specify a string to delimit exported data.

Exporting Alarm Events to a File

Step 1 From the Map viewer choose **ASEMSConfig > File Export > Open File Export Properties > Alarm**.

Step 2 In the Export Type field, select **Continuous**.

Step 3 Enter a storage path for the file.

Step 4 Select an action to be performed when file aging occurs:

- **none**—Disables aging; File Age and Aging Directory fields are ignored.
- **delete**—Deletes the aged file from the disk.
- **move**—Moves the aged file into aging directory.
- **moveTarCompress**—Compresses the aged file, and then adds it to the FileExport.tar file which, if it does not already exist, is created in the Aging Directory.

Step 5 Specify the maximum size (in KBytes) of a file before the selected aging action begins. Export then continues to the newly created file.

Step 6 Specify where the file is moved to (or moveTarCompressed to) when aging occurs.

- If you enter a non-existent directory path, it is automatically created.
- This field does not apply to the delete aging action.
- The directory string that you enter must end with a trailing / (forward slash).
- If the Action field is set to moveTarCompress, a tar file named FileExport.tar is created in the Aging Directory for the aged files.

Step 7 Click **Save**:

- Saves user-specified data from this dialog.
- Changes are validated and applied to the system (if valid).
- Generates an Action Report containing results of this action.

Example: Alarm Data Export Format and Sample

Alarm export data is formatted as follows:

```
<Date>|<Time>|<DataType>|<AlarmName>|<AlarmSeverity>|<AffectedObject>|
```

Sample:

```
2000/09/08|08:32:59
EDT|InternalAlarm|communicationEstablished|normal|Physical:/Kanata/AS5
350-1|
2000/09/08|08:33:05
EDT|InternalAlarm|communicationEstablished|normal|Physical:/Kanata/AS5
400-1|
2000/09/08|08:33:06
EDT|InternalAlarm|communicationEstablished|normal|Physical:/Kanata/AS5
800-1|
2000/09/08|08:37:53 EDT|InternalAlarm|fileSysBelowMajor|normal|:/|
2000/09/08|08:37:53 EDT|InternalAlarm|fileSysBelowCritical|normal|:/|
2000/09/08|10:17:45
EDT|SNMPv1|envMonRedundantSupply|major|Physical:/Kanata/AS5800-1|
2000/09/08|10:18:41
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/08|10:18:41
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/10|14:36:45
EDT|SNMPv1|cardInserted|warning|Physical:/Kanata/AS5350-1|
2000/09/10|14:37:06
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5350-1|
2000/09/10|14:57:28
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5350-1|
2000/09/11|17:58:32
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/11|17:58:35
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/11|18:10:18
EDT|SNMPv1|ciscoLinkDown|major|Physical:/Kanata/AS5800-1|
2000/09/11|18:11:20
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/11|18:15:07
EDT|InternalAlarm|entityCommissioned|informational|Physical:/Kanata/AS
5400-1|
2000/09/11|18:23:19
EDT|SNMPv1|envMonRedundantSupply|major|Physical:/Kanata/AS5800-1|
2000/09/11|18:23:59
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/11|18:24:00
EDT|SNMPv1|ciscoLinkUp|normal|Physical:/Kanata/AS5800-1|
2000/09/12|10:20:23
EDT|SNMPv1|ciscoLinkDown|major|Physical:/Kanata/AS5800-1|
```

Example: Sample Configuration File for Fault Management

You can view and edit some Cisco UGM attributes by changing a configuration file in ASCII format; the file is located at:

<CEMFROOT>/config/ASMainCtrl/ASMainCtrlUserData.ini

Sample of the ASMainCtrlUserData.ini file showing items relevant to fault management in Cisco UGM:

```
====================================================
; Configurable controller settings.
; ====================================================

; This section defines settings for file-system monitoring:
; * MajorThreshold    : If file-system usage exceeds this percentage,
;                  major alarm is raised.
; * CriticalThreshold : If file-system usage exceeds this percentage,
:                  critical alarm is raised.
; * MonitoringInterval: How often each file-system is checked in
:                       minutes. If the value is 0, self-monitoring
;                  is disabled for all file-systems.
;
; - Threshold percentages must be integer values > 0 and < 100.
; - MonitoringInterval must be integer value >= 0.
;
[SelfMonitor]
MajorThreshold = 90
CriticalThreshold = 95
MonitoringInterval = 10
```

Troubleshooting Cisco UGM

To verify Cisco UGM system performance and reliability, follow the troubleshooting procedures described in this appendix:

Note See the Release Notes for additional tips and debugging information.

Freeing Up Disk Space

If available disk space on your server is low or unavailable, verify that only the export data that you want is stored. Predefined and customized export data is stored in the directory specified by you in the File Export Properties dialog box. The exported data can be:

- Inventory
- Alarm
- Performance
- Syslogs

To free up disk space, you can delete or archive these files to another location.

Backing Up Your Database

With Cisco EMF, you can back up and restore databases (which are typically located in <CEMFROOT>/.../AVBackup) by using the Cisco EMF script (cemf), typically located in /opt/cemf/bin.

Caution If Cisco UGM is reinstalled (after the Cisco UGM initial installation), any existing data is lost. Back up any existing data before reinstalling Cisco UGM.

Step 1 Start an X-session.

Step 2 Change to the following directory:

cd /opt/cemf/bin

Step 3 To run the backup script, enter:

./cemf backup

This command backs up the databases currently in <CEMFROOT>/.../AVBackup.

Restoring Your Database

With Cisco EMF, you can back up and restore databases (which are typically located in <CEMFROOT>/.../AVBackup) by using the Cisco EMF script (cemf), typically located in /opt/cemf/bin.

Caution Although Cisco EMF allows for selective restoration of its database, Cisco UGM doesn't support this feature. When restoring Cisco UGM data, you must restore all Cisco EMF databases.

Step 1 Start an X-session.

Step 2 Change to the following directory:

cd /opt/cemf/bin

Step 3 Enter the following command to stop Cisco EMF:

./cemf stop

Step 4 Enter the following command:

./cemf restore

Step 5 Enter the date that the backup was created:

mm-dd-yyyy

- *mm* is the month in which the back up was made.
- *dd* is the day on which the back up was made.
- *yyyy* is the year (containing the month and day) in which the backup was made.

Example: Restoring Your Database

If you backed up your database on 5/29/2000, the backup file directory and configuration are saved in a directory named 05/29/2000, which reflects the date when the backup was performed.

In order to restore the database as of 5/29/2000, enter this command:

```
./cemf restore -t 05-29-2000
```

Refer to the *Cisco Element Management Framework Installation Guide* for further details.

About Viewing Log Files

Cisco EMF stores system information in log files located in <CEMFROOT>/logs/ (typically /opt/cemf/logs/). The Cisco UGM application-specific log messages are located in the following (ASCII text) log files:

- sysmgr.log, sysmgr.old
- sysmgrClient.log, sysmgrClient.old
- ASMainCtrl.log, ASMainCtrl.old

  This log file contains ASMainCtrl controller information: This consists of all Cisco UGM areas not listed in IOSCtrl.log, IOSFmgrCtrl.log, and commonCtrl.log.
- IOSCtrl.log, IOSCtrl.old

  This log file contains IOSMgr controller information: IOS operations dialog and scheduled actions.
- IOSFmgrCtrl.log, IOSFmgrCtrl.old

  This log file contains IOSFmgr controller information: NAS File Repository and Associate File Repository Object with Device dialog boxes and operation.
- commonCtrl.log, commonCtrl.old

  This log file contains commonEM controller information: Telnet and Show Command, Device Readiness, Device Information, Log Configuration, Group Authentication, System Information dialog boxes.

The name of each .log file corresponds to the Cisco UGM process that generates the log file.

Each .old file is the backup file for the .log file. (For example, commonCtrl.old is the backup file for commonCtrl.log.

Viewing DEBUG Entries

By default, DEBUG entries are not included in log files. To see log messages of DEBUG severity (this includes all other severities), follow these steps:

Step 1 Locate the loggercommon.include file in the <CEMFROOT>/config/init/ directory.

Step 2 Change this setting to **15** (1111 binary).

By default the loggingLevelMask is set to 10 (1010 binary).

Note Changing the level to 15 affects how quickly the log files are archived as .old files. Any changes you make to the loggercommon.include file do not take effect until you restart Cisco UGM.

Changing the Log Level in ASMainCtrl and commonCtrl Log Files

For the ASMainCtrl and commonCtrl files, you can change the log level without starting and stopping Cisco EMF.

Choose **commonEM > ASMainCtrlLog > Log Level Configuration.**

Or
Choose **commonEM > commonCtrlLog > Log Level Configuration.**

Changing the Size of ASMainCtrl, IOSCtrl, IOSFmgrCtrl, or commonCtrl Log Files

Note Numerous other log files are also available for troubleshooting. They are stored in the <CEMFROOT>/logs/ directory.

Tips From time to time, run the listCores script in <CEMFROOT>/bin/ (typically /opt/cemf/bin). The report shows any core files affected by any malfunctioning processes. Whenever you see an affected core file, report it to Cisco customer support.

Step 1 Locate the corresponding .ini file in the <CEMFROOT>/config/init/ directory.

Step 2 In the logger section of the .ini file, enter the size (in KBytes):

```
[logger]
#include "loggercommon.include"
loggingName = xxxxCtrl
maxLogfileSize = 5000
```

(In this example, the user specified a 5 MB log file.)

Step 3 Stop and restart Cisco EMF.

When the .log file reaches the maximum size that you specified, it is archived to a corresponding .old file, and a new .log file is created.

Loading historyCriteria Files

If you reset and restart Cisco EMF, the historyCriteria files are not loaded automatically. If you do not see any monitored performance parameter in the Performance Manager, follow this procedure:

Step 1 On an X terminal, enter these commands:

/opt/cemf/bin/cemf shell

Step 2 Check the existing historyCriteria files in the system by entering:

/opt/cemf/bin/historyAdmin list

Step 3 If you do not find a historyCriteria file, enter these commands:

/opt/cemf/bin/historyAdmin add /opt/cemf/bin/historyCriteria

Configuration Errors

If any of the following actions fail:

- Associate File Repository Object with Device
- View Configuration File
- Build Config File from Default 5*xxx* Template

Check the message in the Action Report window.

ERROR: input file does not exist or is not a valid file

If the ERROR: input file does not exist or is not a valid file message appears when you re-associate file repository object with a new file, follow these steps:

Step 1 Enter the correct file path and name in the New File Path field.

Note You must specify a file that exists.

Step 2 Enter the correct file type.

Tips If you re-associate a configuration file object with a new file, make sure that the new file is an ASCII file; if you re-associate an image (IOS image, modem image, or SPE image) file object with a new file, make sure that the file is executable.

ERROR:Configuration file (or IOS/Modem/SPE Image file) not found. Association not present or file object was deleted

This error occurs when you try to download configuration or image files.

Step 1 Associate the configuration or image file object with the device object.

See the "Task 5: Option 1: Associating a Configuration File with a Device Object" section on page4-12.

Step 2 Check that the file object was not deleted.

Discovery and Deployment Errors

This section describes errors that may occur during the discovery and deployment of Cisco UGM managed devices.

Deployment Failed

If the "Deployment Failed" message appears when you are importing files or images, follow these steps:

Step 1 Enter the correct file path and name.

Note You must specify a file that exists.

Step 2 Enter the correct file type.

If you import a configuration file, make sure that the file is an ASCII file; if you import an image (IOS image, modem image, SPE image), make sure that the file is executable.

Step 3 Enter this UNIX file command to identify the type of file:

```
file <aConfigurationFile>
<aConfigurationFile>:ascii text
```

Locating Undiscovered Devices

If discovery displays an error icon for some devices in a specified discovery range:

Step 1 Check if IP routes have been defined for these devices.

Step 2 Check if the devices are receiving power and operational.

Step 3 Delete the errored devices and run discovery again.

Manual Deployment Failure

Step 1 Check that you specified the correct device.

Step 2 Check that the specified IP address and device name are unique to the Cisco UGM-managed network.

Troubleshooting Loss of Communication with a Device

Step 1 Check the Event Browser window for traps that may identify a problem with the device.

Step 2 Check if SNMP is still accessible by using a tool (such as SNMP Walk) to read SNMP tables.

Step 3 Ping the device.

Fault Management Errors

This section describes errors that may occur while managing faults generated by Cisco UGM managed devices.

Troubleshooting Missing Events from a Device

Step 1 Check that the required SNMP trap groups are enabled (through Cisco IOS) on the device.

Step 2 Verify that the IP address of the Cisco UGM server is properly configured (through Cisco IOS) as a trap recipient on the device.

Step 3 Verify that the device can reach the Cisco UGM server. (By using Cisco IOS, ping the Cisco UGM server from the device.)

Step 4 Verify that the Cisco UGM server is receiving SNMP traps sent from the device.

Step 5 Verify that SNMP traps from the device are reaching the main controller process (ASMainCtrl). You can do this by enabling the informational logging level, and scanning for “SNMP Trap” messages within this log file:

<CEMFROOT>/logs/ASMainCtrl.log

Troubleshooting Trap Forwarding

If a remote host that was configured as a destination for trap forwarding is not receiving SNMP traps:

Step 1 Verify that the remote host object and its associated list of trap specifier objects were properly created in the hierarchical object tree under the TrapForwarding object in ASEMSConfig view.

Step 2 Verify that the correct remote host destination (IP address or hostname) was configured in Cisco UGM.

Step 3 Verify that the Cisco UGM server can reach the remote host. (By using Cisco IOS, ping the remote host from the Cisco UGM server.)

Step 4 Verify that the correct trap specifier values (Enterprise ID, Generic ID, and Specific ID) are configured in Cisco UGM.

Step 5 Click Accept Saved Setting in the Trap Forwarding Properties dialog box.

Performance Polling Errors

This section describes errors that may occur while obtaining performance data from Cisco UGM managed devices.

Missed Poll

If you receive frequent Missed Poll messages in the Cisco EMF Performance Manager while charting performance parameters for a managed device, the performance polling load exceeds the capacity of Cisco EMF to complete the specified polling operations.

Select one of these options:

- Select a longer polling period for the same performance parameters.

  See the “Changing Polling Period Intervals” section on page A-12.

- Stop performance polling on some managed devices.

  See the “Stopping Performance Polling on Devices” section on page A-13.

Changing Polling Period Intervals

If you observe that Cisco UGM takes longer to poll than the polling period that you selected in the Cisco EMF Performance Manager, select a longer polling period for the same performance parameters.

Change the polling period by following this procedure:

Step 1 In the Map View, choose **ASEMSConfig > PerfPollConfig > Open Global Performance Polling Configuration**.

Step 2 Click the appropriate tabs for the performance parameters that you need to change.

Step 3 In the drop-down menu, select a longer polling interval.

Step 4 Click **Save** in the menu bar.

Stopping Performance Polling on Devices

Step 1 In the Map View, right-click a site (or other container) icon.

Step 2 Choose **ASMainEM > Start/Stop Performance Polling**.

Step 3 Select one or more devices.

Step 4 Select **PerformancePolling - OFF**.

Step 5 Click the **Save** button.

Configuring Administrative State Errors

This section describes errors that may occur while configuring the administrative state of Cisco UGM managed devices.

Correcting Ping Failure

The Action Report indicates a ping failure which indicates that a telnet connection cannot be established to the device where the card is installed. This is likely due to ping failure during session setup, or bad device configuration.

To resolve ping failure, complete these steps:

Step 1 Retry the Configure Administrative State action twice.

See Chapter 6, "Configuring the Administrative State of Objects."

Step 2 Open a telnet session to the device to verify that the passwords are correct and the device is reachable.

Step 3 Retry the Configure Administrative State action twice.

If the ping failure persists, the device configuration (particularly the passwords) specified for Cisco UGM may not match the passwords known to the device.

Step 4 Enter passwords for Cisco UGM:

a. In the Physical view, right-click the chassis object.

b. Select **Open Device Readiness Configuration** dialog box.

c. Select **Group** (if authenticating with TACACS), or select **Local**.

d. Enter the passwords.

Unexpected Dialog Box Updates

Dialog box display fields are updated, even though you do not click an Action button.

This occurs because you started an action for a card, closed the dialog box, and then reopened the dialog box for the same card.

Even if the dialog box is closed, the action continues until the number of active DS0s drop to 0 and the card shuts down.

There is no resolution for this occurrence.

Note Once the dialog box is closed, there is no indication that the action is still in progress. The only ways to determine this is to reopen the dialog box for that object, or start another Configure Administrative State action.

Tips Action Reports are not generated for closed dialog boxes (even if you reopen them).

Graceful Shutdown Interrupted and Accept Traffic Interrupted

These messages appear in the Event Browser and are generated under the following circumstances:

- During Cisco UGM startup (if any Configure Administrative Actions were in progress when Cisco UGM last shut down).
- An error occurred during Configure Administrative State action processing.
- Configure Administrative State ended prematurely due to the state change which occurred because of:
  - A loss of communication with the device
  - A Decommission action for the card or device object

Online Insertion or Removal (OIR) is described in the "Graceful Shutdown Alarm" section on pageA-16.

The alarm indicates that the card is in an indeterminate state. (For example: a busyout command may have been issued for the card but without the required subsequent shutdown command).

Step 1 Retry the action. (Click either **Graceful Shutdown** or **Accept Traffic**).

Step 2 Manually clear the alarm when the action succeeds.

False Completion

The Progress Information field indicates that an action was completed before you clicked the button.

Any information that you see in the display fields may have been generated by another (possibly previous, possibly currently running) Configure Administrative State action.

The timestamp in the Progress Information field tells you when an action ended. The field is updated if an action is currently running.

There is no resolution for this occurrence.

Graceful Shutdown Alarm

Indicates that a graceful shutdown is in progress; the number of active DS0s reaches 0, an alarm event is raised, and a graceful shutdown occurs.

Reasons for this alarm are:

- Card online insertion or removal (OIR) is not supported; the alarm may indicate an internal Cisco UGM error.
- The chassis supports card OIR, and the chassis is sending OIR traps to Cisco UGM.

Note You may ignore the alarm temporarily.

A graceful shutdown for the chassis is implemented as a busyout followed by a shut down. Therefore, when the number of DS0s reaches 0, the card is shut down. This causes a “card removed” trap to be generated. Cisco UGM then deletes the card object, causing any activity for that card (e.g. Graceful Shutdown) to end abruptly. Thereby, an alarm is raised.

Clear the alarm manually.

Accepting Traffic Failure

This error occurs when the Accept Traffic command fails to bring up some or all T1/E1/T3 controllers.

Accept Traffic directs Cisco UGM to bring up all possible T1/E1/T3 controllers (as appropriate) for the specified card. After telling the chassis to bring up the controllers for the card, the Accept Traffic logic delays checking for “up” T1/E1/T3 controllers until approximately 40 seconds have elapsed. Any controllers that do not come up within that time are identified in the Action Report.

Note This explanation does not describe all possible reasons for an Accept Traffic failure.

Click Accept Traffic again. If the problem persists, there could be a possible IOS configuration problem or a switch (signaling) problem.

IOS Operations Errors

This section describes errors that may occur during IOS operations running with Cisco UGM.

ERROR logging in. Invalid password

Make sure you set the Line and Enable Password correctly in the Device Readiness Configuration dialog box.

See the "Task 1: Preparing the Device for Configuration" section on page4-3.

ERROR:No response from device

Step 1 Check that the device is in the normal (commissioned) state.

Step 2 If you use the console Configuration Interface, check that the console address and port number are set correctly.

Step 3 **Ping** the IP address to see if there is any network delay.

ERROR:Unable to connect. Port may be in use or inaccessible

Make sure that there is no other console login session running because only one user (at a time) can log in from the console.

Cards Supported in Cisco UGM Devices

Cisco UGM devices support the following cards:

Device	Supported Cards
Cisco AS5350	DFC-2 PRI T1/E1 DFC-4 PRI T1/E1 DFC-8 PRI T1/E1 DFC-NP60 DFC-NP108
Cisco AS5400	DFC-4 PRI T1/E1 DFC-8 PRI T1/E1 DFC-CT3 DFC-NP108
Cisco AS5800	CT3 E1/T1 HMM/DMM UPC
Cisco AS5850	UPC 1 CT3, 2 NP 108 1 8 PRI E1, 2 NP 108 RSC

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

X