Cisco Universal Gateway Manager User Guide

Version 2.0

CONTENTS

Preface

Purpose

This document describes how to operate the Cisco Universal Gateway Manager (Cisco UGM) Version 2.0.

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 Available on Cisco.com

- *Cisco Universal Gateway Manager (Version 2.0) Quick Start Guide*
- Cisco Universal Gateway Manager (Version 2.0) Release Note
- *Cisco Universal Gateway Manager (Version 2.0) Installation, Upgrade, and Troubleshooting Guide* (this document)
- *Cisco Universal Gateway Manager (Version 2.0) User Guide*
- *Cisco Universal Gateway Manager (Version 2.0) Documents* (CD-ROM insert)
- *Cisco Element Management Framework (Release 3.2) Installation and Administration Guide*
- *Cisco Element Management Framework (Release 3.2) User Guide*
- Cisco Element Management Framework (Release 3.2) Release Note
- Deployment Release Notes for Cisco Element Management Framework (Release 3.2) Patch 1
- Deployment Release Notes for Cisco Element Management Framework (Release 3.2) Patch 1.1

Online Help

- Cisco Universal Gateway Manager Online Help
- Cisco Element Management Framework Online Help

Where To Get the Latest Version of This Guide

The online copy of this guide is always current and incorporates the latest enhancements to the product. Cisco also provides separate release notes or configuration notes for spares, hardware, and software enhancements occurring between major releases.

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.

Tip   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 with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, 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.

C H A P T E R 1

Deploying, Discovering, and Exporting Inventory Data with Cisco UGM

Deployment, in the context of Cisco UGM operation, represents the creation of object modeling elements in the database. The creation of these modeling elements is necessary in order for Cisco UGM to manage the corresponding device objects in the network.

The autodiscovery function allows you to examine the network for IP and SNMP devices and create a managed object for each new device discovered.

This chapter contains the following sections:

Overview of Deployment and Discovery

In order to set up Cisco UGM to manage network devices, you must first create new objects representing managed network elements. This created object represents a real object in the network: a managed device (Cisco AS5300, AS5350, AS5400, AS5800, AS5850) is represented by a device object, and the cards and ports in the device are represented by device component objects.

The device object can transition between several states (see the "Overview of Discovering a Device Component" section on page 1-12). Device objects can be manually deployed using the Cisco EMF deployment wizard, or autodiscovered using the Cisco EMF autodiscovery application. Device component objects, however, can only be autodiscovered.

During the course of operation, Cisco UGM rediscovers device components. Rediscovery enables Cisco UGM to synchronize its database with the configuration information on the managed devices in the network, and is necessary to manage the device and component objects.

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

The order in which deployment and discovery tasks are carried out are:

1. Deploy container objects.

2. Deploy or auto-discover device objects.

3. Auto discover device components.

About Container Objects

A container object provides a way to group or organize your network elements. You can group managed devices geographically or functionally, and assign names to the container objects.

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

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

- A site object (representing the physical site of the managed devices).

- A bay object (representing a group of managed devices).

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

The Deployment Wizard uses Deployment Profiles to prompt you for information that is required to deploy container objects. For more information on the Deployment Wizard and Deployment Profiles (or templates), refer to the *Cisco Element Management Framework User Guide*.

Deploying Region, Site, or Bay Container Objects

Step 1   Right-click the physical node where you want to deploy the container object, and select **Deployment > Deploy generic objects**.

Step 2   In the Deployment Wizard dialog box, select one of these options: **Region**, **Site**, or **Bay**.

Step 3   Click **Next**.

Step 4   Enter responses to the Deployment Selector Screen and click **Next**.

Step 5   In the Object Details screen, specify a site name.

Step 6   In the Deployment Summary screen, click **Finish** and wait until the deployment process is completed.

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

About Device States in Deployment and Discovery

State	Description
Deploying	Device components are being created in the database.
Initializing	Device data is being loaded from the database.
Commissioning	Device components are being discovered (SNMP discovery).
Handover	The active device is taking over the dial-shelf cards (only for Cisco AS5800 and AS5850 redundant systems).
Normal	Deployment or initializing are successfully completed.
Decommissioned	The device is deployed as decommissioned, or is manually decommissioned.
Errored	The device is unreachable.

About Cisco UGM-Assigned Names for Device Objects

If the managed device has an assigned hostname, Cisco UGM uses that hostname as part of the device object name that appears in the Map Viewer.

Deployment Type	Device Hostname Assigned	Name in Map Viewer
Autodiscovery	Yes	SystemName[1]_IP address Example: LM-5300-1.cisco.com_171.22.41.95
Autodiscovery	No	ChassisClassName_IP address Example: AS5300.cisco.com_171.22.41.95
Manual deployment by using the Template for AS5xxx as Decommissioned	N/A	IP address or loopback address Example: 171.22.41.95
Manual deployment by using the Template for AS5xxx with Sub-Chassis Discovery	Yes	SystemName[2]_IP address Example: LM-5300-1.cisco.com_171.22.41.95
Manual deployment by using the Template for AS5xxx with Sub-Chassis Discovery	No	ChassisClassName_IP address Example: AS5300_171.22.41.95

1. The SystemName consists of the device name and domain name.
2. The SystemName consists of the device name and domain name.

Note
- You can change device object names by choosing
  AS5xxx > **View Manipulation** > **Rename Object**.

- Do not include spaces when you assign object names.
  Example: Site A1 is named Site_A1.

- If you rename device objects, subsequent discovery procedures maintain the
  new device object names in the Map Viewer.

About Deploying Device Objects

You can deploy Cisco UGM device objects manually by using deployment
profiles or templates. You can start the Deployment Wizard only from a container
object. (See the "Deploying a Device Object Manually" section on page 1-8.)

In addition, you can discover device objects automatically by using the
autodiscovery function.

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 components.

Tip   This template creates an object in a decommissioned state. (See the "Overview
of Discovering a Device Component" section on page 1-12.)

Cisco UGM does not communicate with a decommissioned device, and
consequently does not process its traps or collect its performance data.

You can create an object in a decommissioned state to use it as a placeholder
for a device that is currently unavailable or for future expansion of your
network.

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

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

Deploying a Device Object Manually

⚠

Caution   When you manually deploy device objects:

Check that the IP address or loopback address 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 raises an alarm. The created device object cannot be used by Cisco UGM. Delete the object and deploy a device object that matches the template.

Step 1   Right-click a site or region in the left pane and choose: **Deployment > Deploy Access Servers> Deployment Wizard—Templates**. Select the template that you want.

Step 2   Enter the number of objects. If you enter a number greater than 1, repeat Step 3 for each object.

Step 3   Enter the IP address or loopback address of the device that you want to deploy.

Step 4   Enter values for:

- SNMP V1 Read Community
- SNMP V1 Write Community
- SNMP V2 Read Community
- SNMP V2 Write Community

The defaults are public for the Read (SNMP Get) variable and private for the Write (SNMP Set) variable.

Step 5   Select an SNMP version.

Step 6   Enter the Login User Name as specified in the Device Authentication Information dialog box. (See the "Task 1: Authenticating the Device Object" section on page 3-3.)

Step 7   Enter the Login Password as specified in the Device Authentication Information dialog box. (See the "Task 1: Authenticating the Device Object" section on page 3-3.

Step 8   Enter the Enable Password as specified in the Device Authentication Information dialog box. (See the "Task 1: Authenticating the Device Object" section on page 3-3.

Note   Cisco UGM does not validate the entries in these fields.

Step 9   Click **Forward**.

The device components are deployed automatically only if you chose a template with component (sub-chassis) discovery.

See the "Overview of Initializing Cisco UGM Devices" section on page 1-25.

About Autodiscovery of Device Objects

The autodiscovery function allows you to examine the network for IP and SNMP devices and create a managed object for each new device that is discovered.

Note   The difference between this method of populating your network view and that described in the "Deploying a Device Object Manually" section on page 1-8, is that this procedure is automatic. Cisco UGM goes out and examines the network for relevant objects.

Device objects are discovered first, followed by the component objects. After device objects are discovered, Cisco UGM discovers device component objects. (See the "About the Device Component Discovery Throttling Mechanism" section on page 1-12.)

Device and component objects are discovered and located in the region or site from where you initiate discovery.

If your network has devices configured to support redundancy, see the "Overview of Redundancy and High Availability Support" section on page 1-18.

Autodiscovering a Device Object

Step 1   From the Cisco EMF Launchpad, click **Auto discovery**.

Or

From the Map Viewer, select the container object (region, site, or bay) that you want to discover.

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

Step 3   Enter a range of device IP addresses.

This confines the discovery process to a known area of the network. You can enter a loopback address.

Step 4   Enter the Device Subnet Mask address.

Step 5   Select the drop-down menu next to Discovery Method and select **SNMP** or **IP and SNMP**.

Step 6   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 7   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 8   Enter a value for **SNMP Retries**. This is the number of times the system tries 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 9   In the data entry box next to **SNMP Timeout**, enter the required time. The default is 10 seconds.

Step 10   In the **New Community** data entry box, select **Read-Write**.

If Read-Write is not selected, autodiscovery will work, but subsequent tasks such as image management fail.

Step 11   Click **Add**.

Step 12   In the Physical Location panel, click **Use Physical Path**. If required, select **Get Path** for the correct physical view.

Step 13   (Optional) You can restrict the IP address range that the system interrogates by double-clicking a range of addresses in the **Interface Attributes** panel.

The Discovery Interface window appears.

Step 14   (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 15   To start the discovery process, select the device from the Interface Attributes list.

Step 16   Click **Start**.

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

Cisco UGM first discovers all the managed device objects and then proceeds to discover device components, such as cards and ports. This component discovery leads to the creation (under the NAS object) of the hierarchy of component objects.

Each device object discovery is immediately followed by the creation of a corresponding Config Files folder, which is created for both commissioned and decommissioned devices.

Overview of Discovering a Device Component

When Cisco UGM is discovering device components, the parent device object is in these states:

- Commissioning—Cisco UGM detects the components of the device object and determines which component objects should be created in the database.

- Deploying—Cisco UGM compares the current device component objects in the database with the component objects detected. As a result of this comparison, Cisco UGM deletes obsolete objects and creates new objects in the database.

See the "Overview of Discovering a Device Component" section on page 1-12.

About the Device Component Discovery Throttling Mechanism

The discovery and deployment functions can impact overall system performance and overload the management network. A throttle mechanism controls the number of device objects actively being discovered and deployed.

The discovery and deployment activities are controlled independently.

About SNMP Tables Retrieved while Discovering a Device Component

Cisco UGM discovers device components by analyzing the information in 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-MGMT-MIB.cmLineStatusTable

About Events Generated while Discovering a Device Component

There are two kinds of events generated during component discovery:

- Informational events that apprise the user of the progression of discovery.

  These events cancel each other and can be an be viewed only in the Event
  History table that has an advantage over log files because there are no size or
  aging parameters to truncate the table.

Tip   In case a device component discovery hangs, you can change these values:
SNMP timeout, which is set by default to 500msec, and SNMP retries, which
are set to 4 (meaning a maximum of 5 packets are sent)

In the *<CEMFdirectory>*/config/ASMainCtrl/ASMainCtrlUserData.ini file,
change these values:

```
[deployment]
attrValueSnmpRetries = 4
attrValueSnmpTimeout = 500
```

You must stop and start Cisco EMF for the changes to take affect.

- Alarm events that indicate a loss of communication. This indicates that Cisco
  UGM failed to retrieve information from the SNMP tables. These events
  remain in the Event Browser until they are either acknowledged or cleared.

Alarm Event	Description
Discovery failed due to loss of communication with device.	Usually caused by network delays. See the previous Tip for suggestions.
Discovery failed due to UGM internal error.	Caused by an internal Cisco UGM error or by a Cisco IOS image error.
Deployment failed due to UGM internal error.	
Discovery interrupted.	You manually interrupted the deployment or discovery of the device or its components.
Deployment interrupted.	

About Cisco UGM-Assigned Names for Device Component Objects

When Cisco UGM discovers a card, it automatically assigns a name with this format:

Card type-Slot-Serial number

Example:

8CT1_4Serial-0-Serial#:21668561

Where,

8CT1_4Serial—represents the type of card.

-0—represents the device slot in which the card is installed.

Serial#:21668561—represents a unique identifier read directly from the card.

Tip   If the Map Viewer does not display the complete card object name, open the Card Properties dialog to check if all card information was entered.

Auto Discovering Device Component Objects

Note   You cannot manually deploy device components.

Step 1   From the Cisco EMF Launchpad, click **Auto discovery**.

Or

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 **Deployment > Auto discovery**.

Step 3   Enter a range of device IP addresses.

You can enter a loopback address.

Tip   Enter a range of IP addresses for Cisco UGM to discover. This confines the discovery process to a known area of the network.

Step 4 Enter the Device Subnet Mask address.

Step 5 Select the drop-down menu next to Discovery Method and select **SNMP** or **IP and SNMP**.

Step 6 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 7 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 8 Enter a value for **SNMP Retries**. This is the number of times the system tries 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 9 In the data entry box next to **SNMP Timeout**, enter the required time. The default is set to 10 seconds.

Step 10 In the **New Community** data entry box, select **Read-Write**.

If you do not select Read-Write, autodiscovery will work, but subsequent tasks such as image management fail.

Step 11 Click **Add**.

Step 12 In the Physical Location panel, click **Use Physical Path**. If required, select **Get Path** for the correct physical view.

Step 13 (Optional) You can restrict the IP address range that the system interrogates by double-clicking a range of addresses in the **Interface Attributes** panel.

The Discovery Interface window appears.

Step 14   (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 15   To start the discovery process, select the device from the Interface Attributes list.

Step 16   Click **Start**.

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

Overview of Rediscovery

After initially discovering devices, Cisco UGM rediscovers device components to synchronize the database with the device configuration.

> **Note**   In some cases, if you reconfigure a device by using the configlet window (see the "(Optional) Task 11: Viewing and Editing Configuration Files and Configlets" section on page 2-28), the database may not be synchronized with the device.
>
> If this occurs, manually deploy the device object and discover its component objects.

Rediscovery is triggered by:

- Monitoring device reload events (see the "About Monitoring Device Reload Events" section on page 1-17).

- Card insertion and removal events (see the "About Card Insertion and Removal Events" section on page 1-18).

If the underlying device components have changed, corresponding changes are made during rediscovery leading to deletion or creation of device component objects.

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

About Monitoring Device Reload Events

Cisco UGM monitors device reload events that trigger rediscovery:

- Presence Polling based on RFC1213.sysUpTime Object, page 1-17
- Cold and Warm Start Traps, page 1-17

Presence Polling based on RFC1213.sysUpTime Object

Cisco UGM uses the presence polling feature to read the sysUpTime value of the device.

The last reboot time for the device is calculated based on the sysUpTime value and the current time on the server. The reboot time is then checked against the values in the database. If a mismatch (of 60 seconds or more) is detected, the chassis is rediscovered. See the "Overview of Attributes Sampled for Presence Polling" section on page 8-3.

Note In order to obtain accurate readings for the sysUpTime and server clock values, make sure that you synchronize the Cisco UGM clock with the clocks of all managed devices in the network. Use NTP to achieve this synchronization.

If you do not synchronize clocks, the timings for the Cisco UGM server and managed devices may drift and cause inaccurate readings of the sysUpTime value. This may cause false indications of device reboots.

Cold and Warm Start Traps

When a cold start or warm start trap is received, Cisco UGM triggers rediscovery.

About Card Insertion and Removal Events

Cisco UGM monitors two card insertion and removal events that trigger rediscovery:

- Card-Level Presence Polling, page 1-18
- Online Insertion and Removal (OIR) Traps, page 1-18

Card-Level Presence Polling

Cisco UGM uses the presence polling feature to read the device's cardTablevalue. This attribute detects if cards were installed or removed from the device

Online Insertion and Removal (OIR) Traps

Cisco UGM receives an Online Insertion and Deletion (OIR) trap (from a device that supports OIR).

Overview of Redundancy and High Availability Support

Cisco UGM supports redundancy features for Cisco AS5800 devices, and High Availability support for Cisco AS5850 devices in the areas of discovery, deployment, and configuration. These features implement cold standby redundancy: An active device controls a set of feature cards. In the event of a failure, the redundant peer device identifies the failure, resets the feature cards, and takes control of them.

Cisco UGM identifies redundant devices and creates a new container object in the Physical view. This container object is a visual representation of the association between devices in a redundant pair.

Feature card objects are created under a device object only if the device object actually controls these cards at the time of deployment.

About Cisco AS5800 Redundancy Support

The Cisco AS5800 device works in one of the following configurations:

- Single router shelf with one or two dial-shelf controllers (DSCs)
- Dual router shelves in a split mode
- Dual router shelves in redundancy mode

Each time a Cisco AS5800 device is discovered or deployed, its redundancy status is read from the device.

Redundant Cisco AS5800 devices can be in one of the two states: active or standby.

- The active device controls all the dial-shelf cards and contains its own interface cards and all the dial-shelf cards in its containment hierarchy.
- The standby device controls only its own router shelf resources. It does not control the dial-shelf cards except the DSC card (connected to its router shelf using a DSI interconnect cable).

About Identifying Redundant Cisco AS5800 Devices (Redundancy Identifier)

To facilitate matching Cisco AS5800 redundant device pairs, each device is identified by its dial-shelf identification (id). If two devices have the same dial-shelf id, they are identified as redundant peers. In this context, the dial-shelf id is called the redundancy identifier.

Note   Configure the dial-shelf id so that redundant devices have the same dial-shelf id value, and the dial-shelf id values are unique across the managed network.

When deploying Cisco AS5800 devices, Cisco UGM reads the dial-shelf id from the device. The device is then reparented under a special redundancy container object. If Cisco UGM has detected the redundant peer (for the device), it is already positioned under the redundancy container object, and the new device is reparented under the same container object. If there is no peer device, a new redundancy container is created, and the new device is reparented under it.

Cisco AS5800 Device Redundancy Container Object

The redundancy container object shows an association between redundant Cisco AS5800 device objects. Such a container object is assigned a name which contains the redundancy identifier of the corresponding devices.

About the Cisco AS5800 Device Failover Event

In the event of a failure, the redundancy state of one or both redundant devices changes. The standby device becomes active and vice versa. Traps are sent from the devices to alert the management station about the failure event. Cisco UGM monitors these traps. When such a trap is received the device transitions to a handover state. This new state in the Cisco AS5800 state machine waits until the active device finishes the takeover of the dial-shelf cards. This process can take up to several minutes.

When the takeover is completed, Cisco UGM starts device rediscovery. The device remains in the handover state for a predefined period of time, which is currently set to 90 seconds.

You can change this time duration by accessing:

`ASMainCtrlUserData.ini`

`AS5800ChassisHandoverLingerSec`

When the time duration ends, the device is moved into a commissioning state to finish the rediscovery.

Because traps can be unreliable, Cisco UGM also uses a redundancy polling feature to ensure that changes in redundancy state are identified. If the polling mechanism identifies a change for a given device, rediscovery is started by moving the device into the Commissioning state.

If a redundancy state change is identified, a warning severity alarm is raised against the device object.

About Identifying a Dial-Shelf Card

In a redundancy configuration, only the cards controlled by a device object are created as device component objects.

If a card is not controlled by the device, its operational status is:

value not specified (1).

About Configuration Changes

If a device undergoes a configuration change that affects redundancy, the periodic redundancy presence polling eventually detects this, and rediscovery occurs. If a device becomes nonredundant, it is reparented under the immediate parent of the corresponding redundancy container in the Physical view. If the device was the last object under the redundancy container, the container is deleted.

If a redundancy identifier is modified, the device is reparented under the redundancy container corresponding to the new redundancy identifier. If such a container does not exist, it is created.

About IOS Images Backward Compatibility

Since the redundancy feature for Cisco AS5800 devices is only supported by newer Cisco IOS images, Cisco UGM addresses the issue of backward compatibility with older IOS images. The redundancy feature comes with a management interface that uses the CISCO-C8500-REDUNDANCY-MIB. If this MIB is not supported, Cisco UGM assumes that the current IOS image does not support redundancy. In this case Cisco UGM sets the redundancy state to N/A.

About the Redundancy Status Dialog Box

The Redundancy Status dialog box shows the current redundancy status of the device, and is described in the "Checking the Redundancy Status of a Cisco AS5800 Device" section on page 6-35.

Note   This dialog box shows the status as read from the device. Cisco UGM may be temporarily unsynchronized with the status on the device. It may take several minutes for redundancy presence polling to get the new status from the device and to reflect the new status in the dialog box.

Cisco AS5850 High Availability Feature Support

The Cisco AS5850 device has 14 slots. Slots 6 and 7 are designated for Router Shelf Controller (RSC) cards.

In a High Availability configuration, RSCs control their parts of the shelf under normal conditions. If one RSC fails, the surviving RSC takes control of all the cards that were formerly controlled by the failed RSC, reloads the cards, and places them back in service.

Every time a Cisco AS5850 device is discovered or deployed, Cisco UGM reads the redundancy status from the device. If a device is configured in High Availability mode, a special container object is created in the Physical view, and the device is reparented under this container.

A redundant Cisco AS5850 device can be in one of three states:

*   Active. In this condition, the device controls only its half of the shelf. The other half is controlled by the second RSC.

*   ActiveExtraload. In this condition, the device controls all the cards installed in the shelf. The other RSC in this situation may be absent or in standby mode.

*   Standby. In this condition, the device does not control any of the shelf resources, except the RSC card and its interfaces.

Identifying Redundant Cisco AS5850 Devices - Redundancy Identifier

To match redundant Cisco AS5850 peer devices, every device is identified by using its backplane shelf identifier. This string identifier is programmed during the manufacturing process. If two devices have the same backplane shelf identifier, they share the shelf.

Note The redundancy identifier for the Cisco AS5850 device is transparent. Its value is unique across any managed network in the entire universe.

During Cisco AS5850 device deployment, Cisco UGM reads the redundancy identifier from the device. The device is then reparented under a special redundancy container object. If the redundant peer (for the device) has been discovered, it is already positioned under the redundancy container object, so that the new device is reparented under the same container object. If there is no peer device a new redundancy container is created, and the new device is reparented under this new container.

Cisco AS5850 Device Redundancy Container

The redundancy container object shows an association between redundant Cisco AS5850 peer devices. The name assigned to this container object contains the redundancy identifier of the corresponding device.

Cisco AS5850 Device Failover Event

In an event of a failover, the redundancy state of one or both redundant devices changes. The traps are usually sent from the devices to alert the management station about the event. Cisco UGM monitors these traps. When such a trap is received, the device transitions to a handover state. This is a new state in the Cisco AS5850 state machine, which represents the wait until the active device finishes the takeover of the dial-shelf cards. This process can take up to several minutes.

When the takeover ends, you can start rediscovering devices. The device remains in the handover state for a predefined period, which is currently set to 90 seconds.

You can change this time by accessing:

`ASMainCtrlUserData.ini`

`AS5850ChassisHandoverLingerSec`

When the timer ends, the device is moved into the commissioning state to finish the rediscovery.

Because traps can be unreliable, Cisco UGM also uses a special redundancy polling feature to ensure that changes in redundancy state are identified. If the polling mechanism identifies a change for a given device, rediscovery is started by moving the device into the Commissioning state.

If a redundancy state change is identified, a warning severity alarm is raised against a device object.

About Identifying Router Shelf Cards

In a High Availability configuration, only the resources controlled by a device object are created as the device component objects.

If a card is not controlled by the device, its operational status is "value not specified (1)."

Configuration Changes

If a Cisco AS5850 device undergoes a configuration change which affects redundancy, the periodic redundancy presence polling detects this and rediscovery takes place. If a device becomes nonredundant it is reparented under the immediate parent of the current redundancy container in the Physical view. If it was the last object in the redundancy container, the container is also deleted.

If a redundancy identifier is modified, the device is reparented under the redundancy container corresponding to the new redundancy identifier. If such a container does not exist, it is created.

About Cisco IOS Image Support for the High Availability Feature

Since the High Availability feature is only supported by newer Cisco IOS images, Cisco UGM addresses the issue of backward compatibility with older IOS images. The High Availability feature includes a management interface that uses CISCO-RF-MIB. If this MIB is not supported, Cisco UGM assumes that the current Cisco IOS image does not support this feature. In this case, Cisco UGM sets the redundancy state to N/A.

Redundancy and Configuration Status Dialog Box

The Redundancy Status and Configuration dialog box shows the current High Availability status of the Cisco AS5850 device. The dialog box is described in "Checking the Redundancy Status of a Cisco AS5850 Device" section on page 6-36.

Note   The Redundancy Status and Configuration dialog box shows the status value as read from the device. At times, Cisco UGM may be temporarily unsynchronized with the status on the device, and may take several minutes for redundancy presence polling to get the new status from the device.

Overview of Initializing Cisco UGM Devices

When you stop and restart Cisco UGM, existing device objects move into an Initializing state where all devices and components are reconciled with the Cisco UGM database. Values from the device object initialization are later used for performance polling and rediscovery.

- Device object initialization works on a small number of devices at a time. The default value is 5. You can modify this value in the .ini file located at:

  <CEMFROOT>/config/ASMainCtrl/ASMainCtrlUser.ini

  [ChassisInitialization]

  maxSubChassisQueries=

  In order for this change to take effect, stop and start Cisco EMF. See the *Cisco Element Management Framework Installation and Administration Guide*.

- During device initialization, no presence or performance polling is carried out on the device. Cisco UGM receives traps from these devices, but does not process them.

Note   Check the device state by choosing *Device* > **Chassis** > **Open Access Server Chassis Properties**.

Alarms Generated During Device Initialization

- Initialization for chassis failed
- Chassis initialization interrupted

   You can view these major alarms in the Event Browser.

   If either of these conditions occur, decommission and then commission the device in order to initiate initialization. If a chassis was not initialized properly, the performance polling and rediscovery will fail.

State Changes that Accompany Device Object Initialization

Table 1-1   Device Object Initialization State Changes

State Before Initializing	State After Initializing
deploying	commissioning
IOSImageDownload	normal
IOSImageUpgrade	normal
IOSImageDownloadToRouter	normal
IOSImageDownloadToDial	normal
ModemImageDownload	normal
ModemImageUpgrade	normal
SPEImageDownload	normal
SPEImageUpgrade	normal

Table 1-1   Device Object Initialization State Changes (continued)

State Before Initializing	State After Initializing
VFCImageDownload	normal
VFCImageUpgrade	normal

For all other states not covered in this table, the device state after initialization is the same as the state before initialization.

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 export task (at a time) for inventory data export. If multiple export tasks are scheduled 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 physical view (of the managed devices) in a flat file. Data output consists of device types 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, moveTarCompress) for the inventory output files.

- Exported inventory objects consist of all objects in the Map Viewer Physical view, including cards. Components below the card level (such as port or modem) are not exported.

- Exported attributes include IP address, shelf, slot, and descriptions for component objects. (See Table 1-2 for a complete list of supported attributes.)

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 is updated for the selected objects. To export the inventory data, see the "Exporting Inventory Data Immediately" section on page 1-28.

Exporting Inventory Data Immediately

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

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

Step 3   Select **on demand**.

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 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 5   Enter the aging interval (in days) of the file before the selected aging action is performed. Export then continues in the newly created file.

Step 6   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 7   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.

Step 8   Click **Export Now**.

- Triggers the immediate export of inventory data by using the saved Storage Path.

   The export data filename is
   invFileName.EXPORT_YY-MM-DD_HH-MM-SEC

   Where,

   invFileName is the filename specified in Step 6.

   EXPORT_YY-MM-DD_HH-MM-SEC is a timestamp appended to the file.

- Generates an Action Report containing results of this action.

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 **ASEMSConfig > File Export > Open File Export Properties**.

Step 2   In the Export Type field, select **Scheduled**.

Step 3   Enter a storage path for the inventory data 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 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 5   Enter the aging interval (in days) of the file before the selected aging action is performed. Export then continues in the newly created file.

Step 6   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 7   Select the frequency of data export:

- **hourly**

- **daily**

- **weekly**

- **monthly**

Step 8   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 9   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 10   Select the scheduled day of the month for the export:

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

Step 11   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 page 1-36.

Note   The export data filename is
invFileName.EXPORT_YY-MM-DD_HH-MM-SEC
Where,
invFileName is the filename specified in Step 6.
EXPORT_YY-MM-DD_HH-MM-SEC is a timestamp appended to the file.

Attributes Sampled for Inventory Data Export

Note   If a device or component 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.

Table 1-2   Inventory Data Export Attributes

Object	Attribute	Attribute Name	Value
Region	Name	regionName	0 to 255 characters
Site	Name	SiteName	0 to 255 characters
	Contact name	AV-SITE-MIB.contact1Name	0 to 255 characters
	Contact phone	AV-SITE-MIB.contact1Phone	0 to 255 characters
	Contact pager	AV-SITE-MIB.contact1Pager	0 to 255 characters
	Contact e-mail	AV-SITE-MIB.contact1Email	0 to 255 characters
	Site Phone	AV-SITE-MIB.sitePhone	0 to 255 characters
	Site Fax	AV-SITE-MIB.siteFax	0 to 255 characters
	Site Address	AV-SITE-MIB.siteAddress	0 to 255 characters
	Site City	AV-SITE-MIB.siteCity	0 to 255 characters
	Site State	AV-SITE-MIB.siteState	0 to 255 characters
	Site ZIP	AV-SITE-MIB.siteZip	0 to 255 characters

Table 1-2   Inventory Data Export Attributes (continued)

Object	Attribute	Attribute Name	Value
AS5300	IP address	AMAF-MGMT-MIB.ipaddress	N/A
AS5350	Chassis version	OLD-CISCO-CHASSIS-MIB. chassisVersion	0 to 255 characters
AS5400	Chassis type	OLD-CISCO-CHASSIS-MIB. chassisType	Enumeration (integer 00-99)
AS5800	Chassis ID	OLD-CISCO-CHASSIS-MIB. chassisId	0 to 255 characters
AS5850	Slots in chassis	OLD-CISCO-CHASSIS-MIB. chassisSlots	Integer
	ROM monitor version	OLD-CISCO-CHASSIS-MIB. romVersion	0 to 255 characters
	ROM system software version	OLD-CISCO-CHASSIS-MIB. romSysVersion	0 to 255 characters
	System name	SNMPv2-MIB.sysName	0 to 255 characters
	System contact	SNMPv2-MIB.sysContact	0 to 255 characters
	System location	SNMPv2-MIB.sysLocation	0 to 255 characters
	System description	SNMPv2-MIB.sysDescr	0 to 255 characters
Card	Software version	OLD-CISCO-CHASSIS-MIB. cardSwVersion	0 to 255 characters
	Hardware version	OLD-CISCO-CHASSIS-MIB. cardHwVersion	0 to 255 characters
	Serial number	OLD-CISCO-CHASSIS-MIB. cardSerial	Integer (0 to 9999999999)
	Slot number	OLD-CISCO-CHASSIS-MIB. cardSlotNumber	Integer (00 to 99)
	Slots in this card	OLD-CISCO-CHASSIS-MIB. cardSlots	Integer (00 to 99)

Example of an Inventory Export File

See the "Format of Exported Data" section on page 1-36 for a description of fields in this file.

Note   If Cisco UGM fails to retrieve a value for an attribute, "no value retrieved" appears. In the example shown in this section, the value of the AV-SITE-MIB.attributes are " ."

```
<region>
RegionName="West"

<Site>
SiteName="Site-1"

AV-SITE-MIB.siteZIP=""
AV-SITE-MIB.siteState=""
AV-SITE-MIB.siteCity=""
AV-SITE-MIB.siteAddress=""
AV-SITE-MIB.siteFAX=""
AV-SITE-MIB.sitePhone=""
AV-SITE-MIB.contact1EMail=""
AV-SITE-MIB.contact1Pager=""
AV-SITE-MIB.contact1Phone=""
AV-SITE-MIB.contact1Name=""

<Chassis>
AMAF-MGMT-MIB.ipaddress="10.85.66.112"

OLD-CISCO-CHASSIS-MIB.chassisVersion="A.32"
OLD-CISCO-CHASSIS-MIB.chassisType=73
OLD-CISCO-CHASSIS-MIB.chassisId="21667966"
OLD-CISCO-CHASSIS-MIB.chassisSlots=3
OLD-CISCO-CHASSIS-MIB.romVersion="
System Bootstrap, Version 12.0(2)XD1, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Copyright (c) 2001 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info

"OLD-CISCO-CHASSIS-MIB.romSysVersion="Cisco Internetwork Operating
System Software
IOS (tm) 5300 Software (C5300-BOOT-M), Version 12.0(4)T1,  RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 18-May-01 13:58 by kpma"

RFC1213-MIB.sysLocation=""
RFC1213-MIB.sysDescr="Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C5300-JS-M), Version 12.2(1a), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
```

```
Compiled Fri 25-May-01 22:32 by pwade"

RFC1213-MIB.sysContact=""
RFC1213-MIB.sysName="lm-5300-1"
<Card>
OLD-CISCO-CHASSIS-MIB.cardDescr="Quad Port Channelized T1/PRI Dial
Feature Card"
OLD-CISCO-CHASSIS-MIB.cardSwVersion=""
OLD-CISCO-CHASSIS-MIB.cardHwVersion="1.1"
OLD-CISCO-CHASSIS-MIB.cardSerial=41706
OLD-CISCO-CHASSIS-MIB.cardSlotNumber=2
OLD-CISCO-CHASSIS-MIB.cardSlots=0
</Card>

<Card>
OLD-CISCO-CHASSIS-MIB.cardDescr="Nextport Dial Feature Card"
OLD-CISCO-CHASSIS-MIB.cardSwVersion=""
OLD-CISCO-CHASSIS-MIB.cardHwVersion="3.4"
OLD-CISCO-CHASSIS-MIB.cardSerial=3440083
OLD-CISCO-CHASSIS-MIB.cardSlotNumber=1
OLD-CISCO-CHASSIS-MIB.cardSlots=0
</Card>

<Card>
OLD-CISCO-CHASSIS-MIB.cardDescr="Nextport Dial Feature Card"
OLD-CISCO-CHASSIS-MIB.cardSwVersion=""
OLD-CISCO-CHASSIS-MIB.cardHwVersion="4.2"
OLD-CISCO-CHASSIS-MIB.cardSerial=41803
OLD-CISCO-CHASSIS-MIB.cardSlotNumber=3
OLD-CISCO-CHASSIS-MIB.cardSlots=0
</Card>

</Chassis>
</Site>
```

Format of Exported Data

- Integer data uses the syntax Attribute_ID=N, where Attribute_ID is the attribute ID string, and N is the numerical value. An empty value is shown as 0.

- Character data uses the syntax Attribute_ID="CHAR", where Attribute_ID is the attribute ID string and "CHAR" (with double quotation marks) is the character string. An empty value is shown as " ".

Inventory export data in the flat file follows a defined sequence and structure.

The file consists of nested values. Each record begins with an <object> tag and ends with a </object> tag. These records can contain other values.

Note   Inventory data flat files do not contain object names. For additional information on objects (chassis, card) open the Device Properties dialog box or the Card Properties dialog box.

Configuring Devices with Cisco UGM

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

Building the Configuration File, page 2-15.

- Task 3: Option 2: Using an Existing Configuration File, page 2-16.

- Task 3: Option 3: Importing a Configuration File, page 2-17.

- (Optional) Task 4: Importing a Configlet, page 2-18.

- Task 5: Associating a Configuration File with a Device Object, page 2-23.

- (Optional) Task 6: Associating a Configlet with a Device Object, page 2-24.

- Task 7: Sending a Configuration File from the Cisco UGM Server to the Startup File of a Device Object, page 2-25.

- (Optional) Task 8: Sending a Configlet to the Running Configuration File, page 2-26.

- (Optional) Task 9: Uploading the Device Startup Configuration File to the Cisco UGM Server, page 2-27.

- (Optional) Task 10: Copying the Running Configuration to the Startup Configuration File, page 2-28.

- (Optional) Task 11: Viewing and Editing Configuration Files and Configlets, page 2-28.

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.

Cisco UGM performs all Cisco IOS operations through the Ethernet interface used to discover the device.

Tip   Before testing Cisco IOS commands on your Cisco UGM system, save the original configuration file from the device.

Device configuration files are stored in the corresponding ConfigurationFiles folder under each device. Configuration files used by Cisco UGM are:

- Uploaded from the startup configuration of a device.

- Imported from a UNIX file system.

- Generated from the default template.

Note   Redundancy and split mode functionality for the Cisco AS5800 and AS5850 devices are not configured by Cisco UGM. You can configure these features by using Cisco IOS configlets.

For information on configuring this functionality, check the Cisco IOS documents.

State Changes in Supported Devices

This table indicates if a state change results from configuration actions available for Cisco UGM-managed devices.

Table 2-1   State Changes Associated with Configuration Actions

Configuration Action	State Change
Generate configuration file from a template	No
Get Startup Configuration	No
Associate a configuration file with a device	No
Associate a configlet with a device	No
Send Configuration to Startup	Yes (only if followed by a reload)
Send Configlet to Running	No
Copy Running to Startup	No

> **Note** You cannot schedule file operations, and they do not change the state of the managed device.

Task 1: Authenticating the Device Object

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

Step 1 From a container or device object to be configured, select **Configure Device > Open Device Authentication Information**.

Step 2 If you opened this dialog box from a container, select a device object.

Step 3 Enter the Login User Name as configured on the device.

Step 4 Enter and verify a Login Password.

> **Note** If the device has vty line password configured, enter the vty line password for the Login Password.

Step 5 Enter and verify an Enable password.

Step 6 Enter the Operation Timeout value in seconds. The default value is 10 seconds.

You can change this value located at:

```
IOSConfigCtrlUserData.ini
attrValueOpTimeout=n
```

Step 7 Enter the Prompt Timeout value in seconds. The default value is 10 seconds.

You can change this value located at:

```
IOSConfigCtrlUserData.ini
attrValuePromptTimeout=n
```

✎
Note   Enter values in all the fields in this dialog. If you do not enter these values, the
following operations will fail:
Show CLI
Configure Administrative State
All actions on the IOS Operations dialog.

Step 8   Click **Save**.

Task 2: Selecting a Reload Option After a Configuration Download

Step 1   Choose **AS5*xxx* > Configure Device > Perform IOS Operations.**

Step 2   Under Options, select an option for Reload After Config Download.

- **Yes**—The managed device reboots after the Send Configuration to Startup
  operation.

- **No**— The managed device does not reboot immediately after the Send
  Configuration to Startup operation, and you can schedule the device reload
  operation.

✎
Note   Even though you can perform the Reload operation on multiple
devices, do not reload more than three devices at a time.

Since Reload is a scheduled operation, you can schedule up to three
devices to be reloaded at time A then, schedule the next group (up to
three devices) at time A+30 minutes, and follow the same sequence
with the remaining devices.

Step 3   Click **Save**.

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

Cisco UGM does not allow you to define your own configuration file template. You must use the templates provided.

Note When building a configuration file from template, do not enter values for the user name, user password, and enable password. These values are automatically retrieved from the Device Authentication Information dialog box.

To build a configuration file from a template for Cisco AS5300, AS5350, AS5400, and AS5800 devices, complete the following procedures in this order:

1. Selecting Access Parameters (General Tab), page 2-7

2. (Optional) Selecting Split-Mode Parameters for the Cisco AS5850 Device (Redundancy Tab), page 2-8

3. (Optional) Selecting Card Parameters for the Cisco AS5850 Device (Slots 0-5 Tab; Slots 8-13 Tab), page 2-10

4. Entering SNMP Information for a Trap (SNMP Tab), page 2-11

5. Selecting Cisco IOS Core Dump, Logging, and Time Parameters (Management Tab), page 2-12

6. Entering Modem and SPE Parameters (SPE and Modem Tabs), page 2-13

7. Entering Network Communication Parameters (Other Tab), page 2-14

8. Building the Configuration File, page 2-15

To build a configuration file from a template for a Cisco AS5850 device, complete the following procedures in this order:

1. Selecting Access Parameters (General Tab), page 2-7

2. (Optional) Selecting Split-Mode Parameters for the Cisco AS5850 Device (Redundancy Tab), page 2-8

3. (Optional) Selecting Card Parameters for the Cisco AS5850 Device (Slots 0-5 Tab; Slots 8-13 Tab), page 2-10

4. (Optional) Selecting Card Parameters for the Cisco AS5850 Device (Slots 0-5 Tab; Slots 8-13 Tab), page 2-10

5. Entering SNMP Information for a Trap (SNMP Tab), page 2-11

6. Selecting Cisco IOS Core Dump, Logging, and Time Parameters (Management Tab), page 2-12

7. Entering Modem and SPE Parameters (SPE and Modem Tabs), page 2-13

8. Entering Network Communication Parameters (Other Tab), page 2-14

9. Building the Configuration File, page 2-15

To use an existing configuration file, see the "Task 3: Option 2: Using an Existing Configuration File" section on page 2-16. To import a configuration file, see the "Task 3: Option 3: Importing a Configuration File" section on page 2-17.

Tip   If you are building configuration files for several managed devices, first select each individual device and specify unique parameters, such as a hostname and an IP address. Then, select all the devices and specify common configuration parameters for them.

Selecting Access Parameters (General Tab)

Step 1   From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5*xxx* Template.**

Step 3   Click the **General** tab.

Step 4   Enter the host name of the device.

Step 5   Select the authentication method for users, accounting, administration, the network, and Point-to-Point Protocol (PPP) users if necessary.

Step 6   Enter the authentication key to use with Radius or Terminal Access Controller Access Control System (TACACS) servers if necessary.

Step 7   Enter the list of Radius or TACACS servers to use for authentication.

Note   Cisco UGM does not check these parameters for validity. Your entries are inserted into the configuration file.

Step 8   Enter local user names and passwords for additional users.

✎

Note   Do not enter user names and user passwords entered previously in the Device Authentication Information dialog box. Values from that dialog box are automatically retrieved when building the configuration file.

Step 9   Click **Save**.

(Optional) Selecting Split-Mode Parameters for the Cisco AS5850 Device (Redundancy Tab)

Step 1   From the Map Viewer window, select the Cisco AS5850 device object for which you wish to build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5850 Template.**

Step 3   Click the **Redundancy** tab.

Step 4   Select a Redundancy Mode for the device:

✎

Note   Select the same split mode (Classic-split or Handover-split) for both devices in a split-mode configuration.

- **Classic-split**—In this mode, the configuration file you are building configures cards controlled by the Router Shelf Controller (RSC) that you select in Step 5.

- **Handover-split**—In this mode, the configuration file you are building configures all cards installed in all slots in this device.

Step 5   Select a Router Shelf Controller (RSC) for the device:

- **RSC6**—Specifies that the RSC is installed in slot 6 of the parent device. The Ethernet information in slot 7 is ignored. (This configuration file configures Ethernet ports in slot 6 only.)

    – If you selected the Classic-split mode in Step 4, this configuration file configures cards installed in slots 0 through 5 only.

      – If you selected the Handover-split mode in Step 4, this configuration file configures all the cards installed in all the slots on the device.

    • **RSC7**—Specifies that the RSC is installed in slot 7 of the parent device. The Ethernet information in slot 6 is ignored. (This configuration file configures Ethernet ports in slot 7 only.)

      – If you selected the Classic-split mode in Step 4, this configuration file configures cards installed in slots 8 through 13 only.

      – If you selected the Handover-split mode in Step 4, this configuration file configures all the cards installed in all the slots on the device.

Step 6　Repeat this procedure for the next Cisco AS5850 managed device.

Step 7　Click **Save** (under the General tab).

Selecting Card Parameters (Slots Tab)

Step 1　From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2　Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3　Click the **Slots** tab.

Step 4　Select the type of card installed in each slot.

Step 5　(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 6　(Optional) Select the controller line code for this slot.

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

Step 7　(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).

Step 8　Select an ISDN switch for the D channel.

Step 9　Click **Save** (under the General tab).

(Optional) Selecting Card Parameters for the Cisco AS5850 Device (Slots 0-5 Tab; Slots 8-13 Tab)

Step 1 From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2 Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3 If you selected RSC6 in "(Optional) Selecting Split-Mode Parameters for the Cisco AS5850 Device (Redundancy Tab)" section on page 2-8, click the **Slots 0-5** tab.

Or

If you selected RSC7 in "(Optional) Selecting Split-Mode Parameters for the Cisco AS5850 Device (Redundancy Tab)" section on page 2-8, click the **Slots 8-13** tab.

Step 4 Select the type of card installed in each slot.

Step 5 (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 6 (Optional) Select the controller line code for this slot.

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

Step 7 (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).

Step 8 Select an ISDN switch for the D channel.

Step 9 Click **Save** (under the General tab).

Selecting Interface Parameters (Interface Tab)

✎

Note Cisco UGM default configuration templates support IP connectivity over Ethernet or Loopback interfaces only.

Step 1   From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3   Click the **Interface** tab.

Step 4   Select the ISDN switch type.

Step 5   Enter Ethernet and Fast Ethernet IP addresses and masks.

Step 6   Enter loopback IP addresses and masks.

Step 7   Click **Save** (under the General tab).

Entering SNMP Information for a Trap (SNMP Tab)

Step 1   From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3   Click the **SNMP** tab.

Step 4   Enter the location and owner of this system.

Step 5   Enter the SNMP read and write community strings.

Step 6   Enter the Cisco IOS Trap Source (name of the interface).

Step 7   Enter the IP addresses of hosts where the traps will be sent.

The Cisco UGM server IP address is automatically configured as a trap host.

Step 8   Click **Save** (under the General tab).

Selecting Cisco IOS Core Dump, Logging, and Time Parameters (Management Tab)

Step 1 From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2 Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3 Click the **Management** tab.

Step 4 To enable a Cisco IOS core dump transfer to all the hosts on the core dump list, select:

- **Yes**

- **No**

Step 5 (Optional) Select a transfer method to use when sending the Cisco IOS core dump file to its destinations:

- **ftp**

- **tftp**

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

Step 6 (Optional) Enter the FTP User Name.

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

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

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

Step 8 (Optional) Enter a filename for the Cisco IOS core dump file being transferred.

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

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

Step 9 (Optional) Enter a list of hosts or IP addresses that will receive the Cisco IOS core dump file.

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

Step 10   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 11   Select a Logging Facility.

Step 12   Select a level of traps to be sent to the logging server.

Step 13   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 14   To set the time parameter, select the time zone in which this device is located.

Step 15   Specify if this device uses daylight savings time.

Step 16   Enter the IP addresses of Network Time Protocol (NTP) servers.

Step 17   Click **Save** (under the General tab).

Entering Modem and SPE Parameters (SPE and Modem Tabs)

Step 1   From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3   Click the **SPE/Modem** tab.

Step 4   Specify if you want to enable the modem or SPE firmware upgrade in the configuration file.

Step 5   (Optional) Select the modem/SPE firmware upgrade method:

- **busyout** (Graceful)—Prevents idle modems from accepting calls, but allows completion of any calls in progress. When the call is complete, the modem moves to the busyout state and does not accept any new calls. When all the modems on a card are in the busyout state, the firmware is upgraded on the card, and the card (and modems) move to the normal state.

A card does not move to the busyout state if even one of its modems is processing a call. This can prevent the firmware upgrade. You can terminate calls by using the Cisco IOS clear command.

- **reboot** (Forceful)—Upgrades the modem or SPE image during the next device reboot.

- **recovery**—The firmware upgrade is delayed until recovery maintenance time.

- **download-maintenance—**The firmware image is upgraded only when the managed device is taken offline for maintenance purposes.

  You can schedule download-maintenance windows by using Cisco IOS commands. When you select the download-maintenance option for firmware upgrade, the modems run the old firmware until Cisco UGM enters the scheduled maintenance window. During this scheduled maintenance, any calls in progress are dropped. When the firmware upgrade is complete, the modems resume call processing by using the new firmware.

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

Note   You can select the firmware upgrade method either here or in the IOS Operations dialog box (see the "Task 2: Selecting a Reload Option After a Configuration Download" section on page 2-5).

You can select the firmware upgrade method from either location in order to set the same Cisco UGM variable.

Step 6   Enter the SPE firmware file name that is stored in Flash memory.

Step 7   Click **Save** (under the General tab).

Entering Network Communication Parameters (Other Tab)

Step 1   From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3   Click the **Other** tab.

Step 4   Enter the beginning and ending IP addresses of the local IP address pool.

Step 5   Specify if Enhanced Interior Gateway Routing Protocol (EIGRP) should be enabled by selecting **Yes** or **No**.

Step 6   Enter a list of EIGRP network IP addresses.

Step 7   Specify if Virtual Private Dialing Network (VPDN) support is enabled for this device.

Step 8   Enter the VPDN source IP address.

Step 9   Enter a list of DNS server IP addresses.

Step 10   Enter a list of NetBIOS Name Service (NBNS) server IP addresses.

Step 11   Enter a list of default route IP addresses.

Step 12   Enter a list of IP addresses for name servers.

Step 13   Click **Save** (under the General tab).

Building the Configuration File

✎

Note   Before you start building the configuration file, save all parameters that you entered by selecting the **General** tab and then clicking **Save**.

Step 1   From the Map Viewer window, select the device object for which you will build a configuration file.

Step 2   Select **Configure Device > Build Config File from Default AS5***xxx* **Template.**

Step 3   Click the **General** tab.

Step 4   Click **Build Configuration**.

Cisco UGM creates a configuration file object in the ConfigurationFiles folder under the device object in the Physical view.

Cisco UGM saves the new configuration file object under the following file name: autoGenerated_*year_month_day_hour_minute_second*.

For example, if the new file name is autoGenerated_2001_04_06_13_28_50, this indicates that the configuration file was created from the default template on April 6, 2001 at 13:28:50.

You can now associate the file with a device as described in the "Task 5: Associating a Configuration File with a Device Object" section on page 2-23.

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 2-6.

When you click **Get Startup Configuration** in the IOS Operations Dialog box, you upload the configuration file from a device to the /tftpdir directory on the Cisco UGM server. This is a real-time operation that cannot be scheduled later.

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

If the running configuration on the target device is different from its startup configuration and you want to retrieve the running configuration, first click **Copy Running to Startup** before following this procedure.

Step 1   From the Map Viewer, select the device 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 Startup Configuration**.

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

Cisco UGM saves the new configuration file object under the following file name: startup_*year_month_day_hour_minute_second*.

For example, if the new file name is startup_2001_04_26_17_28_50, this indicates that the configuration file was created from the default template on April 26, 2001 at 17:28:50.

You can now associate the file with a device as described in the "Task 5: Associating a Configuration File with a Device Object" section on page 2-23.

To edit the configuration file, see the "(Optional) Task 11: Viewing and Editing Configuration Files and Configlets" section on page 2-28.

Task 3: Option 3: Importing a Configuration File

Before importing a configuration file, you must deploy a managed device.

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

Step 2 From a ConfigurationFiles object, a container object, or a device object, select **Deployment > Import NAS File Object**.

Step 3 If you launch the dialog box is from a ConfigurationFiles or container object, the Deployment Wizard appears:

  a. In the Template Choices window, select the Store Configuration File option and click **Forward**.

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

  c. Enter the full-path filename and description of the Cisco IOS configuration file to be imported.

> **Note** If you enter an invalid full-path filename (or no path) for the configuration file, the import operation fails.

  d. Click **Forward**.

  e. Proceed to Step 5.

Step 4 If you launch the dialog box from a device object, the Deployment Wizard appears:

  a. In the Template Choices window, select the Store Configuration File option and click **Forward**.

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

c. Enter the full-path filename and description of the Cisco IOS configuration file to be imported.

d. Click **Forward**.

e. Click **Select Relationships**.

f. Expand the Physical tree until the ConfigFiles folder is visible.

g. Select the folder and click **Apply**.

h. Click **Forward**.

i. Proceed to Step 5.

Step 5   Click **Finish**.

The user-supplied Cisco IOS configuration file is now stored in the ConfigurationFiles folder for the appropriate device object. Now, you can associate the file with a specific device in the network. See the "Task 5: Associating a Configuration File with a Device Object" section on page 2-23.

(Optional) Task 4: Importing a Configlet

Step 1   Copy the configlet that you want to import to a directory accessible from the Cisco EMF server where Cisco UGM is installed.

Step 2   From the Configlets folder in the NAS-File-Repository, select **Deployment > Import NAS File Object**.

The Deployment Wizard appears.

Step 3   In the Template Choices window, select **Store Configlet** and click **Forward**.

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

Step 5   Enter the full path to the filename and a description of the configlet to be imported.

Note   If you enter an incorrect path for the configlet, the import operation fails.

   If you leave the path field blank, an empty configlet is created. You can add content to the configlet by editing it later. See the "(Optional) Task 11: Viewing and Editing Configuration Files and Configlets" section on page 2-28.

Step 6   Click **Forward**.

Step 7   Click **Finish**.

Note   Configlet contents do not need begin and end statements.

   Cisco UGM does not check the contents of the configlet.

   The user-supplied configlet is now stored in the Configlets folder under the NAS-File-Repository. Now you can associate the configlet with one or more devices in the network. See the "(Optional) Task 6: Associating a Configlet with a Device Object" section on page 2-24

Cisco UGM Predefined Configlets

Note   The predefined configlets listed in Table 2-2 are examples. Modify them as necessary to work in your network environment.

Table 2-2   Predefined Configlets

Configlet Object Name	Configlet Content
AAA	aaa new-model
	aaa authentication login default none
	aaa authentication login h323 group radius
	aaa authentication login NONE none
	aaa authorization exec h323 group radius
	aaa accounting connection h323 start-stop group radius
	enable password test
BusyoutDS0	controller t1 <num>
	busyout ds0 <range>
CodecClass	voice class codec 88
	codec preference 1 g729br8 bytes 50
	codec preference 3 g729r8 bytes 50
	codec preference 5 g723ar53
	codec preference 6 g723ar63 bytes 144
	codec preference 7 g723r53
	codec preference 8 g723r63 bytes 120
	dial-peer voice 1000 voip
DTMFRelay	dial-peer voice 1000 voip
	dtmf-relay h245-alphanumeric h245-signal cisco-rtp
EnableT38	dial-peer voice 1000 voip
	fax protocol t38 ls-redundancy 5 hs-redundancy 0

Table 2-2   Predefined Configlets (continued)

Configlet Object Name	Configlet Content
IVR	call application voice debit tftp://ivrserver/tcl/debitcard.tcl
	call application voice debit warning-time 30
	call application voice debit language 1 en
	call application voice debit language 2 ch
	call application voice debit set-location en 0 tftp://ivrserver/au/en/
	call application voice debit set-location ch 0 tftp://ivrserver/au/ch
NTP	ntp clock-period 17178985
	ntp server 10.19.29.100
	ntp update-calendar
RadiusAccounting	radius-server host 2.10.6.26 auth-port 1645 acct-port 1646
	radius-server retransmit 3
	radius-server timeout 4
	radius-server deadtime 5
	radius-server key cisco
	radius-server vsa send accounting
	radius-server vsa send authentication
RadiusWithAAA	radius-server host 156.151.37.252 auth-port 1812 acct-port 1813
	radius-server retransmit 0
	radius-server key testing123
	radius-server vsa send accounting
	radius-server vsa send authentication

Table 2-2   Predefined Configlets (continued)

Configlet Object Name	Configlet Content
T1CAS	controller T1 0
	framing esf
	clock source line primary
	linecode b8zs
	ds0-group 0 timeslots 1-24 type e&m-immediate
T1PRI	isdn switch-type primary-5ess
	!
	controller T1 0
	framing esf
	clock source line primary
	linecode b8zs
	pri-group timeslots 1-24
	!
	interface Serial0:23
T1PRI (continued)	description Abacus ORIGINATING PRI#1
	no ip address
	ip mroute-cache
	isdn switch-type primary-5ess
	isdn tei-negotiation first-call
	isdn incoming-voice modem
	fair-queue 64 256 0
	no cdp enable

Table 2-2   Predefined Configlets (continued)

Configlet Object Name	Configlet Content
VOIPGatewayWithGatekeeper	interface FastEthernet0
	description rack subnet
	ip address 10.10.2.1 255.255.255.0
	duplex auto
	speed auto
	h323-gateway-voip interface
	h323-gateway-voip id ogk-zone1 ipaddr 10.10.2.201 1719 priority 1
	h323-gateway-voip id ogk-zone1 ipaddr 10.10.2.203 1719 priority 10
	h323-gateway-voip h323-id orig-gw1
	h323-gateway-voip tech-prefix 21#

Task 5: Associating a Configuration File with a Device Object

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

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

Step 1   In the Cisco UGM tree, from a container or device object choose **Configure Device > Associate Configuration File Object with Device**.

Step 2   From the Device list, select one of these device objects:

• **AS5300Chassis**

• **AS5350Chassis**

• **AS5400Chassis**

- **AS5800Chassis**

- **AS5850Chassis**

> **Note** If the selected device has a configuration file already associated with it, the name of the file appears in the Associated with Config File field.

Step 3   From the Configuration File list, select the file (corresponding to your selected devices) to associate with the selected device. This is a Cisco IOS configuration file with prespecified parameters.

Step 4   Click **Save Association**.

The Associated with Config File field is updated to reflect the new configuration file association.

In the Map Viewer, the associated configuration file has _current added to the filename.

For example, if the filename (before association) was autoGenerated_2001_04_06_13_28_50, the same file (after association) appears in the Map Viewer as autoGenerated_2001_04_06_13_28_50_current.

A device can be associated with only one configuration file at a time. The current association always erases the previous association.

(Optional) Task 6: Associating a Configlet with a Device Object

You must associate a configlet with a device object before you can download it to the device.

> **Note** You can associate the same configlet with multiple devices in the same operation, however, a device can be associated with only one configlet at a time.

Step 1   In the Cisco UGM tree, from a container or device object choose **Configure Device > Associate Configlet Object with Device**.

Step 2   From the Device list, select one or more of these device objects:

- **AS5300Chassis**
- **AS5350Chassis**
- **AS5400Chassis**
- **AS5800Chassis**
- **AS5850Chassis**

Note   If the selected device has a configlet already associated with it, the name of the configlet appears in the Associated with Configlet field.

Step 3   From the Configlet list, select the configlet to associate with the selected device. This is a file that consists of Cisco IOS CLI commands.

Step 4   Click **Save Association**.

The Associated with Configlet field is updated to reflect the new configlet association.

In the Map Viewer, configlet names do not change after association with a device object. To check a configlet association, access the Associate Configlet Object with Device dialog box.

Task 7: Sending a Configuration File from the Cisco UGM Server to the Startup File of a Device Object

You can download a configuration file from the Cisco UGM server to a managed device by clicking **Send Configuration to Startup** in the 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.
- With **Send Configuration to Startup**, you can download the same configuration file to multiple devices.

If you are downloading a configuration file to several devices, first check that all the selected devices are of the same type, and then associate the configuration file with each individual device.

Step 1   From a container or device object choose **Configure Device > Perform IOS Operations.**

Step 2   Select **Yes** or **No** to specify if the device should be rebooted after a configuration is downloaded.

The default is **No** (no reload).

Step 3   Click **Save**.

Step 4   Select the devices from the list in the left panel and click **Send Configuration to Startup**.

The Action Result window shows the success of the operation.

If you selected the Reload After Config Download option, the device reboots. (See the "Task 2: Selecting a Reload Option After a Configuration Download" section on page 2-5.)

(Optional) Task 8: Sending a Configlet to the Running Configuration File

You can download a configlet from the Cisco UGM server to one or more managed devices by clicking **Send Configlet to Running** in the 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 configlet.

- The **Send Configlet to Running** operation can be performed on multiple devices.

If you are installing a configlet on several managed devices, first check that all the selected devices are of the same type, and then associate the configlet with the devices.

Step 1   From a container or device object, choose **Configure Device > Perform IOS Operations.**

Step 2   Select the devices from the list in the left panel and click **Send Configlet to Running**.

The Action Result window shows the success of the operation.

Note   In order to save the configlets and current configuration, click Copy Running to Startup. See the "(Optional) Task 10: Copying the Running Configuration to the Startup Configuration File" section on page 2-28.

(Optional) Task 9: Uploading the Device Startup Configuration File to the Cisco UGM Server

You can upload a startup configuration file (from a managed device) to the Cisco UGM server by clicking **Get Startup Configuration** in the IOS Operations dialog box.

- This is a real time operation that cannot be scheduled to run at a future time.

- The managed device must be in the normal state before you can start the uploading process.

- The **Get Startup Configuration** operation can be performed on multiple devices.

- The configuration file object is created in the ConfigurationFiles folder under the corresponding chassis in the Physical view.

- The configuration file object name assigned is startup_*timestamp* where *timestamp* has the following format:

  year_month_day_hour_minute_second

  Example: startup_2001_04_26_13_28_50

Step 1   From a container or device object, choose **Configure Device > Get startup Configuration**.

Step 2 Select the devices from the list in the left panel and click **Get startup Configuration**.

The Action Result window shows the success of the operation.

(Optional) Task 10: Copying the Running Configuration to the Startup Configuration File

You can copy the running configuration file (from a managed device) to its startup configuration file by clicking **Copy Running to Startup** in the IOS Operations dialog box.

- This is a real time operation that cannot be scheduled to run at a future time.
- The managed device must be in the normal state before you can start the copy process.
- The **Copy Running to Startup** operation can be performed on multiple devices.

Step 1 From a container or device object, choose **Configure Device > Perform IOS Operations.**

Step 2 Select the devices from the list in the left panel and click **Copy Running to Startup**.

The Action Result window shows the success of the operation.

(Optional) Task 11: Viewing and Editing Configuration Files and Configlets

You can use this procedure to create a configlet. If you imported an empty configlet earlier (see "(Optional) Task 4: Importing a Configlet" section on page 2-18), you can now view the empty configlet and create content for it.

Step 1   From the Map Viewer, select a configuration file or configlet object to view or edit.

Step 2   Choose **Edit Configuration File** or **Edit Configlet**.

The description and content of the file appears. The text can be edited directly in the dialog box.

Step 3   Click **Save**.

The revised configuration file or configlet is saved under the original filename.

Managing Images and Scheduling Actions with Cisco UGM

This chapter contains the following sections:

Overview of Managing Images

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 AS5300, AS5350, AS5400, AS5800, and AS5850:

Table 3-1   Image Management Actions and the Devices Where They Are Supported

	AS5300	AS5350	AS5400	AS5800	AS5850	State Change	Can Be Scheduled
Reload	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade IOS Image	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade Modem Image	Yes	N/A	N/A	Yes	N/A	Yes	Yes
Upgrade SPE Image	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade VFC Image	Yes	N/A	N/A	N/A[1]	N/A	Yes	Yes

1. For Cisco AS5800 devices, the VFC image is always bundled with the Cisco IOS image.

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

Note Cisco IOS image operations do not cause a state change in the managed device, and cannot be scheduled.

Task 1: Authenticating the Device Object

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

Step 1 From a container or device object to be configured, select **Configure Device > Open Device Authentication Information**.

Step 2 Enter the Login User Name as configured on the device.

Step 3 Enter a Login Password.

Note If the device has vty line password configured, enter the vty line password for the Login Password.

Step 4 Enter an Enable password.

Step 5 Enter the Operation Timeout value in seconds. The default value is 240 seconds.

You can change this value located at:

```
IOSConfigCtrlUserData.ini
attrValueOpTimeout=n
```

Step 6 Enter the Prompt Timeout value in seconds. The default value is 10 seconds.

You can change this value located at:

```
IOSConfigCtrlUserData.ini
attrValuePromptTimeout=n
```

> **Note** Enter values in all the fields in this dialog box. If you do not enter these values, the following commands will fail:
> Show CLI
> Configure Administrative State
> All actions on the IOS Operations dialog.

Step 7   Enter a user name.

Step 8   Enter a user password.

Step 9   Click **Save**.

Task 2: Selecting Upgrade, Reload, and TFTP Host Options

You can download images by using the Trivial File Transfer Protocol (TFTP) that downloads the image from the Cisco UGM server to the Flash memory on the device.

You can also download the image from the Cisco UGM server to a managed device (on a WAN), and then download the image from that device to the other managed devices in the network (on a LAN).

Step 1   Choose **AS5***xxx* **> Configure Device > Perform IOS Operations.**

Step 2   Under Options, select an SPE Upgrade Method:

- **busyout**—Prevents idle modems from accepting calls, but allows completion of any calls in progress. When the call is complete, the modem moves to the busyout state and does not accept any new calls. When all the modems on a card are in the busyout state, the firmware is upgraded on the card, and the card (and modems) move to the normal state.

  A card does not move to the busyout state if even one of its modems is processing a call. This can prevent the firmware upgrade. You can terminate calls by using the Cisco IOS **clear** command.

- **reboot**—The managed device is rebooted, and the firmware is immediately upgraded.

- **download-maintenance**—The firmware image is upgraded only when the managed device is taken offline for maintenance.

   You can schedule download-maintenance windows by using Cisco IOS commands. When you select the download-maintenance option for firmware upgrade, the modems run the old firmware until Cisco UGM enters the scheduled maintenance window. During this scheduled maintenance, any calls in progress are dropped. When the firmware upgrade is complete, the modems resume call processing by using the new firmware.

- **recovery**—The firmware upgrade is delayed until recovery maintenance time.

Step 3   Select a Modem Upgrade Method:

- **busyout**

- **reboot**

- **download-maintenance**

- **recovery**

These methods are described in Step 2 of this procedure.

Note   You can select the firmware upgrade here or in the Build Configuration File from Default 5xxx Template dialog box (see the "Entering Modem and SPE Parameters (SPE and Modem Tabs)" section on page 2-13).

You set the same Cisco UGM variable when you select the firmware upgrade from either location.

Step 4   Select an option for Reload After IOS Image Upgrade.

- **Yes**—The managed device reboots immediately after the Upgrade IOS Image operation.

- **No**—The managed device does not reboot immediately after the Upgrade IOS Image operation. Click **Reload** to schedule the reboot.

> **Note** Even though you can perform the Reload operation on multiple devices, do not reload more than three devices at a time.
>
> Because you can schedule reloads, Cisco recommends that you schedule up to three devices to be reloaded at time A; then, schedule the next group (up to three devices) at time A+30 minutes, and follow the same sequence with the remaining devices.

Step 5 Select an option for Reload After VFC Image Upgrade.

- **Yes**—The managed device reboots immediately after the Upgrade VFC Image operation.

- **No**—The managed device does not reboot immediately after the Upgrade VFC Image operation. Click **Reload** to schedule the reboot.

  See Note in Step 4.

Step 6 Specify if you will use a TFTP host.

- **Yes**—Indicates that selected managed devices will use the associated NAS as a TFTP server for image upgrades. (See the "Task 4: Option 3: Associating a NAS TFTP Server with a Device" section on page 3-12.)

- **No**—Indicates that upgraded images will be downloaded from the Cisco UGM server. (This is the default value.)

Step 7 Click **Save**.

Task 3: Option 1: Importing a Non-AS5800 Image File into the NAS-File-Repository

⚠️

Caution   Cisco UGM does not check the integrity of the type of image selected. In other words, it does not check if the modem image file imported is indeed a modem image.

Cisco UGM only checks if the imported file is in binary format. If the file is in ASCII format, the import fails.

⚠️

Caution   Cisco UGM does not check for compatibility between the Cisco IOS image and firmware (modem and SPE) image installed on a device.

Before installing images on your managed devices, check if they are compatible by contacting the Cisco Technical Assistance Center.

Step 1   From the AS5xxxImages folder in the NAS-File-Repository, choose **Deployment > Import NAS File Object**.

The Deployment Wizard appears.

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

- **Store AS5300 Image File**
- **Store AS5350 Image File**
- **Store AS5400 Image File**
- **Store AS5850 Image File**
- **Store Modem Image File**
- **Store SPE Image File**
- **Store VFC Image File**

To import an image file for the AS5800, see the "Task 3: Option 2: Importing an AS5800 Image File into the NAS-File-Repository" section on page 3-8.

Step 3   Click **Forward**.

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

Step 5   Enter the path, filename, and description of the image file that you want to import into the NAS-File-Repository.

Note   If you enter an incorrect filename or path for the image file, the import fails.

If you do not enter a path, the import operation fails.

Step 6   Click **Forward**.

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

The user-supplied image file is now stored in the /tftpdir directory on the Cisco UGM server, and appears in the appropriate folder (AS5300Images, AS5350Images, AS5400Images, AS5800Images, AS5850Images, ModemImages, SPEImages, or VFCImages) under the NAS-File-Repository object. Now you can associate it with a specific device in the network.

Task 3: Option 2: Importing an AS5800 Image File into the NAS-File-Repository

Caution   Cisco UGM does not check for compatibility between the Cisco IOS image and firmware (modem and SPE) image installed on a device.

Before installing images on your managed devices, check if they are compatible by contacting the Cisco Technical Assistance Center.

Step 1   From the AS5800Images folder in the NAS-File-Repository, choose **Deployment > Import NAS File Object**.

The Deployment Wizard appears.

Step 2   In the Template Choices window, select **Store AS5800 Image File.**

To import an image file for any of the other managed devices, see the "Task 3: Option 1: Importing a Non-AS5800 Image File into the NAS-File-Repository" section on page 3-7.

Step 3   Click **Forward**.

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

Step 5   Enter the complete path and the filename of the router shelf image.

Step 6   Enter the complete path and the filename of the dial shelf image.

Note   If you enter an incorrect complete path and filename for either image file, the import fails.

Cisco UGM checks if the image file is a binary file; if it is not binary, the import fails.

Caution   The router shelf and the dial shelf must both run images from the same Cisco IOS version. If you upgrade one image, the other must be upgraded as well.

Step 7   Enter the description of the image file.

Step 8   Click **Forward**.

Step 9   View the summary dialog box. If this is correct, click **Finish**.

The user-supplied image files are now stored in the AS5800Images folder in the NAS-File-Repository view.

Task 4: Option 1: Associating a Cisco IOS Image with a Device Object

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

Step 1 From a container or device object, choose **Configure Device > Associate IOS Image File Object with Devices**.

Step 2 In the Associate Image File Object with Devices dialog box, select a device object.

If you select multiple devices, make sure that they are all of the same type: all Cisco AS5300, AS5350, AS5400, AS5800, or AS5850 devices.

Step 3 From the Image File Category, select the correct group of images for the device.

Note Cisco UGM checks for a match between the device and the Image File Category that you selected. If you select an incorrect group of images for the device, the association fails at Step 6.

Caution Cisco UGM does not check for compatibility between the Cisco IOS image and firmware (modem and SPE) image installed on a device.

Before installing images on your managed devices, check if they are compatible by contacting the Cisco Technical Assistance Center.

Step 4 Select the image file to associate with the device object.

Step 5 Enter a description for the selected Cisco IOS image file.

Step 6 Click **Save Association**.

The Image field in the Device panel is updated to reflect the new Cisco IOS image file association.

The Map Viewer does not indicate which Cisco IOS image is associated with a device. To check this association, access the Associate Image File Object with Devices dialog box.

You can now proceed to the ""Task 5: Option 2: Downloading a Modem Image" section on page 3-17" section on page 3-14.

Task 4: Option 2: Associating a Firmware Image with a Device Object

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

- You can associate Cisco IOS images with all Cisco UGM-supported devices.

- You can associate Modem images with Cisco AS5300 and AS5800 devices.

- You can associate SPE images with Cisco AS5350, AS5400, AS5800, and AS5850 devices.

- You can associate VFC images with Cisco AS5300 devices.

Step 1 From a container or device object, choose **Configure Device > Associate Firmware File Object with Devices**.

Step 2 In the Associate Firmware File Object with Devices dialog box, select a device object.

If you select multiple devices, make sure that they are all of the same type: all Cisco AS5300, AS5350, AS5400, AS5800, or AS5850 devices.

Step 3 From the Firmware File Category, select the type of image that you want to install on the device.

Note Cisco UGM checks for a match between the device and the Firmware File Category that you selected. If you select an incorrect group of firmware images for the device, the association fails at Step 6.

⚠️

Caution   Cisco UGM does not check for compatibility between the Cisco IOS image
and firmware image installed on a device.

Before installing images on your managed devices, check that they are
compatible by contacting the Cisco Technical Assistance Center.

Step 4   Select the firmware file to associate with the device object.

Step 5   Enter a description for the firmware file.

Step 6   Click **Save Association**.

The SPE File, Modem File, or VFC File field in the Associated With panel is
updated to reflect the new firmware image file association.

The Map Viewer does not indicate which firmware image is associated with a
device. To check this association, access the Associate Firmware File Object with
Devices dialog box.

Task 4: Option 3: Associating a NAS TFTP Server with a Device

To download upgraded images from one managed device to other managed
devices, you must associate a NAS TFTP server with the devices.

✎

Note   Make sure that the device that acts as a TFTP server has been configured to do
so by using configlets, building a configuration file, or Cisco IOS commands.

For details on the Cisco IOS commands, refer to the *Cisco IOS Release 12.0
Configuration Fundamentals Configuration Guide*. (Chapter: File
Management, Section: Configuring Additional File Transfer Functions.)

Step 1   From a container or device object, choose **Configure Device > Open Associate
NAS TFTP Server with Device**.

Step 2   In the Associate NAS TFTP Server with Device dialog box, from the list on the
left, select one or more device objects.

Step 3   From the list on the right, select one device that functions as the TFTP server. The upgraded image will be downloaded from this device to the other devices.

Step 4   Click **Save Association**.

Step 5   Check that the correct TFTP server path appears in the Associated With window.

You can now proceed to one of these options:

Task 5: Option 1: Downloading a Cisco IOS Image

You can schedule an image download to a device for a later date or 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 the scheduled action object from the ScheduledActions view.

See the "(Optional) Task 6: Viewing or Cancelling Scheduled Actions" section on page 3-23.

- The target devices must be in a normal state before you can download a Cisco IOS image to a device.

- You can perform the Upgrade IOS Image operation on multiple devices.

- The Cisco IOS image that you send to a target device must be smaller than the available Flash space on that device or the transfer fails.

Note Check available Flash space before you download a Cisco IOS image. Cisco UGM does not perform this check.

- More than one Cisco IOS image can reside on the device if there is adequate Flash space.

- Before downloading the Cisco IOS image (with the Reload option) to a Cisco AS5800 device:

  – Check that the Flash on the router shelf can accommodate the new Cisco IOS image for the router shelf.

  – Check that the boot Flash and Flash on the dial shelf are empty.

  – Check that there is no boot command in the dial shelf configuration file.

- Cisco AS5800 devices consist of a router shelf and a dial shelf. These components run the same Cisco IOS image version. One Cisco UGM AS5800 image object represents two component images (router shelf and dial shelf). If you want to upgrade one component image, you must upgrade the other as well.

  The router shelf image is copied to the Flash memory on the router shelf, and the dial shelf image is copied to the boot Flash memory on the dial shelf.

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

Changes in Device State During a Cisco IOS Image Upgrade

- The device must be in a normal state when you start the upgrade procedure.

- If the device is not reloaded, it transitions from normal > IOSImageDownload > IOSImageUpgrade > normal.

- If the device is reloaded, it transitions from normal > IOSImageDownload > IOSImageUpgrade > reload > normal.

- A Cisco AS5800 device (without reloading) transitions from normal > IOSImageDownloadToRouter > IOSImageDownloadToDial > IOSImageUpgrade > normal.

- A Cisco AS5800 device (with reloading) transitions from normal > IOSImageDownloadToRouter > IOSImageDownloadToDial > IOSImageUpgrade > reload > normal.

Note   Even if the image upgrade fails, the device returns to the normal state. (This is because the normal state indicates connectivity only.) An alarm is raised.

Check the progress window to see if the image upgrade was successful, or check the Event Browser for details on the alarm.

Step 1   Check the Cisco IOS image file associated with the device object. (See the "Task 4: Option 1: Associating a Cisco IOS Image with a Device Object" section on page 3-10.)

Step 2   From a container or device object, choose **Configure Device > Perform IOS Operations**.

Step 3   Select the devices from the list in the left panel and click **Upgrade IOS Image**.

If you selected more than one device, each device is upgraded with its associated image. The device reboots if you selected the Reload After IOS Image Download option. (See the "Task 2: Selecting Upgrade, Reload, and TFTP Host Options" section on page 3-4.)

Note   If you used a TFTP server to download the image, be aware that the files in the /tftpdir directory are not erased with the Cisco EMF reset command.

When you reset Cisco EMF, go into the /tftpdir directory and delete all files with a series of numbers as the filename. (Example: 545648).

Troubleshooting Alarms Generated During a Cisco IOS Image Upgrade

UpgradeIOSImageFailed

This major alarm is raised against the device when the Cisco IOS image upgrade fails. Some of the reasons for this occurrence:

-   Inadequate Flash memory on the device.
-   Cisco UGM lost connectivity to the device.

The device returns to the normal state.

UpgradeIOSImageInterrupted

This major alarm is raised against the device when the Cisco IOS image upgrade is interrupted because the ASMainCtrl process crashed or stopped.

The alarm is raised when the ASMainCtrl process restarts. The device returns to the normal state.

Task 5: Option 2: Downloading a Modem Image

> **Note** Modem images are upgraded on MICA cards in Cisco AS5300 and AS5800 devices only.

You can schedule an image download to a device for a later date or 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 the scheduled action object from the ScheduledActions view.

See the "(Optional) Task 6: Viewing or Cancelling Scheduled Actions" section on page 3-23.

- The target devices must be in normal state before you can download a modem image.
- You can perform the Upgrade Modem Image operation on multiple devices.
- 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 fails.
- 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 affects all modems on the device.

You can press the Upgrade Modem Image button in the Performing IOS Operations dialog to download an associated image file from the Cisco UGM server to a managed device.

Changes in Device State During a Modem Image Upgrade

- The device must be in a normal state when you start the upgrade procedure.
- The device transitions from normal > ModemImageDownload > ModemImageUpgrade > normal.

Note Even if the image upgrade fails, the device returns to the normal state. (This is because the normal state indicates connectivity only.) An alarm is raised.

Check the progress window to see if the image upgrade was successful, or check the Event Browser for details on alarms.

Step 1 Check that the modem image file is associated with the device object. (See the "Task 4: Option 2: Associating a Firmware Image with a Device Object" section on page 3-11.)

Step 2 From a container or device object, choose **Configure Device > Perform IOS Operations**.

Step 3 Select the devices from the list in the left panel and click **Upgrade Modem Image**.

If you selected more than one device, each device is upgraded with its associated image. The device reboots in keeping with the Modem Upgrade Method you selected. (See the "Task 2: Selecting Upgrade, Reload, and TFTP Host Options" section on page 3-4.)

Note If you used a TFTP server to download the image, the files in the /tftpdir directory are not erased, even with the Cisco EMF reset command.

When you reset Cisco EMF, go into the /tftpdir directory and delete all files with a series of numbers as the filename. (Example: 545648).

Troubleshooting Alarms Generated During a Modem Image Upgrade

UpgradeModemImageFailed

This major alarm is raised against the device when the modem image upgrade fails. Some of the reasons for this occurrence:

- Inadequate Flash memory on the device.
- Cisco UGM lost connectivity to the device.

The device returns to the normal state.

UpgradeModemImageInterrupted

This major alarm is raised against the device when the modem image upgrade is interrupted because the ASMainCtrl process crashed or stopped.

The alarm is raised when the ASMainCtrl process restarts. The device is returned to the normal state.

Task 5: Option 3: Downloading an SPE Image

You can schedule an image download to a device for a later date or 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 the scheduled action object from the ScheduledActions view.

- The target devices must be in normal state before you can download SPE images.
- You can perform the Upgrade SPE Image operation on multiple devices.
- The SPE image that you send to a target device must be smaller that the available Flash space on that device, or the transfer fails.
- 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 affects all SPEs on the device.

Changes in Device State During an SPE Image Upgrade

- The device must be in a normal state when you start the upgrade procedure.

- The device transitions from normal > SPEImageDownload > SPEImageUpgrade > normal.

Note   Even if the image upgrade fails, the device returns to the normal state. (This is because the normal state indicates connectivity only.) An alarm is raised.

Check the progress window to see if the image upgrade was successful, or check the Event Browser for details on alarms.

Step 1   Check that the SPE image file is associated with the device object. (See the "Task 4: Option 2: Associating a Firmware Image with a Device Object" section on page 3-11.)

Step 2   From a container or device object, choose **Configure Device > Perform IOS Operations**.

Step 3   Select the devices from the list in the left panel and click **Upgrade SPE Image**.

If you selected more than one device, each device is upgraded with its associated image. The device reboots in keeping with the SPE Upgrade Method that you selected. (See the "Task 2: Selecting Upgrade, Reload, and TFTP Host Options" section on page 3-4.)

Note   If you used a TFTP server to download the image, the files in the /tftpdir directory are not erased, even with the Cisco EMF reset command.

When you reset Cisco EMF, go into the /tftpdir directory and delete all files with a series of numbers as the filename. (Example: 545648).

Troubleshooting Alarms Generated During an SPE Image Upgrade

UpgradeSPEImageFailed

This major alarm is raised against the device when the SPE image upgrade fails. See the following reasons for this occurrence:

- Inadequate Flash memory on the device.
- Cisco UGM lost connectivity to the device.

The device is returned to the normal state.

UpgradeSPEImageInterrupted

This major alarm is raised against the device when the SPE image upgrade is interrupted because the ASMainCtrl process crashed or stopped.

The alarm is raised when the ASMainCtrl process restarts. The device returns to the normal state.

Task 5: Option 4: Downloading a VFC Image

For details on VFC image upgrade, see the *Upgrading Cisco AS5300 Voice-over-IP Feature Card VCWare* document available on Cisco.com.

You can schedule an image download to a device for a later date or 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 the scheduled action object from the ScheduledActions view.

See the "(Optional) Task 6: Viewing or Cancelling Scheduled Actions" section on page 3-23.

- The target devices must be in normal state before you can download VFC images.
- The Upgrade VFC Image operation can be performed on multiple devices.
- The VFC 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 VFC image can reside on the device if there is adequate Flash space.

Changes in Device State During a VFC Image Upgrade

- The device must be in a normal state when you start the upgrade procedure.

- The device transitions from normal > VFCImageDownload > VFCImageUpgrade > normal.

Note   Even if the image upgrade fails, the device returns to the normal state. (This is because the normal state indicates connectivity only.)

Check the progress window to see if the image upgrade was successful.

Step 1   Check that the VFC image file is associated with the device object. (See the "Task 4: Option 2: Associating a Firmware Image with a Device Object" section on page 3-11.)

Step 2   From a container or device object, choose **Configure Device > Perform IOS Operations**.

Step 3   Select the devices from the list in the left panel and click **Upgrade VFC Image**.

If you selected more than one device, each device is upgraded with its associated image. The device reboots in keeping with the VFC Upgrade Method you selected. (See the "Task 2: Selecting Upgrade, Reload, and TFTP Host Options" section on page 3-4.)

Note   If you used a TFTP server to download the image, the files in the /tftpdir directory are not erased, even with the Cisco EMF reset command.

When you reset Cisco EMF, go into the /tftpdir directory and delete all files with a series of numbers as the filename. (Example: 545648).

Troubleshooting Alarms Generated during a VFC Image Upgrade

UpgradeVFCImageFailed

This major alarm is raised against the device when the VFC image upgrade fails. See the following reasons for this occurrence:

- Inadequate Flash memory on the device.
- Cisco UGM lost connectivity to the device.

The device returns to the normal state.

UpgradeVFCImageInterrupted

This major alarm is raised against the device when the VFC image upgrade is interrupted because the ASMainCtrl process crashed or stopped.

The alarm is raised when the ASMainCtrl process restarts. The device returns to the normal state.

(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 not deleted automatically after the action is completed, but its result is updated. You must manually delete the scheduled action object.

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

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

Step 1   To view the scheduled but unexecuted image installations, expand the Scheduled Actions root node in the Map Viewer .

The scheduled operations are labeled by type (Cisco 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, page 4-1

Overview of Configuring Administrative States

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

- Shutdown 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 box 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 That 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 modem, SPE, VFC, and Carrier cards, the device, and DS0 channels.

About the Graceful Shutdown Function

Before performing this function, set up authentication values for the device. (See the "Task 1: Authenticating the Device Object" section on page 2-4.)

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

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.

An Action Report appears at the end of a Graceful Shutdown and shows the results of the action.

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

For details, see the "Objects That Support Administrative State Configuration" section on page 4-2.

Object State Transitions During the Graceful Shutdown Action

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.

About the Accept Traffic Function

Note   When you accept traffic, 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."

Note If you perform a Graceful Shutdown action on a Cisco AS5350 or AS5400 device, you cannot enter the Accept Traffic command.

For details, see the "Configuring the Administrative State for a Supported Object" section on page 4-5.

Object State Transitions During the Accept Traffic Action

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 Configure Administrative State dialog box.

Note The Configure Administrative State option (and Accept Traffic) is available only for some Cisco UGM objects. For details, see the "Objects That Support Administrative State Configuration" section on page 4-2.

About Processing Times for Configuring Administrative States

This section describes processing times associated with Configure Administrative State actions:

• The dialog box fields are updated every 10 seconds.

• After you click Accept Traffic, allow approximately 60 seconds for the card to start.

• 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 tree (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.
- When a Configure Administrative State action is being executed on one managed device, you cannot initiate a Configure Administrative State action on another managed device.
- If you perform a Graceful Shutdown action on a Cisco AS5350 or AS5400 device, you cannot enter the Accept Traffic command because 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>* Cisco IOS command to the device.

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

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 components:

- 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 or a set of users identified by a name 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.

Preset Cisco UGM Feature Lists and Access Specifications

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

Table 5-1   Cisco UGM Preset 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.
UGM_ASMainEM_PerformancePollingConfig	Performance polling configuration and start/stop dialog boxes.
UGM_ASMainEM_Provision_AccessServers	Manual deployment of access servers dialog boxes.
UGM_ASMainEM_TrapForwarding	All trap forwarding configuration dialog boxes.
UGM_ASMainEM_Redundancy_Features	All redundancy feature dialog boxes.
UGM_ASMainEMLaunchTelnetSession	Capability to start a Telnet session.
UGM_LaunchCiscoView	CiscoView application start dialog boxes.
IOSConfigEMDialogFeatureList	Cisco IOS configuration dialog boxes.
IOSConfigEMProvisioningFeatureList	File import dialog boxes.

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

Table 5-2   Cisco UGM Preset 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_ASMainEM_LaunchTelnetSession	Read-Write-Admin	UGM_ASMainEMLaunchTelnetSession
UGM_LaunchCiscoView	Read	UGM_LaunchCiscoView
IOSConfigEM	Read-Write-Admin	IOSConfigEMDialogFeatureList
		IOSConfigEMProvisioningFeatureList

Table 5-3   Cisco UGM Features with Associated Permissions

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

Table 5-3   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
ASMainEMAS5800ChassisOpenRedundancyStatusService	Read
ASMainEMAS5850ChassisOpenRedStatusAndConfigService	Read
ASMainEMASGenericRedContainerOpenAccessServerChassisService	Read
ASMainEMASGenericRedContainerOpenRedundancyPropertiesService	Read
ASMainEMAS5800RedContainerOpenRedundancyStatusService	Read
ASMainEMAS5850RedContainerOpenRedStatusAndConfigService	Read
ASMainEMAS5300ChassisOpenShow5300Service	Read-Write
ASMainEMAS5800RedContainerOpenShow5800Service	Read-Write
ASMainEMAS5850RedContainerOpenShow5850Service	Read-Write
ASMainEMASGenericRedContainerOpenChassisCommissioningService	Read-Write
ASMainEMContainerOpenShow5300Service	Read-Write
ProvisionASMainEMASTrapForward	Read-Write
ASMainEMASCT3CardOpenDS3PropertiesService	Read

Table 5-3   Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
ASMainEMASGenericCardOpenCardPropertiesService	Read
ASMainEMASVFCCardOpenVFCProperties Service	Read
ASMainEMASVFCCardOpenDSPPropertiesService	Read
ASMainEMASDSPOpenDSPPropertiesService	Read
ASMainEMASDS1E1OpenChannelStatisticsService	Read
ASMainEMASEMSOpenEMSAboutService	Read
ASMainEMASEMSOpenEMSSettingsService	Read-Write
ASMainEMContainerOpenStartStopPerfPollingService	Read-Write
ASMainEMASDS1E1OpenDs1e1propertiesService	Read
ASMainEMASPerPollConfigOpenStartStopPerfPollingService	Read-Write
ASMainEMASPerPollConfigOpenGlobalPerfPollConfigService	Read-Write
ASMainEMASGenericNetworkIfOpenEthernetPortService	Read
ASMainEMASGenericChassisOpenModemUniversalPortService	Read
ASMainEMContainerOpenChassisCommissioningService	Read-Write
ASMainEMASModemCardOpenModemUniversalPortService	Read
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

Table 5-3   Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
ASMainEMASGenericRedContainerOpenStartStopPerfPollingService	Read-Write
ASMainEMContainerOpenPerfPollBulkConfigService	Read-Write
ASMainEMASGenericChassisOpenPerfPollBulkConfigService	Read-Write
ASMainEMASGenericRedContainerOpenPerfPollBulkConfigService	Read-Write
ASMainEMASBulkFileFtpConfigOpenBulkFileFtpConfigService	Read-Write
ASMainEMTelnetSessionService	Read-Write
IOSConfigEMugmCtrlLoggingOpenIOSConfigCtrlLoggingLevelConfigurationService	Read-Write
IOSConfigEMLoggingConfigurationOpenIOSConfigCtrlLoggingLevelConfigurationService	Read-Write
IOSConfigEMContainerOpenBuildConfigFileFrom5300TemplateService	Read-Write
IOSConfigEMContainerOpenBuildConfigFileFrom5350TemplateService	Read-Write
IOSConfigEMContainerOpenBuildConfigFileFrom5400TemplateService	Read-Write
IOSConfigEMContainerOpenBuildConfigFileFrom5800TemplateService	Read-Write
IOSConfigEMContainerOpenBuildConfigFileFrom5850TemplateService	Read-Write
IOSConfigEMContainerOpenAssociateConfigFileWithDeviceService	Read-Write
IOSConfigEMContainerOpenAssociateImageFileWithDeviceService	Read-Write
IOSConfigEMContainerOpenAssociateFirmwareFileWithDeviceService	Read-Write
IOSConfigEMContainerOpenDeviceAuthenticationService	Read-Write
IOSConfigEMContainerOpenIOSOperationsService	Read-Write
IOSConfigEMIOS5300ConfigParamOpenBuildConfigFileFrom5300TemplateService	Read-Write
IOSConfigEMIOS5350ConfigParamOpenBuildConfigFileFrom5300TemplateService	Read-Write
IOSConfigEMIOS5400ConfigParamOpenBuildConfigFileFrom5300TemplateService	Read-Write
IOSConfigEMIOS5800ConfigParamOpenBuildConfigFileFrom5300TemplateService	Read-Write

Table 5-3   Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
IOSConfigEMIOS5850ConfigParamOpenBuildConfigFileFrom5300TemplateService	Read-Write
IOSConfigEMCiscoTechObjOpenAssociateConfigFileWithDeviceService	Read-Write
IOSConfigEMCiscoTechObjOpenAssociateImageFileWithDeviceService	Read-Write
IOSConfigEMCiscoTechObjOpenAssociateFirmwareFileWithDeviceService	Read-Write
IOSConfigEMCiscoTechObjOpenDeviceAuthenticationService	Read-Write
IOSConfigEMIOSTechObjOpenIOSOperationsService	Read-Write
IOSConfigEMConfigFileCategoryOpenEditConfigFileService	Read-Write
IOSConfigEMConfigFileVersionOpenEditConfigFileService	Read-Write
IOSConfigEMIOSScheduledActionOpenScheduledActionPropertiesService	Read-Write
IOSConfigEMScheduledActionsOpenScheduledActionPropertiesService	Read-Write
IOSConfigEMCiscoTechObjOpenAssociateNASTftpWithDeviceService	Read-Write
IOSConfigEMCiscoTechObjOpenAssociateConfigletWithDeviceService	Read-Write
IOSConfigEMConfigletCategoryOpenEditConfigletService	Read-Write
IOSConfigEMConfigletVersionOpenEditConfigletService	Read-Write
IOSConfigEMContainerOpenAssociateNASTftpWithDeviceService	Read-Write
IOSConfigEMContainerOpenAssociateConfigletWithDeviceService	Read-Write
IOSConfigEMugmFileVersionDeleteService	Read-Write
IOSConfigEMIOSScheduledActionDeleteService	Read-Write
IOSConfigEMugmCtrlLoggingOpenObjectConfigService	Read-Write
IOSConfigEMugmFileCategoryOpenObjectConfigService	Read-Write
IOSConfigEMugmFileVersionOpenObjectConfigService	Read-Write
IOSConfigEMIOSScheduledActionOpenObjectConfigService	Read-Write
ProvisionIOSConfigEMContainer	Read-Write
ProvisionIOSConfigEMIOS5300ImageFileCategory	Read-Write
ProvisionIOSConfigEMConfigFileCategory	Read-Write

Table 5-3   Cisco UGM Features with Associated Permissions (continued)

Feature	Permission
ProvisionIOSConfigEMIOS5400ImageFileCategory	Read-Write
ProvisionIOSConfigEMDSPFileCategory	Read-Write
ProvisionIOSConfigEMSPEFileCategory	Read-Write
ProvisionIOSConfigEMIOS5800ImageFileCategory	Read-Write
ProvisionIOSConfigEMIOS5350ImageFileCategory	Read-Write
ProvisionIOSConfigEMConfigletCategory	Read-Write
ProvisionIOSConfigEMNAS-File_Repository	Read-Write
ProvisionIOSConfigEMIOS5850ImageFileCategory	Read-Write
ProvisionIOSConfigEMModemFileCategory	Read-Write
ProvisionIOSConfigEMciscoTechObj	Read-Write
CiscoViewService	Read

Creating an Access Specification

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

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

Step 1   From the Launchpad, click **Access** to start the Access Manager.

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 a User

> **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 a User, a User Group, and an Access Specification

Tip   Only a system administrator can modify an Access Manager User, a 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.

■ **Preset Cisco UGM Feature Lists and Access Specifications**

C H A P T E R **6**

Managing the Performance of Cisco UGM-Controlled Devices

This chapter contains the following sections:

Overview of Performance Management Features

Note With Cisco UGM, you can select frequency of data polling and SNMP trap forwarding destinations. When making these selections, consider the number of managed ports and devices in your network, and be aware that your selections affect system performance and scalability.

With the Performance Manager, you can:

- Collect selected performance attributes at specific times.

- Store SNMP-polled performance attributes in the database of the attribute history server.

- Enable or disable data collection (by device) at specified intervals.

- View SNMP-polled performance data (stored in the attribute history server) by using the Performance Manager.

- Performance polling is carried out only on devices in the normal (commissioned) state. Performance polling is not affected by the state of device components.

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

  For example, if you specify 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 predefined performance attributes. You cannot modify or add attributes.

Overview of SNMP Polling

This section contains the following:

- About Adding SNMP MIB Attributes to be Polled, page 6-4

- Information on Performance Polling Configuration Dialog Tabs, page 6-4

- About Polling Intervals and the Number of Devices Polled, page 6-5

- Selecting Performance Polling Intervals, page 6-5

- Starting and Stopping Performance Polling for the Device and its Components, page 6-6

About Adding SNMP MIB Attributes to be Polled

- fiveMin, fifteenMin, thirtyMin, sixtyMin polling periods—SNMP MIB attributes 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 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 Performance Polling Configuration Dialog Tabs

- Chassis and Chassis... tabs refer to the Cisco AS5300, AS5350, AS5400, AS5800, and AS5850 managed devices.

- DS0 dialog tab refers to the DS0 channel.

- DS1 and DS1... dialog tabs refer to the DS1 port, DS1 channel, and E1 port.

- DS3 dialog tab refers to the DS3 port.

- DSP dialog tab refers to the DSP port.

- Ethernet Port dialog tab refers to the Ethernet, Fast Ethernet, and GigaBit Ethernet ports.

- Modem dialog tab refers to the modem and universal ports.

- 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 "Exporting a File" section on page 6-28.)

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 component 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, DSP ports, voice ports, modem ports, and universal ports.)

Note   If the polling load in your system exceeds Cisco UGM capacity, frequent "Missed Poll" messages appear.

Selecting Performance Polling Intervals

Default performance polling intervals for sampling SNMP MIB attributes from the device and its components are:

- Chassis—fifteen minutes
- DS0, DS1, DS1..., DS3, DSP, Ethernet, Modem—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 Performance Polling Configuration Dialog Tabs" section on page 6-4 for more details.

Step 3   Select 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.

Start performance polling as described in the "Starting and Stopping Performance Polling for the Device and its Components" section on page 6-6.

Starting and Stopping Performance Polling for the Device and its Components

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   From the devices listed on the left, select the devices to be polled.

Step 3   Select the **performancePolling - ON** option.

If you want to stop performance polling later, select the **performancePolling - OFF** option.

Step 4   Click the **Save** button.

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

Overview of Real-Time Display of SNMP-Polled Performance Data

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

Tip   You cannot view some data online; export it to a flat file; then, view it.

Line Charts and Tables

With line charts and tables, you can view SNMP-polled device or card attribute data. Cisco UGM plots data corresponding to attributes that you select 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.

Overview of SNMP MIB Performance Attributes That You Can View

Table 6-1   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.
Average Busy 5 min	OLD-CISCO-CPU-MIB avgBusy5	Represents the 5-minute exponentially degraded moving average of the CPU busy percentage.

Table 6-1   Chassis Performance Attributes (continued)

Text Field	MIB Attribute Name	Description
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.
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
ISDN Cfg B-Channels in Use	CISCO-POP-MGMT-MIB cpmISDNCfgBChanInUse	Indicates the number of configured ISDN B-channels that are currently occupied by both analog and digital calls.
ISDN Cfg B-Channels in Use for Analog	CISCO-POP-MGMT-MIB cpmISDNCfgBChanInUseForAnalog	Indicates the number of configured ISDN B-channels that are currently occupied by analog calls.
ISDN Calls Rejected	CISCO-POP-MGMT-MIB cpmISDNCallsRejected	Indicates the number of rejected ISDN calls in this managed device.

Table 6-1   Chassis Performance Attributes (continued)

Text Field	MIB Attribute Name	Description
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.
PPP Calls	CISCO-POP-MGMT-MIB cpmPPPCalls	Indicates the current number of active PPP calls received by the managed device.
V110 Calls	CISCO-POP-MGMT-MIB cpmV110Calls	Indicates the current number of active V.110 calls received by the managed device.
V120 Calls	CISCO-POP-MGMT-MIB cpmV120Calls	Indicates the current number of active V.120 calls received by the managed device.
Modem Calls Rejected	CISCO-POP-MGMT-MIB cpmModemCallsRejected	Number of modem calls rejected.
Modem Calls Cleared Abnormally	CISCO-POP-MGMT-MIB cpmModemCallsClearedAbnormally	Number of modem calls that cleared abnormally.
Modem Calls No Resource	CISCO-POP-MGMT-MIB cpmModemNoResource	Indicates the number of modem calls that were rejected because there was no modem available to handle the call.
Active DS0s	CISCO-POP-MGMT-MIB cpmActiveDS0s	Indicates the number of DS0s that are currently in use.

Table 6-2   Performance Attribute for the DS0 Port

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

Table 6-3   Performance Attributes for the DS1 Port

Text Field	MIB Attribute Name	Description
RFC1406dsx1ConfigTable		
Line Status (from RFC1406dsx1ConfigTable)	RFC1406 dsx1LineStatus	Indicates the line status of the interface, and contains loopback, failure, received alarm, and transmitted alarm information.
Elapsed Seconds	RFC1406 dsx1TimeElapsed	Indicates the number of seconds elapsed since the beginning of the current polling period.
Valid Interval	RFC1406 dsx1ValidIntervals	Indicates the number of previous intervals for which valid data was collected.
RFC1406dsx1CurrentTable		
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.
Errored Framing Seconds	RFC1406 dsx1CurrentSEFs	Indicates the number of errored framing seconds 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.

Table 6-3   Performance Attributes for the DS1 Port (continued)

Text Field	MIB Attribute Name	Description
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.
Bursty Errored Seconds	RFC1406 dsx1CurrentBESs	Indicates the number of bursty errored 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.
Path Code Violations	RFC1406 dsx1CurrentPCVs	Indicates the number of path coding violations encountered by a DS1 interface in the current fifteen-minute interval.
Degraded Minutes	RFC1406 dsx1CurrentDMs	Indicates the number of degraded minutes encountered by a DS1 interface in the current fifteen-minute interval.
RFC1406dsx1TotalTable		
Errored Seconds	RFC1406 dsx1TotalESs	Indicates the total number of errored seconds encountered by a DS1 interface in the previous 24-hour interval.
Severely Errored Seconds	RFC1406 dsx1TotalSESs	Indicates the total number of severely errored seconds encountered by a DS1 interface in the previous 24-hour interval.
Severely Errored Framing Seconds	RFC1406 dsx1TotalSEFSs	Indicates the total number of severely errored framing seconds encountered by a DS1 interface in the previous 24-hour interval.
Unavailable Seconds	RFC1406 dsx1TotalUASs	Indicates the total number of unavailable seconds encountered by a DS1 interface in the previous 24-hour interval.

Table 6-3   Performance Attributes for the DS1 Port (continued)

Text Field	MIB Attribute Name	Description
Controlled Slip Seconds	RFC1406 dsx1TotalCSSs	Indicates the total number of controlled slip seconds encountered by a DS1 interface in the previous 24-hour interval.
Path Code Violations	RFC1406 dsx1TotalPCVs	Indicates the total number of path coding violations encountered by a DS1 interface in the previous 24-hour interval.
Line Errored Seconds	RFC1406 dsx1TotalLESs	Indicates the total number of line errored seconds encountered by a DS1 interface in the previous 24-hour interval.
Bursty Errored Seconds	RFC1406 dsx1TotalBESs	Indicates the total number of bursty errored seconds encountered by a DS1 interface in the previous 24-hour interval.
Degraded Minutes	RFC1406 dsx1TotalDMs	Indicates the total number of degraded minutes encountered by a DS1 interface in the previous 24-hour interval.
Line Code Violations	RFC1406 dsx1TotalLCVs	Indicates the total number of line coding violations encountered by a DS1 interface in the previous 24-hour interval.
RFC1406dsx1FarEndCurrentTable		
Elapsed Seconds	RFC1406 dsx1FarEndTimeElapsed	Indicates the number of seconds elapsed since the beginning of the far-end-current measurement period.
Valid Intervals	RFC1406 dsx1FarEndValidIntervals	Indicates the number of previous far end intervals for which valid data was collected.
Errored Seconds	RFC1406 dsx1FarEndCurrentESs	Indicates the number of far end errored seconds encountered by a DS1 interface in the current fifteen-minute interval.
Severely Errored Seconds	RFC1406 dsx1FarEndCurrentSESs	Indicates the number of far end severely errored seconds encountered by a DS1 interface in the current fifteen-minute interval.

Table 6-3   Performance Attributes for the DS1 Port (continued)

Text Field	MIB Attribute Name	Description
Severely Errored Framing Seconds	RFC1406 dsx1FarEndCurrentSEFSs	Indicates the number of far end severely errored framing seconds encountered by a DS1 interface in the current fifteen-minute interval.
Unavailable Seconds	RFC1406 dsx1FarEndCurrentUASs	Indicates the number of unavailable seconds encountered by a DS1 interface in the current fifteen-minute interval.
Controlled Slip Seconds	RFC1406 dsx1FarEndCurrentCSSs	Indicates the number of far end controlled slip seconds encountered by a DS1 interface in the current fifteen-minute interval.
Line Errored Seconds	RFC1406 dsx1FarEndCurrentLESs	Indicates the number of far end line errored seconds encountered by a DS1 interface in the current fifteen-minute interval.
Path Code Violations	RFC1406 dsx1FarEndCurrentPCVs	Indicates the number of far end path coding violations encountered by a DS1 interface in the current fifteen-minute interval.
Bursty Errored Seconds	RFC1406 dsx1FarEndCurrentBESs	Indicates the number of far end bursty errored seconds encountered by a DS1 interface in the current fifteen-minute interval.
Degraded Minutes	RFC1406 dsx1FarEndCurrentDMs	Indicates the number of far end degraded minutes encountered by a DS1 interface in the current fifteen-minute interval.
RFC1406dsx1FarEndTotalTable		
Errored Seconds	RFC1406 dsx1FarEndTotalESs	Indicates the number of far end errored seconds encountered by a DS1 interface in the previous 24-hour interval.

Table 6-3   Performance Attributes for the DS1 Port (continued)

Text Field	MIB Attribute Name	Description
Severely Errored Seconds	RFC1406 dsx1FarEndTotalSESs	Indicates the number of far end severely errored seconds encountered by a DS1 interface in the previous 24-hour interval.
Severely Errored Framing Seconds	RFC1406 dsx1FarEndTotalSEFSs	Indicates the number of far end severely errored framing seconds encountered by a DS1 interface in the previous 24-hour interval.

Table 6-4   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 framing 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.

Table 6-4   Performance Attributes for the DS3 Port (continued)

Text Field	MIB Attribute Name	Description
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.

Table 6-5   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.
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.

Table 6-5   Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports (continued)

Text Field	MIB Attribute Name	Description
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.
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.
Last Change	IF-MIB ifLastChange	Indicates the value of the sysUpTime variable at the time when the interface entered its current operational state. If the current state was entered before the last Cisco UGM reboot, this field is 0.

Table 6-5   Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports (continued)

Text Field	MIB Attribute Name	Description
Out Queue Length	IF-MIB ifOutQLen	Indicates the number of packets in the output packet queue.
In Multicast Pkts	IF-MIB ifInMulticastPkts	Indicates the number of packets delivered by this sublayer to a higher sublayer, which were addressed to a multicast address at this sublayer.
In Broadcast Pkts	IF-MIB ifInBroadcastPkts	Indicates the number of packets delivered by this sublayer to a higher sublayer, which were addressed to a broadcast address at this sublayer.
Out Multicast Pkts	IF-MIB ifOutMulticastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sublayer. This number includes packets that were discarded or not sent.
Out Broadcast Pkts	IF-MIB ifOutBroadcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sublayer. This number includes packets that were discarded or not sent.
HC In Octets	IF-MIB ifHCInOctets	Indicates the total number of octets received on this interface (including framing characters).
HC In Ucast Pkts	IF-MIB ifHCInUcastPkts	Indicates the number of packets (not addressed to a multicast or broadcast address) delivered by this sublayer to a higher sublayer This object is a 64-bit version of ifInUcastPkts.

Table 6-5   Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports (continued)

Text Field	MIB Attribute Name	Description
HC In Multicast Pkts	IF-MIB ifHCInMulticastPkts	Indicates the number of packets delivered by this sublayer to a higher sublayer, which were addressed to a multicast address at this sublayer. This object is a 64-bit version of ifInMulticastPkts.
HC In Broadcast Pkts	IF-MIB ifHCInBroadcastPkts	Indicates the number of packets delivered by this sublayer to a higher sublayer, which were addressed to a broadcast address at this sublayer. This object is a 64-bit version of ifInBroadcastPkts.
HC Out Octets	IF-MIB ifHCOutOctets	Indicates the total number of octets (including framing characters) transmitted out of the interface. This object is a 64-bit version of ifOutOctets.
HC Out Ucast Pkts	IF-MIB ifHCOutUcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer. This number includes packets that were discarded or not sent. This object is a 64-bit version of ifOutUcast Pkts.

Table 6-5   Performance Attributes for Ethernet, Fast Ethernet, and Giga Ethernet Ports (continued)

Text Field	MIB Attribute Name	Description
HC Out Multicast Pkts	IF-MIB ifHCOutMulticastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer. This number includes packets that were discarded or not sent. This object is a 64-bit version of ifOutMulticastPkts.
HC Out Broadcast Pkts	IF-MIB ifHCOutBroadcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer. This number includes packets that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts.
Interface Speed	IF-MIB ifSpeed	Represents an estimate of the interface's current bandwidth in bits per second.

Table 6-6   Performance Attributes for Modem and Universal Ports

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

Table 6-6   Performance Attributes for Modem and Universal Ports (continued)

Text Field	MIB Attribute Name	Description
Modem State	CISCO-MODEM-MGMT-MIB cmState	Indicates the current state of the modem: • unknown—the current state of the modem is unknown. • onHook—the condition similar to hanging up a telephone receiver. The call cannot enter a connected state when the modem in onHook. • offHook—the condition similar to picking up a telephone receiver to dial or answer a call. • connected—the modem is in a state where it can transmit or receive data over the communications line. • busiedOut—the modem has been taken out of service and cannot send or receive calls. • disabled—the modem is in a reset state and non-functional. • bad—the modem is suspected or proven to be bad. The operator can take it out of service. • loopback—the modem is currently running back-to-back loopback testing. • downloadFirmware—the modem is currently downloading firmware. • downloadFirmwareFailed—the modem is not operational because the firmware download failed.
Call Direction	CISCO-MODEM-MGMT-MIB cmCallDirection	Indicates the direction of the current or previous call (incoming or outgoing).

Table 6-6   Performance Attributes for Modem and Universal Ports (continued)

Text Field	MIB Attribute Name	Description
Call Phone Number	CISCO-MODEM-MGMT-MIB cmCallPhoneNumber	Indicates the dialed outgoing phone number of the current or previous call.
Caller ID	CISCO-MODEM-MGMT-MIB cmCallerID	Identifies the source of the current or previous call.
Manufacturer ID	CISCO-MODEM-MGMT-MIB cmManufacturerID	Identifies the modem with a hardware revision number, firmware revision number, feature set, and serial number.

Table 6-7   Performance Attributes for the DSP Port

Text Field	MIB Attribute Name	Description
CISCO-DSP-MGMT-MIB-cdspStatusTable		
Total Channels	CISCO-DSP-MGMT-MIB cdspTotalChannels	The total number of channels in the DSP. This value is predetermined by the DSP functionality upon initialization. 0 indicates that the channelized DSP mode is turned off.

Table 6-7   Performance Attributes for the DSP Port (continued)

Text Field	MIB Attribute Name	Description
Channels in Use	CISCO-DSP-MGMT-MIB cdspInUseChannels	The number of channels reserved for serving calls. This value is incremented when the DSP channel is reserved for call setup and is decremented after the DSP channel is free (when the call is disconnected). **Note** Channels In Use/Total x 100% = DSP utilization.
Active Channels	CISCO-DSP-MGMT-MIB cdspActiveChannels	The number of channels used by active calls to process media stream. This value is decremented after the reserved DSP channel enters call connection state and is decremented after the call is disconnected. **Note** If the difference between the Active Channels and Channels In Use is greater than 2, you have dangling channels.

Overview of SNMP MIB Performance Attributes that You Cannot View

You cannot view the following attributes by using the Performance Manager; the attributes are uncharted data. Export the data to flat files (see the "Exporting a File" section on page 6-28).

Note   This section includes attribute information from the Others tab in the Global Performance Polling Configuration dialog box. In order to view this data, export it to a flat file.

The default polling period for items under the Others tab is None.

Table 6-8   Performance Attributes Under the Others Tab

Text Field	MIB Attribute Name	Description
CISCO-MEMORY-POOL-MIB		
ciscoMemoryPoolTable		Contains memory pool monitoring entries.
Memory Pool Name	ciscoMemoryPoolName	Identifies the memory pool.
Memory Pool Free	ciscoMemoryPoolFree	Indicates the number of bytes from the memory pool that is currently unused on the managed device.
Memory Pool Used	ciscoMemoryPoolUsed	Indicates the number of bytes from the memory pool that is currently in use by applications on the managed device.
CISCO-ENVMON-MIB		
ciscoEnvMonSupplyStatusTable		Contains power supply status entries maintained by the environmental monitor card.
ciscoEnvMonSupplyStatusDescr		Describes the power supply being monitored.
CISCO-PROCESS-MIB		
cpmCPUTotalTable		Contains overall CPU statistics.

Table 6-9   Performance Attributes for Export Only

Text Field	MIB Attribute Name	Description
Call Phone Number	CISCO-MODEM-MGMT-MIB cmCallPhoneNumber	Indicates the dialed outgoing phone number of the current or previous call.
Caller ID	CISCO-MODEM-MGMT-MIB cmCallerID	Identifies the source of the current or previous call.
Manufacturer ID	CISCO-MODEM-MGMT-MIB cmManufacturerID	Identifies the modem with a hardware revision number, firmware revision number, feature set, and serial number.

Viewing SNMP-Polled 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 >Performance Manager**.

Step 2   In the list in the left panel, click the performance data that you want to view.

See the "Line Charts and Tables" section on page 6-7.

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 page 6-7.

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 page 6-5.

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 component 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 page 6-26.

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 page 6-28.)

  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
```

About Action Reports

File Export Properties dialog fields are updated when you click Save; only the last update for a field is visible in this dialog box. However, all display field updates appear in the Action Report, which 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."

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 page 6-26.

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 page 6-27.

Example: Performance Export Data Format

Performance export data for scalar attributes is formatted as follows:

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

Overview of Near Real-Time Display of Redundancy Attributes

Cisco UGM supports these features in the following devices:

- Cisco AS5800
- Cisco AS5850

Redundancy and split mode functionality is also described in:

- Overview of Redundancy and High Availability Support, page 1-18.
- Overview of Redundancy Presence Polling for Cisco AS5800 and AS5850 Devices, page 8-5

Overview of Redundancy MIB Attributes

Table 6-10   Cisco AS5800 Redundancy Dialog Box MIB Attribute

Text Field	MIB Attribute Name	Description
Redundancy Status	RedundancyStatus CISCO-C8500-REDUNDANCY-MIB	The operational status of a card.

Table 6-11   Cisco AS5850 Redundancy Dialog Box MIB Attributes

Text Field	MIB Attribute Name	Description
Configuration Tab		
Redundancy Mode	cRFCfgRedundancyMode CISCO-RF-MIB	Indicates the type of redundancy currently in effect.
Redundancy Mode Description	cRFCfgRedundancyModeDescr CISCO-RF-MIB	Describes the redundancy mode indicated by cRFCfgRedundancyMode.
Split Mode	cRFCfgSplitMode CISCO-RF-MIB	Indicates whether redundant units can synchronize with each other: • False—Communication is permitted, and the standby unit is reset to recover. • True—Communication is not permitted, and the standby unit will not recover.
Maintenance Mode	cRFCfgMaintenanceMode CISCO-RF-MIB	Indicates whether redundant units can synchronize with each other: • False—Communication is permitted, and the redundant system is in a normal (non-maintenance) mode. • True—Communication is not permitted, and the redundant system is in a maintenance mode.
Notifications Enabled	cRFCfgNotifsEnabled CISCO-RF-MIB	Allows the enabling/disabling of redundancy subsystem notifications.

Table 6-11   Cisco AS5850 Redundancy Dialog Box MIB Attributes (continued)

Text Field	MIB Attribute Name	Description
Notification Timer	cRFCfgNotifTimer CISCO-RF-MIB	When the standby unit progresses to the "standbyHot" state, asynchronous messages are sent from the active device to the standby device. These messages must be acknowledged. If the active device receives the acknowledgement during the time period specified, progression is normal. If the time ends without an acknowledgement, a switch of activity occurs.
Minimum Notification Timer	cRFCfgNotifTimerMin CISCO-RF-MIB	The minimum acceptable value for the notification timer.
Maximum Notification Timer	cRFCfgNotifTimerMax CISCO-RF-MIB	The maximum acceptable value for the notification timer.
Keep Alive Threshold	cRFCfgKeepaliveThresh CISCO-RF-MIB	Indicates the number of lost keep-alive attempts tolerated before a failure condition is declared and a SWACT notification is sent.
Minimum Keep Alive Threshold	cRFCfgKeepaliveThreshMin CISCO-RF-MIB	Indicates the minimum number of keep-alive attempts.
Maximum Keep Alive Threshold	cRFCfgKeepaliveThreshMax CISCO-RF-MIB	Indicates the maximum number of keep-alive attempts.
Keep Alive Timer	cRFCfgKeepaliveTimer CISCO-RF-MIB	The redundancy subsystem expects to receive a keep-alive request within this time period. If a keep-alive request is not received within this time, a SWACT notification is sent.
Minimum Keep Alive Timer	cRFCfgKeepaliveTimerMin CISCO-RF-MIB	The minimum acceptable value for the cRFCfgKeepaliveTimer object.

Table 6-11   Cisco AS5850 Redundancy Dialog Box MIB Attributes (continued)

Text Field	MIB Attribute Name	Description
Maximum Keep Alive Timer	cRFCfgKeepaliveTimerMax CISCO-RF-MIB	The maximum acceptable value for the cRFCfgKeepaliveTimer object.
Status Tab		
Unit Id	cRFStatusUnitId CISCO-RF-MIB	Represents a unique identifier for this device. This identifier is read from the device backplane.

Table 6-11   Cisco AS5850 Redundancy Dialog Box MIB Attributes (continued)

Text Field	MIB Attribute Name	Description
Redundancy Status	RFState CISCO-RF-MIB	Indicates the current state of the redundancy subsystem: • notKnown—The state is unknown. • disabled—Redundancy is not operational on this device. • initialization—Necessary system services are being established on this device. • negotiation—The peer unit is going through discovery and negotiation. • standbyCold—The standby unit is receiving redundancy notification. • standbyColdConfig—The standby device's startup configuration is being updated from the active device's running configuration. • standbyColdFileSys—The standby device's file system is being updated from the active device. • standbyColdBulk—Data is being synchronized between the active and standby devices. • standbyHot—Data is being synchronized between the active and standby devices; the standby device is ready to take control. • activeFast—Indicates call maintenance efforts during a SWACT.

Table 6-11   Cisco AS5850 Redundancy Dialog Box MIB Attributes (continued)

Text Field	MIB Attribute Name	Description
		• activeDrain—Indicates cleanup operations.
		• activePreconfig—Indicates that the device is active but has not read its configuration.
		• activePostconfig—Indicates that the device is active and is processing its configuration.
		• active—Indicates that the device is active and processing calls.
Peer Unit Id	cRFStatusPeerUnitId CISCO-RF-MIB	Represents a unique identifier for the peer device. This identifier is read from the device backplane.
Peer Unit State	cRFStatusPeerUnitState CISCO-RF-MIB	The current redundancy state on the peer unit.
Primary Mode	cRFStatusPrimaryMode CISCO-RF-MIB	Indicates if this device is the primary (True) or secondary device (False). Primary and secondary modes are not synonymous with active and standby modes. A primary or secondary device can be in either active or standby mode. The primary device takes precedence over the secondary device when negotiating activity (usually at initialization).
Duplex Mode	cRFStatusDuplexMode CISCO-RF-MIB	Indicates if the redundant peer unit has been detected: • True—the peer has been detected. • False—the peer has not been detected.

Table 6-11   Cisco AS5850 Redundancy Dialog Box MIB Attributes (continued)

Text Field	MIB Attribute Name	Description
Manual SWACT Inhibit	cRFStatusManualSwactInhibit CISCO-RF-MIB	Indicates if a manual switch of activity is allowed: • True—the manual switch is not allowed. • False—the manual switch is allowed.
Last SWACT Reason Code	cRFStatusLastSwactReasonCode CISCO-RF-MIB	Indicates the reason for the last switch in activity.

Checking Redundancy ID of Cisco AS5800 and AS5850 Devices

Step 1   In the Map Viewer Physical view, right-click the redundancy container object.

For Cisco AS5800 devices, the dial shelf ID (entered when redundancy was configured) appears.

For Cisco AS5850 devices, the unique backplane identifier (read automatically) appears.

Checking the Redundancy Status of a Cisco AS5800 Device

Step 1   In the Map Viewer, right-click the device object.

Step 2   Select **Chassis > Open Redundancy Status...**

One of these values appears:

• Active

• Standby

• Not configured—indicates that the device is configured for split mode operation

- N/A—indicates that the IOS image installed on the device does not support redundancy

Checking the Redundancy Configuration of a Cisco AS5850 Device

Step 1   In the Map Viewer, right click the device object.

Step 2   Select **Chassis > Open Redundancy Status and Configuration...**

Step 3   Click the **Configuration** tab.

The values in this dialog tab are described in the "Overview of Redundancy MIB Attributes" section on page 6-29.

Checking the Redundancy Status of a Cisco AS5850 Device

Step 1   In the Map Viewer, right click the device object.

Step 2   Select **Chassis > Open Redundancy Status and Configuration...**

Step 3   Click the **Status** tab.

The values in this dialog tab are described in the "Overview of Redundancy MIB Attributes" section on page 6-29.

Overview of Modem and Universal Port Management

Cisco UGM manages modems by periodically polling modems on device objects in normal state. The current state of a modem is defined by the CISCO-MODEM-MGMT-MIB.cmState object.

About Modem States

This section describes states implemented by the CISCO-MODEM-MGMT-MIB.

- unknown—Indicates that the current state of the modem is unknown.

- onHook—Indicates a condition similar to hanging up a telephone receiver. The call cannot enter a connected state when the modem is onHook.

- offHook—Indicates a condition similar to picking up a telephone receiver in order to dial or answer a call.

- connected—Indicates that the modem can transmit or receive data over the communications line.

- busiedOut—Indicates that the modem is taken out of service and cannot make outgoing calls or receive incoming calls.

- disabled—Indicates that the modem is in a reset state and nonfunctional.

- bad—Indicates that the modem is suspected or proven to be bad.

- loopback—Indicates that the modem is running back-to-back loopback testing.

- downloadFirmware—Indicates that the modem is currently downloading firmware.

- downloadFirmwareFailed—Indicates that the modem is not operational because of a failed attempt to download firmware.

Note   For an explanation of modem states see the "Setting Modem-Level Status Polling" section on page 6-39.

About Modem Conditions

- When a modem is operating, it is in one of these states:

  - onHook

  - offHook

  - connected

- When a modem has problems, it is in one of these states:

- – unknown

- – bad

- – downloadFirmwareFailed.

- When a modem is offline, it is in one of these states:

- – busiedOut

- – disabled

- – loopback

- – downloadFirmware.

About the Modem Management Alarm

Cisco UGM's modem state polling feature identifies and monitors modem-related events and raises an alarm if necessary. An operational modem does not have any alarms raised against it.

A modem management alarm generates this message:

- Modem/UP is offline in state <STATE>.

- – A warning-severity alarm is raised if a modem goes from the operational or problematic condition to the offline condition.

- – A minor-severity alarm is raised if a modem goes from the operational or offline condition to the problematic condition.

The current alarm is cleared if the modem changes state and moves to a different condition.

Modem states are described in the "About Modem States" section on page 6-37, and modem conditions are described in the "About Modem Conditions" section on page 6-37.

Setting Modem-Level Status Polling

Note   In the Cisco Universal Gateway Manager Settings dialog box, the values you enter depend 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 1   In Map View, choose **ASEMSConfig > EMS > Settings**.

Step 2   In the Modem-Level Status Polling field, enter an integer that is 300 seconds or larger. The default is 305 seconds.

This value sets the modem status polling interval for all modems installed in Cisco UGM-managed devices.

Step 3   Click **Save**.

Overview of Controller Logging Levels

When the IOSConfigCtrl, ASMainCtrl, ASFaultStandAlone, and ASPerformInv controllers start, they read values from the database and set their logging levels accordingly.

These logging levels are stored even if Cisco EMF and Cisco UGM stop operation. The logging levels are erased only if you reset the database.

Tip   You can set logging levels for several controllers at the same time by selecting their corresponding objects from the list in the left pane of the dialog box.

Setting Controller Logging Levels

The Controller Logging Level dialog box allows you to change the logging levels on the ASMainCtrl, IOSConfigCtrl, ASFaultStandAlone, and ASPerformInv controllers.

Step 1   From the Map Viewer, double-click **LoggingConfiguration**.

The Controller Logging Level dialog box opens.

Step 2   Right-click one or more of the controller objects listed in the left panel:

- **ASMainCtrlLog**

- **IOSConfigCtrlLog**

- **ASFaultStandAloneLog**

- **ASPerformInvLog**

Step 3   Select **Change Controller Logging Level**.

Step 4   Select **On** or **Off** values for each of the following:

- Debug Flag

    When you select **On**, the debug values are written to the controller log selected earlier.

    When you select **Off**, the debug values for this controller log are ignored.

- Info Flag

    When you select **On**, the debug values are written to the controller log selected earlier.

    When you select **Off**, the debug values for this controller log are ignored.

- Warning Flag

    When you select **On**, the debug values are written to the controller log selected earlier.

    When you select **Off**, the debug values for this controller log are ignored.

- Error Flag

    When you select **On**, the debug values are written to the controller log selected earlier.

    When you select **Off**, the debug values for this controller log are ignored.

Note   When you first start Cisco UGM, the following values are in effect:
Debug and Info flags are Off
Warning and Error flags are On

Step 5   Click **Save**.

The changes take effect immediately.

About System Log Files

Each controller creates a log file:

- ASMainCtrl.log
- IOSConfigCtrl.log
- ASFaultStandAlone.log
- ASPerformInv.log

These log files are located in *CEMFROOT*/logs.

When a log file reaches its maximum size, its content is moved into a file with the same name and .old extension. (Example: ASMainCtrl.old.)

Modifying the Size of Log Files

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.

Overview of Controller Logging Levels

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 all faults, also known as 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.

Trap handling in Cisco UGM is handled by the ASFaultStandAlone process, and constitutes the main function of the fault management component. A standalone process is started by sysmgr which restarts it in case of a crash.

Monitored Events

Alarm events 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 a device 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. Cisco UGM identifies incoming traps as originating from managed devices by matching the trap source IP address with the IP address of the managed device. Moreover, the set of supported traps is predefined and nonconfigurable.

The SNMP trap source is specified in "Entering SNMP Information for a Trap (SNMP Tab)" section on page 2-11.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices

Alarm Event	Severity Level	Explanation
ciscoColdStart	Warning	The device object was started from a power-off state. **Note** Clear this event manually.
ciscoWarmStart	Warning	The SNMP server was shut down and restarted. **Note** Clear this event manually.
ciscoLinkDown	Major	A DS1, DS3, or Ethernet interface is down.
ciscoLinkUp	Normal	A DS1, DS3, or Ethernet interface is up.
ciscoAuthenticationFailure	Major	The device received a message that was improperly authenticated.
cachePopFailed	Major	Indicates that chassis initialization failed.
cachePopInterrupted	Major	Indicates that chassis initialization was interrupted.
cardInsertedTrap	Warning	An OIR trap indicated that a card was inserted in the device; Cisco UGM initiates discovery on the device.
cardInserted	Warning	Results from the cardInsRemDetected or cardInsertedTrap; contains the card slot number.
cardRemovedTrap	Warning	An OIR trap indicated that a card was removed from the device; Cisco UGM initiates discovery on the device.
cardRemoved	Warning	Results from the cardInsRemDetected or cardRemovedTrap; contains the card slot number.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices (continued)

Alarm Event	Severity Level	Explanation
Card inserted in slot	Informational	A new card was inserted in the device; Cisco UGM completes discovery on the device.
cardInsRemDetected	Informational	Card presence polling detected that cards were moved in the device.
Card removed in slot	Informational	A card was removed from the device; Cisco UGM completes discovery on the device.
Chassis initialization interrupted	Major	The device was removed from the initializing state before the initialization was completed.
chassisTypeMismatch	Major	A chassis was deployed by using the wrong deployment template.
chassisRebootDetected	Informational	The polling mechanism using sysUpTime detected that the device was rebooted.
communicationLost	Major	Cisco UGM lost SNMP connectivity with the device.
communicationEstablished	Normal	Cisco UGM established SNMP connectivity with the device.
discoveryFailed1	Major	Indicates that device component discovery failed due to loss of communication with the device.
discoveryInterrupted	Major	Indicates that device component discovery was interrupted.
discoveryFailed2	Major	Indicates that device component discovery failed due to Cisco UGM or Cisco EMF internal errors.
discoveryFinished	Normal	Indicates that device component discovery was completed successfully.
discoveryStarted	Normal	Indicates that device component discovery has started.
deploymentFailed	Major	Indicates that device component deployment failed due to an internal error.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices (continued)

Alarm Event	Severity Level	Explanation
deploymentInterrupted	Major	Indicates that device component deployment was interrupted.
deploymentFinished	Normal	Indicates that device component deployment was completed successfully.
deploymentStarted	Normal	Indicates that device component deployment has started.
downloadImageCompleted	Normal	Received a trap indicating that an image was downloaded.
envMonShutdown	Critical	A critical environmental condition is detected, and a device shutdown is imminent.
envMonVoltage	Major	A voltage threshold was exceeded on the device.
envMonNormalVoltage	Major	The environment monitor detected normal voltage on the device.
envMonWarningVoltage	Major	The environment monitor detected voltage that exceeded the warning level.
envMonCriticalVoltage	Major	The environment monitor detected voltage that exceeded the critical level.
envMonShutdownVoltage	Major	The environment monitor detected voltage that exceeded the shutdown level.
envMonVoltageNotPresent	Major	Voltage monitoring is not present on this device.
envMonVoltageDisabled	Major	Voltage monitoring is disabled on this device.
envMonTemperature	Major	A temperature threshold was exceeded on the device.
envMonNormalTemperature	Major	The environment monitor detected normal temperature on the device.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices (continued)

Alarm Event	Severity Level	Explanation
envMonWarningTemperature	Major	The environment monitor detected that the temperature exceeded the warning level.
envMonCriticalTemperature	Major	The environment monitor detected that the temperature exceeded the critical level.
envMonShutdownTemperature	Major	The environment monitor detected that the temperature exceeded the shutdown level.
envMonTemperatureNotPresent	Major	Temperature monitoring is not present on this device.
envMonTemperatureDisabled	Major	Temperature monitoring is disabled on this device.
envMonFan	Major	The fan on the device has failed.
envMonNormalFan	Major	The environment monitor detected that the fan is in a normal state.
envMonWarningFan	Major	The environment monitor detected that the fan is at the warning level.
envMonCriticalFan	Major	The environment monitor detected that the fan is at the critical level.
envMonShutdownFan	Major	The environment monitor detected that the fan is at the shutdown level.
envMonFanNotPresent	Major	Fan monitoring is not present on this device.
envMonFanDisabled	Major	Fan monitoring is disabled on this device.
envMonRedundantSupply	Major	The redundant power supply on the device has failed.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices (continued)

Alarm Event	Severity Level	Explanation
envMonNormalRedundantSupply	Major	The environment monitor detected that the redundant power supply is in a normal state.
envMonWarningRedundantSupply	Major	The environment monitor detected that the redundant power supply is at the warning level.
envMonCriticalRedundantSupply	Major	The environment monitor detected that the redundant power supply is at the critical level.
envMonShutdownRedundantSupply	Major	The environment monitor detected that the redundant power supply is at the shutdown level.
envMonRedundantSupplyNotPresent	Major	Redundant power supply monitoring is not present on this device.
envMonRedundantSupplyDisabled	Major	Redundant power supply monitoring is disabled on this device.
entityDecommissioned	Informational	Device or card object has been decommissioned.
entityCommissioned	Informational	Device or card object has been commissioned.
initialClearSysAlarms	Normal	Clears previous file system usage alarms during initialization.
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]
fileSysBelowMajor	Normal	Server disk usage is below the user-defined major threshold.
fileSysBelowCritical	Normal	Server disk usage is below the user-defined critical threshold.
modemGoesOffline	Warning	Indicates that the modem or Universal Port is offline due to a failure.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices (continued)

Alarm Event	Severity Level	Explanation
modemGoesOffline	Minor	Indicates that the modem or Universal Port is administratively offline.
modemGoesOnline	Normal	Indicates that the modem or Universal Port is online.
modemStatusClear	Normal	Indicates that the device is being deployed using the wrong deployment template.
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. Clear this event manually.
redStatusChange	Warning	Cisco AS5800 device operation (in the redundant mode) switched to the standby router shelf.
upgradeSPEImageInterrupted	Major	Indicates that the SPE image upgrade operation was interrupted.
upgradeModemImageInterrupted	Major	Indicates that the modem image upgrade operation was interrupted.
upgradeIOSImageInterrupted	Major	Indicates that the IOS image upgrade operation was interrupted.
upgradeVFCImageInterrupted	Major	Indicates that the VFC image upgrade operation was interrupted.
upgradeSPEImageFailed	Major	Indicates that the SPE image upgrade operation failed.
upgradeModemImageFailed	Major	Indicates that the modem image upgrade operation failed.

Table 7-1   Traps and Alarm Events from Cisco UGM-Managed Devices (continued)

Alarm Event	Severity Level	Explanation
upgradeIOSImageFailed	Major	Indicates that the Cisco IOS image was not upgraded.
upgradeVFCImageFailed	Major	Indicates that the VFC image was not upgraded.

1. For details on changing this threshold, see the "Example: Sample Configuration File for Fault Management" section on page 7-23.
2. For details on changing this threshold, see the "Example: Sample Configuration File for Fault Management" section on page 7-23.

Table 7-2   Alarm Clearing Correlations

Incoming Alarm	Alarms Cleared
ciscoLinkDown	ciscoLinkUp
ciscoLinkUp	ciscoLinkDown
communicationEstablished	communicationLost discoveryFailed1
discoveryFinished	discoveryStarted
deploymentFinished	deploymentStarted
deploymentFinished	deploymentFailed
discoveryFinished	discoveryFailed2
cardInserted	cardInsertedTrap
cardRemoved	cardRemovedTrap
initialClearSysAlarms	fileSysAboveMajor fileSysAboveCritical initialClearSysAlarms
envMonNormalVoltage	envMonWarningVoltage envMonCriticalVoltage envMonShutdownVoltage envMonVoltageNotPresent envMonVoltageDisabled

Table 7-2   Alarm Clearing Correlations (continued)

Incoming Alarm	Alarms Cleared
envMonNormalTemperature	envMonWarningTemperature envMonCriticalTemperature envMonShutdownTemperature envMonTemperatureNotPresent envMonTemperatureDisabled
envMonNormalfan	envMonWarningFan envMonCriticalFan envMonShutdownFan envMonFanNotPresent envMonFanDisabled
envMonNormalRedundantSupply	envMonWarningRedundantSupply envMonCriticalRedundantSupply envMonShutdownRedundantSupply envMonRedundantSupplyNotPresent envMonRedundantSupplyDisabled
modemStatusClear	modemGoesOffline modemGoesOnline modemStatusClear
fileSysAboveMajor	fileSysBelowMajor
fileSysAboveCritical	fileSysBelowCritical
upgradeSPEImageFailed	downloadImageCompleted
upgradeModemImageFailed	downloadImageCompleted
upgradeIOSImageFailed	downloadImageCompleted
upgradeVFCImageFailed	downloadImageCompleted

Overview of Alarm Events

The Map Viewer shows all managed device objects with current alarms. These alarm events are indicated by colored dots next to the objects in the Map Viewer tree, and also by the color and appearance of object device icons in the Map Viewer (right) pane.

Color Identification of Alarms

In the Map Viewer tree, you can see raised alarm events by the presence of colored dots next to tree objects and by object icons in the Map Viewer pane.

The dots are color coded to reflect the following severity levels (highest to lowest): critical, major, minor, warning, informational, and normal.

The defined color coding is:

- Red = Critical
- Orange = Major
- Yellow = Minor
- Cyan = Warning
- White = Informational
- Green = Normal (no events)

Objects and Icons Representing Device States

The icons in this table are specific to Cisco UGM only.

Table 7-3   Cisco UGM Objects and Icons
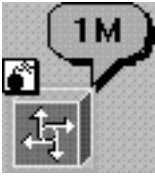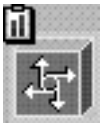
Icon	Device State and Appearance
	Decommissioned. Diagonal lines through the object.
	Deploying Green outline with diagonal lines through the object; arrow icon in upper left corner.

Table 7-3   Cisco UGM Objects and Icons

Icon	Device State and Appearance
	Errored Orange outline; explosive icon in upper left corner.
	Initializing Green outline with diagonal lines through the object; lock icon and arrow icon on upper side.
	Normal Green outline.
	Reload Green outline; clipboard icon in upper left corner.

Alarms Generated by Commissioning or Decommissioning Objects

A device or card object can be in either commissioned or decommissioned state within Cisco UGM.

If an object is in a commissioned state, most alarm events against that object are propagated to the physical tree in the Map Viewer and appear in the parent objects at 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 Commissioning a Device" section on page 8-6 and the "Overview of Decommissioning a Device" section on page 8-6.

Table 7-1 describes Cisco UGM alarm events, their severity, explanation, and recovery procedures.

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 (assuming that there is more than one alarm for the object).

Cisco UGM does not generate all alarm events again, even if the alarm conditions are still present; therefore, be cautious in clearing alarm events.

Tip   You can view cleared alarm events in the Event History.

Step 1   In the Map Viewer, note the color of the status dots to represent the occurrence of alarm events against the objects.

See the "Overview of Trap Forwarding" section on page 7-15.

Step 2   Right-click the object whose list of alarm events you want to view and choose **Tools > Open Event Browser**.

You can acknowledge and clear individual alarm events by clicking the appropriate box next to each event.

Tip   To clear a large number of events, click the first event, press the **Shift** key, and click on the last event you wish to remove. Then click **Clear Events**.

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. The events are color coded to the corresponding alarm. (See "Color Identification of Alarms" section on page 7-11, and the *Cisco Element Management Framework User Guide*.

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.

> **Note**   Only the most severe alarm event against an object appears on 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 Trap Forwarding" section on page 7-15 for an explanation of the colors.

Step 2   Right-click the object whose list of alarm events you want to view and choose **Tools > Open Event Browser**.

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 when the event browser is opened 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 Trap Forwarding

Note   Cisco UGM enables you to select frequency of data polling and SNMP trap forwarding destinations. When making these selections, consider the number of managed ports and devices in your network, and be aware that your selections affect system performance and scalability.

- Cisco UGM monitors UDP port 162 for all SNMPv1 and v2c traps sent from managed devices configured to send traps to this port, and then forwards the traps 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 box.

- 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:

- Deploy host destinations and traps.

- Specify host destinations and traps to be forwarded.

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**.

Trap forwarding reflects any changes made (and saved) in this dialog box. Any previously specified trap forwarding settings are 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 To update trap forwarding, click **Accept Saved Setting**.

Trap forwarding reflects any changes made (and saved) in this dialog box. Any previously specified trap forwarding settings are 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**.

Trap forwarding reflects any changes made (and saved) in this dialog box. Any previously specified trap forwarding settings are replaced.

Tip   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 page 7-16.

Example: Cisco UGM Trap Mapping Tables

Tables 7-4 through 7-8 provide detailed information about SNMP v1 traps handled by Cisco UGM. Each trap is uniquely identified by Enterprise ID, Generic ID, and Specific ID.

Table 7-4   Cisco AS5300 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
ciscoColdStart	1.3.6.1.4.1.9.1.162	0	0	warning
ciscoWarmStart	1.3.6.1.4.1.9.1.162	1	0	warning
ciscoLinkDown	1.3.6.1.4.1.9.1.162	2	0	major
ciscoLinkUp	1.3.6.1.4.1.9.1.162	3	0	normal
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.162	4	0	major

Table 7-5   Cisco AS5350 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
ciscoColdStart	1.3.6.1.4.1.9.1.313	0	0	warning
ciscoWarmStart	1.3.6.1.4.1.9.1.313	1	0	warning
ciscoLinkDown	1.3.6.1.4.1.9.1.313	2	0	major
ciscoLinkUp	1.3.6.1.4.1.9.1.313	3	0	normal
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.313	4	0	major

Table 7-6   Cisco AS5400 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
ciscoColdStart	1.3.6.1.4.1.9.1.274	0	0	warning
ciscoWarmStart	1.3.6.1.4.1.9.1.274	1	0	warning
ciscoLinkDown	1.3.6.1.4.1.9.1.274	2	0	major
ciscoLinkUp	1.3.6.1.4.1.9.1.274	3	0	normal
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.274	4	0	major

Table 7-7   Cisco AS5800 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
ciscoColdStart	1.3.6.1.4.1.9.1.188	0	0	warning
ciscoWarmStart	1.3.6.1.4.1.9.1.188	1	0	warning
ciscoLinkDown	1.3.6.1.4.1.9.1.188	2	0	major
ciscoLinkUp	1.3.6.1.4.1.9.1.188	3	0	normal
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.188	4	0	major

Table 7-8   Cisco AS5850 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
ciscoColdStart	1.3.6.1.4.1.9.1.308	0	0	warning
ciscoWarmStart	1.3.6.1.4.1.9.1.308	1	0	warning
ciscoLinkDown	1.3.6.1.4.1.9.1.308	2	0	major
ciscoLinkUp	1.3.6.1.4.1.9.1.308	3	0	normal
ciscoAuthenticationFailure	1.3.6.1.4.1.9.1.308	4	0	major

Table 7-9 provides detailed information about SNMP v2 traps handled by Cisco UGM.

Table 7-9   SNMP V2 Trap Mapping

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
ciscoColdStart	1.3.6.1.6.3.1.1.5.1	-1	-1	warning
ciscoWarmStart	1.3.6.1.6.3.1.1.5.2	-1	-1	warning
ciscoLinkDown	1.3.6.1.6.3.1.1.5.3	-1	-1	major
ciscoLinkUp	1.3.6.1.6.3.1.1.5.4	-1	-1	normal
ciscoAuthenticationFailure	1.3.6.1.6.3.1.1.5.5	-1	-1	major
cardInserted	1.3.6.1.4.1.9.9.117.2	6	3	warning
cardRemoved	1.3.6.1.4.1.9.9.117.2	6	4	warning
redC5800StatusChange	1.3.6.1.4.1.9.9.105.2.0.1	6	1	warning
redRFStatusChange	1.3.6.1.4.1.9.9.176.2.0.2	6	2	warning
flashCopyCompletion	1.3.6.1.4.1.9.9.10.1.3.0.1	-1	-1	normal
envMonShutdown	1.3.6.1.4.1.9.9.13.3	6	1	critical

Table 7-9   SNMP V2 Trap Mapping (continued)

Class Mapping	Enterprise	Generic ID	Specific ID	Alarm Severity
envMonVoltage	1.3.6.1.4.1.9.9.13.3	6	2	major
envMonTemperature	1.3.6.1.4.1.9.9.13.3	6	3	major
envMonFan	1.3.6.1.4.1.9.9.13.3	6	4	major
envMonRedundantSupply	1.3.6.1.4.1.9.9.13.3	6	5	major

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   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.

Exporting Alarm Events to a File

Step 1   From the Map viewer choose **ASEMSConfig > File Export > Open File Export Properties**.

Step 2   Click the **Alarm** tab.

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

Step 4   Enter a storage path for the file.

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 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 6   Specify the maximum size (in KBytes) of a file before the selected aging action begins. When the maximum file size is reached, export then continues to the newly created file.

Step 7   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; if the path exists, Cisco UGM starts writing data to this location.
- 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 8   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.

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

CEMFROOT>/config/ASFaultStandAlone/TrapConfig.ini

```
[TrapConfig]
LinkDown5300=2 0 1.3.6.1.4.1.9.1.162 yes error
LinkUp5300=3 0 1.3.6.1.4.1.9.1.162 yes normal
LinkDown5350=2 0 1.3.6.1.4.1.9.1.313 yes error
LinkUp5350=3 0 1.3.6.1.4.1.9.1.313 yes normal
LinkDown5400=2 0 1.3.6.1.4.1.9.1.274 yes error
LinkUp5400=3 0 1.3.6.1.4.1.9.1.274 yes normal
LinkDown5800=2 0 1.3.6.1.4.1.9.1.188 yes error
LinkUp5800= 3 0 1.3.6.1.4.1.9.1.188 yes normal
LinkDown5850=2 0 1.3.6.1.4.1.9.1.308 yes error
```

Overview of Exporting Alarm Events

```
LinkUp5850=3 0 1.3.6.1.4.1.9.1.308 yes normal
LinkDownV2=-1 -1 1.3.6.1.6.3.1.1.5.3 yes error
LinkUpV2=-1 -1 1.3.6.1.6.3.1.1.5.4 yes normal
CardRemoved=6 4 1.3.6.1.4.1.9.9.117.2 no commission
CardInserted=6 3 1.3.6.1.4.1.9.9.117.2 no commission
ColdStart5300=0 0 1.3.6.1.4.1.9.1.162 no commission
ColdStart5350=0 0 1.3.6.1.4.1.9.1.313 no commission
ColdStart5400=0 0 1.3.6.1.4.1.9.1.274 no commission
ColdStart5800=0 0 1.3.6.1.4.1.9.1.188 no commission
ColdStart5850=0 0 1.3.6.1.4.1.9.1.308 no commission
ColdStartV2=-1 -1 1.3.6.1.6.3.1.1.5.1 no commission
WarmStart5300=1 0 1.3.6.1.4.1.9.1.162 no commission
WarmStart5350=1 0 1.3.6.1.4.1.9.1.313 no commission
WarmStart5400=1 0 1.3.6.1.4.1.9.1.274 no commission
WarmStart5800=1 0 1.3.6.1.4.1.9.1.188 no commission
WarmStart5850=1 0 1.3.6.1.4.1.9.1.308 no commission
FlashCopyCompletionTrap=-1 -1 1.3.6.1.4.1.9.9.10.1.3.0.1 no
oneDownloadDone
RedundancyC8500StatusChange=6 1 1.3.6.1.4.1.9.9.105.2.0.1 no handover
RedundancyRFStatusChange=6 2 1.3.6.1.4.1.9.9.176.2.0.2 no handover
```

Presence Polling and Loss of Communication

This chapter contains the following sections:

Overview of Presence Polling and Loss of Communication with a Device

Cisco UGM's presence polling function monitors the device for a reboot operation. When Cisco UGM detects a reboot, rediscovery is initiated on that device, and an internal alarm is generated: Chassis has been reloaded and will be rediscovered. This alarm is informational only. Check the Event Browser for alarm details.

When the card-level presence polling function finds card changes, rediscovery is initiated on the parent device, and an internal alarm is generated: Card presence polling discovered card shuffling - chassis will be rediscovered. This alarm is informational only. Check the Event Browser for alarm details.

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.

About 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 the Presence Polling Interval for Cards" section on page 8-4.

About Presence Polling Intervals

Presence polling uses an interval specified in the "Setting Presence Polling Intervals for Devices in Normal, Errored, and Reload States" section on page 8-3. 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. You can view alarm events in the Event Browser.

The default presence polling intervals are:

- 60 seconds during the normal or errored states for devices (device-level).
- Number of retries to detect loss of connectivity is 1.
- 300 seconds for card-level presence polling.

Overview of Attributes Sampled for Presence Polling

These attributes enable Cisco UGM to detect the addition or removal of cards in a device, and then initiate rediscovery of the device.

Table 8-1   Presence Polling MIB Attributes

MIB Attribute Name	Description
sysUpTime RFC1213-MIB	Detects if Cisco UGM was rebooted.
cardTable OLD-CISCO-CHASSIS-MIB	Detects if cards were installed or removed from the device.

Setting Presence Polling Intervals for Devices in Normal, Errored, and Reload States

Note   In the Cisco Universal Gateway Manager Settings dialog box, the values you enter depend 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 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 greater than 30 seconds. The default is 60 seconds.

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 greater than 30 seconds. The default is 60 seconds.

Step 4   Enter the interval at which a device should be polled in the reload state.

The interval should be an integer value that is greater than 30 seconds. The default is 60 seconds.

Step 5   Click **Apply**.

Setting the Presence Polling Interval for Cards

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

Step 2   Enter the interval at which cards should be polled.

The interval should be an integer value that is greater than 30 seconds. The default is 300 seconds.

Note   This value depends on the total number of managed devices and components 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   Click **Apply**.

Setting the 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, Errored, and Reload States" section on page 8-3. 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 that you enter 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**.

Overview of Redundancy Presence Polling for Cisco AS5800 and AS5850 Devices

The failure of the active device and the activation of the standby device is detected by Cisco UGM's redundancy presence polling feature. This redundancy state change generates a warning alarm against the device object.

When Cisco UGM receives traps from these devices, both devices transition to a "handover" state while control of the cards is transferred. The process can take several minutes and prevents the possible reading of incorrect values and subsequent failure to create new objects in the rediscovery that follows.

Note   The handover interval is currently set to 90 seconds. If you find that this interval is inadequate to transfer control, change the value of the appropriate variable in the ASMainCtrlUserData.ini configuration file: AS5800ChassisHandoverLingerSec or AS5850ChassisHandoverLingerSec.

In order for these new values to take effect, restart the ASMainCtrl controller

by typing these commands:

cd /opt/cemf/bin
cemf shell
sysmgrClient -k ASMainCtrl
sysmgrClient -x ASMainCtrl

The handover state is followed by the commissioning state when device component rediscovery is completed.

Overview of Commissioning a Device

Note Do not commission or decommission more than three devices at a time.

Commission a device to return it to a normal (commissioned) state within the EMS.

When you commission a device, an informational alarm is raised in Event Browser, and Cisco UGM starts discovery on the device to resolve any card inventory changes that may have occurred while the device 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 components (cards and ports) also transition into the commissioned state.

The procedure to commission a device is described in the "Commissioning and Decommissioning a Device or Card" section on page 8-8.

Overview of Decommissioning a Device

Note Do not commission or decommission more than three devices at a time.

With Cisco UGM, you can decommission a device from any state, and an informational alarm is raised in Event Browser.

You can decommission a device due to one of these causes:

- The device was manually deployed.

- You decommissioned the device to suspend alarm propagation when the device is rebooted or undergoing maintenance.

A decommissioned object is still managed by Cisco UGM, and has alarms raised against it unconditionally. Performance or presence polling is carried out, and alarm events are collected and viewed by using the Event Browser. In addition, the color of the icon representing the object in the Map Viewer indicates the severity and number of alarms raised. However, because the object is in a decommissioned state, no alarm propagation takes place.

Note When a chassis is decommissioned, all its components (cards and ports) also transition into the decommissioned state.

The procedure to commission a device is described in the "Commissioning and Decommissioning a Device or Card" section on page 8-8.

Overview of 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 is removed from the device, the corresponding card object is deleted.

Note When a parent device is commissioned, all its components (cards and ports) also transition into the commissioned state. Likewise, when a card is commissioned, all its ports are also commissioned.

The procedure to commission a device is described in the "Commissioning and Decommissioning a Device or Card" section on page 8-8.

Overview of 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.

A decommissioned object is still managed by Cisco UGM, and has alarms raised against it unconditionally. Performance or presence polling is carried out, and alarm events are collected and viewed by using the Event Browser. In addition, the color of the icon representing the object in the Map Viewer indicates the severity and number of alarms raised. However, because the object is in a decommissioned state, no alarm propagation takes place.

When a parent device is decommissioned, all its components (cards and ports) also transition into the decommissioned state. Likewise, when a card is decommissioned, all its ports are also decommissioned.

The procedure to commission a device is described in the "Commissioning and Decommissioning a Device or Card" section on page 8-8.

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**.

Tip   Decommissioned devices appear as shaded icons in the right-hand pane of the Map Viewer.

Cards Supported in Devices Managed by Cisco UGM

This appendix contains the following tables:

- Cisco UGM-Supported Card Types, Part Numbers, and Prefixes (Table A-1 on page A-2)
- Cisco UGM-Supported Card OIDs and Cisco EMF Classes (Table A-2 on page A-5)

Overview of Table Values

- The Card Part Number (in Table A-1) is the official Cisco name for the component. (Use this description when ordering the component.)
- The Cisco UGM Card Name Prefix (in Table A-1) is added to the names of components displayed in the Physical view of the Map Viewer.
- The Vendor OID (in Table A-2) is the SNMP value in the ENTITY-MIB.entPhysicalTable that allows Cisco UGM to discover these components.

Table A-1   Cisco UGM-Supported Card Types, Part Numbers, and Prefixes

Device	Card Type	Card Part Number	Cisco UGM Card Name Prefix
Cisco AS5300	Voice	AS53-CC-48VOXD	AS5300VFC
		AS53-CC-60VOXD	AS5300VFC
		AS53-CC-24VOX	AS5300VFC
		AS53-CC-30VOX	AS5300VFC
	Modem	AS53-48-CC2	ModemCard
		AS53-60-CC2	ModemCard
		AS53-96-CC2	ModemCard
		AS53-120-CC2	ModemCard
		AS53-CC2-DM	ModemCard
	Trunk	AS53-4CT1	4CT1
		AS53-4CE1	4CE1
		AS53-4CT1+4Serial	4CT1_4Serial
		AS53-4CE1+4Serial	4CE1_4Serial
		AS53-8CT1+4Serial	8CT1_8Serial
		AS53-8CE1+4Serial	8CE1_8Serial

Table A-1   Cisco UGM-Supported Card Types, Part Numbers, and Prefixes (continued)

Device	Card Type	Card Part Number	Cisco UGM Card Name Prefix
Cisco AS5350	Universal Port	AS535-DFC-60NP	NP60DFC
		AS535-DFC-108NP	NP108DFC
	Trunk	AS535-DFC-2 PRI T1/E1	T1_2_PRI_DFC/ E1_2_PRI_DFC
		AS535-DFC-4 PRI T1/E1	T1_4_PRI_DFC/ E1_4_PRI_DFC
		AS535-DFC-8 PRI T1/E1	T1_8_PRI_DFC/ E1_8_PRI_DFC
		AS535-DFC-2CT1	T1_2_PRI_DFC
		AS535-DFC-2CE1	E1_2_PRI_DFC
		AS535-DFC-4CT1	T1_4_PRI_DFC
		AS535-DFC-4CE1	E1_4_PRI_DFC
		AS535-DFC-8CT1	T1_8_PRI_DFC
		AS535-DFC-8CE1	E1_8_PRI_DFC
		AS535-DFC-CT3	CT3_DFC
Cisco AS5400	Universal Port	AS54-DFC-108NP	NP108DFC
		AS54-DFC-60NP	NP60DFC
	Trunk	AS54-DFC-4 PRI T1/E1	T1_4_PRI_DFC/ E1_4_PRI_DFC
		AS54-DFC-8 PRI T1/E1	T1_8_PRI_DFC/ E1_8_PRI_DFC
		AS54-DFC-CT3	CT3_DFC
Cisco AS5800	Voice	DS58-192VOX	AS5800VFC
		DS58-96VOX	AS5800VFC
		DS58-192-MC-VOX	AS5800VFC
		DS58-336-MC-VOX	AS5800VFC
	DSC	DSC	AS5800DSController

Table A-1   Cisco UGM-Supported Card Types, Part Numbers, and Prefixes (continued)

Device	Card Type	Card Part Number	Cisco UGM Card Name Prefix
	DSI	DSI	AS5800DSController
	Trunk	DS58-12CT1	AS5800_12T1
		DS58-12CE1	AS5800_12E1
		CT3	AS5800_T3
	Modem	HMM	AS5800micaHmm
		DS58-144DM-CC	AS5800micaDmm
Cisco AS5850	Universal Port	AS58-324UPC-CC	UP324Card
	Combination	AS58-1CT3/216U	CT3UP216Card
	Router Shelf Controller	AS5850RSC2GECard	As5850Rsc2GeCard
		AS5850RSCCard	As5850RSCCard
	Trunk	AS58-24E1	24CE1Card
		AS58-24T1	24CT1Card

Table A-2   Cisco UGM-Supported Card OIDs and Cisco EMF Classes

Card Part Number	Vendor OID	Cisco EMF Class
AS53-CC-48VOXD	cisco.12.3.1.9.11.7	ASVFCard
AS53-CC-60VOXD	cisco.12.3.1.9.11.7	ASVFCard
AS53-CC-24VOX	cisco.12.3.1.9.11.7	ASVFCard
AS53-CC-30VOX	cisco.12.3.1.9.11.7	ASVFCard
AS53-48-CC2	cisco.12.3.1.9.11.3	ASModemCard
AS53-60-CC2	cisco.12.3.1.9.11.3	ASModemCard
AS53-96-CC2	cisco.12.3.1.9.11.5	ASModemCard
AS53-120-CC2	cisco.12.3.1.9.11.10	ASModemCard
AS53-CC2-DM	cisco.12.3.1.9.11.15	ASModemCard
AS53-4CT1	cisco.12.3.1.9.11.1	AST1Card
AS53-4CE1	cisco.12.3.1.9.11.2	ASE1Card
AS53-4CT1+4Serial	cisco.12.3.1.9.11.13	AST1Card
AS53-4CE1+4Serial	cisco.12.3.1.9.11.14	ASE1Card
AS53-8CT1+4Serial	cisco.12.3.1.9.11.11	AST1Card
AS53-8CE1+4Serial	cisco.12.3.1.9.11.12	ASE1Card
AS535-DFC-60NP	cisco.12.3.1.9.2.27	ASUPCard
AS535-DFC-108NP	cisco.12.3.1.9.2.37	ASUPCard
AS535-DFC-2 PRI T1/E1	N/A	AST1Card /ASE1Card
AS535-DFC-4 PRI T1/E1	N/A	AST1Card /ASE1Card
AS535-DFC-8 PRI T1/E1	cisco.12.3.1.9.2.25/24	AST1Card /ASE1Card
AS535-DFC-2CT1	cisco.12.3.1.9.2.36	AST1Card
AS535-DFC-2CE1	cisco.12.3.1.9.2.35	ASE1Card
AS535-DFC-4CT1	cisco.12.3.1.9.2.34	AST1Card
AS535-DFC-4CE1	cisco.12.3.1.9.2.33	ASE1Card
AS535-DFC-8CT1	N/A	AST1Card
AS535-DFC-8CE1	N/A	ASE1Card

Table A-2   Cisco UGM-Supported Card OIDs and Cisco EMF Classes (continued)

Card Part Number	Vendor OID	Cisco EMF Class
AS535-DFC-CT3	cisco.12.3.1.9.2.26	AST3Card
AS54-DFC-108NP	cisco.12.3.1.9.2.27	ASUPCard
AS54-DFC-60NP	cisco.12.3.1.9.2.37	ASUPCard
AS54-DFC-4 PRI T1/E1	N/A	AST1Card /ASE1Card
AS54-DFC-8 PRI T1/E1	cisco.12.3.1.9.2.25/24	AST1Card /ASE1Card
AS54-DFC-CT3	cisco.12.3.1.9.2.26	ASCT3Card
DS58-192VOX	cisco.12.3.1.9.12.8	ASVFCard
DS58-96VOX	cisco.12.3.1.9.12.8	ASVFCard
DS58-192-MC-VOX	cisco.12.3.1.9.12.11	ASVFCard
DS58-336-MC-VOX	cisco.12.3.1.9.12.11	ASVFCard
DSC	csco.12.3.1.9.12.1	ASCommonCard
DSI	csco.12.3.1.9.12.1	ASCommonCard
DS58-12CT1	csco.12.3.1.9.12.3	AST1Card
DS58-12CE1	csco.12.3.1.9.12.2	ASE1Card
AS58-24CE1	cisco.12.3.1.9.37.5	ASE1Card
CT3	cisco.12.3.1.9.12.5	ASCT3Card
HMM	cisco.12.3.1.9.12.4	ASModemCard
DS58-144DM-CC	cisco.12.3.1.9.12.7	ASModemCard
AS58-1CT3/216U	cisco.12.3.1.9.37.2	ASCT3UPCard
AS58-324UPC-CC	cisco.12.3.1.9.37.4	ASUPCard
AS58-1CT3/216U	cisco.12.3.1.9.37.2	ASCT3UPCard
1 8 PRI E1, 2 NP 108	cisco.12.3.1.9.37.3	ASE1UPCard
RSC-2GE	cisco.12.3.1.9.37.1	ASCommonCard
RSC	cisco.12.3.1.9.5.38	ASCommonCard
AS58-24E1	cisco.12.3.1.9.37.5	ASE1Card
AS58-24T1	cisco.12.3.1.9.37.6	AST1Card