



## Basic VHM Configuration

---

The Administration folder within the Voice Health Monitor folder contains the tools you need to configure VHM. A user in a CiscoWorks2000 Network Admin role can update the VHM configuration. Users in the Network Operator role can view the configuration data. Users in all other roles have no access to the Administration folder.

The following topics explain how to use the applications in the Administration folder to effectively configure VHM:

- [Overview of VHM Configuration Tasks, page 5-2](#)
- [Using the Administration Console, page 5-3](#)
- [Scheduling Inventory Collection, page 5-21](#)
- [Configuring Trap Receiving, page 5-25](#)
- [Configuring Fault Notification, page 5-26](#)
- [Configuring ICS 7750 for Use with VHM, page 5-51](#)
- [Configuring CCM for Use with VHM, page 5-53](#)

# Overview of VHM Configuration Tasks

Within the Administration folder, the following applications allow you to configure the VHM system:

- **Administration Console**—Import device into VHM; change the default polling and threshold parameters that VHM provides; manage and unmanage devices.
- **Inventory Collection Scheduling**—Schedule regular inventory collection that synchronizes VHM inventory with DFM and probes devices.
- **Trap Configuration**—Specify the port VHM uses for receiving traps.
- **Fault Notification**—Configure notifiers to send email, send trap messages, and log events to the alarm log.
- **Synthetic Transaction Administration**—Configure test transactions to run against Cisco CallManagers. The related instructions are in [Chapter 6, “Synthetic Transaction Configuration.”](#)



---

**Note**

You must configure any SPE on ICS 7750, enabling trace and enabling SNMP. See the “[Configuring ICS 7750 for Use with VHM](#)” section on page 5-51 for instructions.

---



---

**Note**

CCM must be configured for use with VHM. See the “[Configuring CCM for Use with VHM](#)” section on page 5-53.

---

# Using the Administration Console

This topic explains how to start the Administration Console and describes the kind of information included in the console.

To start the Administration Console:

---

**Step 1** Use one of the following procedures:

- From the **Voice Health Monitor** drawer, select **Administration > Administration Console**. The Administration Console is displayed in its own window.
  - From any Summary View or Status View in the Real-Time Dashboard, select **Tools > Administration Console**. The Administration Console is displayed in its own window.
- 

The Administration Console contains two panels. The left panel displays an Inventory Browser that lists the system classes. Each type of managed element is represented by a system class, which consists of properties that describe a managed element. Properties include *description*, *attributes*, *groups*, and *events*.

Classes for VHM include InlinePowerSwitch, MediaServer, SkinnyVoiceGateway, VoiceGateway, VoiceServices, WorkFlowApp, Voice Cluster, Unsupported, and Undiscovered. When a class is selected, the right panel displays the properties of the class in three separate tabs. [Table 5-1](#) lists the available properties of the class.



**Caution**

---

When the VHM domain is manually attached in DFM using the DFM Administration Console, the classes listed above will not be displayed by default under VHM Domain in the DFM Administration Console. Please use the VHM Administration Console to see the correct class list under VHM Domain.

---

**Table 5-1 VHM System Class Properties**

Tab	Description
Attributes	Lists the attributes of the class. Note that the attributes do not contain values.
Events	Events that occur in instances of the class, or events that can affect instances of the class.
Groups	Groups and settings that pertain to polling and threshold for that particular device.

The Administration Console layout and how to customize it are more fully described in the *Device Fault Manager User Guide*.

This section contains the following topics:

- [Managing and Unmanaging Voice Devices in VHM, page 5-4](#)
- [Managing Inline Power Switch Ports, page 5-9](#)
- [Configuring Polling and Thresholds, page 5-10](#)

## Managing and Unmanaging Voice Devices in VHM

You must add voice devices to VHM. You may also unmanage or delete devices from VHM. The voice devices that you import into VHM are used as the basis of discovery for the voice network.

This section contains the following topics:

- [Adding Individual Devices, page 5-5](#)
- [Importing Devices from a Seed File, page 5-5](#)
- [Deleting Devices from VHM, page 5-7](#)
- [Unmanaging Devices, page 5-7](#)
- [Synchronizing SNMP Community String for a Device, page 5-8](#)

## Adding Individual Devices

You can add individual voice devices for VHM to manage by adding an agent.

To add an agent:

- 
- Step 1** On the Administration Console, select **Inventory > Add Agent**. The Add Agent window appears.
  - Step 2** Select VHM and click **OK**.
  - Step 3** Enter the Agent Name and Read Community strings for the device. If a Read Community string is not specified, a default value of public is used.
  - Step 4** Click **OK**.
- 

## Importing Devices from a Seed File

You can import an initial voice network topology into the VHM server from a seed file.

**Note**

---

If voice gateways are registered with CallManagers, Media Servers running those CallManagers must be discovered before the voice gateways so that VHM can capture the registration relationship between these two entities.

---

A seed file consists of:

- Lines containing one or two columns
- Any combination of spaces and tab characters separating the columns.

The first column identifies the network device. You can specify either a name or an IP address. The second column defines the read community string (by default it is "public"). To make your seed file more readable, you can include blank lines and comment lines. A comment line is one whose first character is "#."

**Note**

---

The voice network discovery will not try to access any devices whose names are included on comment lines.

---

The following is an example of the contents of a seed file.

```
# Sample seed file
192.168.121.25
example.cisco.com public
192.168.1.200 private
access-router-1 private
```

IP Address or DNS Name	Community String
192.168.121.25	
example.cisco.com	public
192.168.1.200	private
access-router-1	


**Note**

If a community string is not specified, VHM will use the default value (public).

The default read community string (public, unless changed) is used for the devices at IP address 192.168.121.25 and access-router-1, because an alternate string is not specified. The read community string for 192.168.1.200 is private, and the read community string for example.cisco.com is public.

When adding devices to VHM using a seed file, add all Media Convergence Servers (MCSs) in one seed file and all other devices using a separate seed file. Import the seed files in the following order:

1. Import the seed file containing the MCS.
2. Wait until the addition of the first seed files is complete. Look at the "Discovery Progress" popup dialog box. The "Ready" state on the dialog box indicates completion.
3. Import the seed file containing all other devices.

To import devices from a seed file:

- 
- Step 1** On the Administration Console, select **Inventory > Import from seed file**. The Import from seed file window appears.
- Step 2** From the list of domain managers, select VHM and click OK.
- Step 3** Enter the path where the seed file resides (for example, NMSROOT\conf\seedfile).



---

**Note** NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.

---

- Step 4** Click OK.



---

**Note** When devices are imported using the seed file option, they are added to the device list. If a device in the seed file already exists, the community string of the device is overridden with the community string value from the seed file.

---

## Deleting Devices from VHM

See the [“Deleting Devices from Inventory”](#) section on page 5-24 for instructions on deleting devices from VHM.

## Unmanaging Devices

The manage and unmanage operations enable you to control whether a domain manager monitors a particular device or element. It is useful to unmanage a device when, for example, a switch or a card is taken offline for maintenance and you do not want to receive error or performance notifications regarding that device.

The general procedures for managing and unmanaging objects are described in the *Device Fault Manager User Guide*.

## Synchronizing SNMP Community String for a Device

The SNMP community string must match in both VHM and DFM. If there is a change in the SNMP community string for a device, the community string must be synchronized in both VHM and DFM.

The procedure is the same for both VHM and DFM.

To change the SNMP community string on a device:

- 
- Step 1** Open the Administration Console. See the [“Using the Administration Console” section on page 5-3](#).
  - Step 2** Select the device from the inventory list.
  - Step 3** Navigate to SNMPAgent for the device. For example: **VHM > VoiceGateway > HostsServices > SNMPAgent > SNMP-<Device Name>**.
  - Step 4** Double click the Attribute Value column for ReadCommunity.
  - Step 5** Enter the new community string value.
  - Step 6** Click **Apply**.
  - Step 7** After making changes, reconfigure the domain.
    - Select **Inventory > Reconfigure > VHM/DFM**, and click **OK**.
    - Or
    - Click the Reconfigure icon on the tool bar.
-

## Managing Inline Power Switch Ports

By default, VHM does not manage inline power switch ports. If you want VHM to manage inline power switch ports, you must configure it to do so.

### Configuring VHM to Manage Inline Power Switch Ports

There are two ways to configure VHM to manage inline power switch ports: through the Administration Console (see the *Device Fault Manager User Guide* for a complete description on managing and unmanaging devices) or by using the EtherPortManagement utility.

The EtherPortManagement utility enables you to change the managed state of multiple inline power switch ports from unmanaged to managed, all at one time.

To configure VHM to manage inline power switch ports:

- 
- Step 1** On your VHM machine, open a DOS command prompt.
- Step 2** Use the **cd** command to access the NMSROOT\objects\vhm\bin directory.

**Note**

NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

---

- Step 3** Enter the following command:

```
EtherPortManagement manage --type inlinepowerswitch
```

This command changes the state of all inline power switch device ports from unmanaged to managed.

[Table 5-2](#) describes the EtherPortManagement commands.

- Step 4** Press Enter.
-

**Table 5-2 EtherPortManagement Utility Commands**

Command	Result
EtherPortManagement manage --type all	All devices' inline power ports are changed to managed.
EtherPortManagement unmanage --type all	All devices' inline power ports are changed to unmanaged.
EtherPortManagement manage --type inlinepowerswitch	All inline power switch device ports are changed to managed.
EtherPortManagement unmanage --type inlinepowerswitch	All inline power switch device ports are changed to unmanaged.
EtherPortManagement manage --type voicegateway	All inline power ports of voice gateway devices are changed to managed.
EtherPortManagement unmanage --type voicegateway	All inline power ports of voice gateway devices are changed to unmanaged.
EtherPortManagement manage --device 172.20.13.15 (any IP address)	All inline power ports in the designated IP address are changed to managed.
EtherPortManagement unmanage --device 172.20.13.15 (any IP address)	All inline power ports in the designated IP address are changed to unmanaged.

## Configuring Polling and Thresholds

Voice network health depends upon the performance of voice-enabled devices. VHM polls these devices on a regular basis at user-configured polling intervals. During polling, if VHM determines that the thresholds you have set have been violated, alarms are generated to notify you of these events.

VHM is preconfigured with default polling intervals and threshold parameters. You can change these default values to suit your needs.



### Note

After changing polling or threshold settings, you should save inventory and reconfigure VHM.

**Note**

---

To ensure reliable correlation between VHM and DFM, synchronize the polling intervals in VHM with those in DFM.

---

For additional information about interdependencies, see [Table 1-1 on page 1-4](#).

Threshold and polling parameters are applied to a group of devices.

The following are default polling groups for VHM:

- Media Servers
- Voice Gateways
- Inline Power Switches
- Integrated Communication System (ICS)
- SPE
- Skinny Voice Gateways
- Other Systems
- Skinny Voice Interfaces (Skinny Voice Interface and Other Systems)

The following are default threshold groups for VHM:

- Media Servers
- SPE
- Other Systems

Thresholds for voice-enabled routers (Voice Gateways) and switches (Inline Power Switches) must be set using DFM.

**Note**

---

To ensure that the changes take effect, always reconfigure the VHM (or DFM) domain after changing the polling or threshold values.

---

Instructions for updating polling and threshold groups are included in the *Device Fault Manager User Guide*.

To start the Polling and Thresholds window:

- 
- Step 1** From the Administration Console, select **Edit > Polling and Thresholds**.  
The Polling and Thresholds window appears.
- Step 2** Select either the Polling or Threshold tab at the bottom of the window.  
Configuration groups are displayed in the left panel of the window.
- Step 3** Click a configuration group to display that group's settings. At this point, you can also display the description, priorities, and matching criteria for the group.
- Step 4** Review the default information for the groups of the domain.
- Step 5** After making changes, reconfigure the domain so that the changes will take effect.
- Select **Inventory > Reconfigure > VHM/DFM**, and click **OK**.
- Or
- Click the Reconfigure icon on the tool bar.



**Note**

---

Changes to the polling intervals take effect after the current polling cycle is completed. For example, if the current polling cycle of 10 minutes is changed to 30 seconds, you will have to wait for the current polling cycle to complete before the new setting of 30 seconds takes effect.

---



**Note**

---

The Polling and Thresholds window and its menus, buttons, and functions are described in the *Device Fault Manager User Guide*.

---

## Configuring Polling

You can access or change the settings on the Polling tab of the Polling and Thresholds window. This window and its menus, buttons, and functions are described in the *Device Fault Manager User Guide*. For instructions on starting the Polling and Thresholds window, see the [“Configuring Polling and Thresholds” section on page 5-10](#).

This section contains the following topics:

- [Environment Polling—Power Supply, Fan, and Temperature Sensor, page 5-13](#)
- [Environment Polling—RIB Card, page 5-14](#)
- [External Polling, page 5-14](#)
- [Performance Polling—Disk Usage and Virtual Memory, page 5-15](#)
- [Performance Polling—CPU and Physical Memory \(RAM\), page 5-15](#)
- [Performance Polling—DS1 Voice Port, page 5-16](#)
- [Performance Polling—E1 Voice Port, page 5-16](#)
- [Performance Polling—Inline Power Switch Ethernet Port, page 5-17](#)
- [Performance Polling—Power Supply, page 5-17](#)
- [Performance Polling—Interface, page 5-18](#)
- [Voice Port to Cisco CallManager Connectivity Polling, page 5-18](#)

## Environment Polling—Power Supply, Fan, and Temperature Sensor

Environment Polling settings configure polling intervals used to monitor the environmental conditions of a system. System components such as the power supply, fan, voltage sensor, and temperature sensor elements are monitored. [Table 5-3](#) lists the parameters included in the Environment Polling settings.

**Table 5-3** *Environment Polling—Power Supply, Fan, and Temperature Sensor Settings*

Parameters	Default Value
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive connectivity polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Environment Polling—RIB Card

Environment Polling settings configure polling intervals used to monitor the environmental conditions of a system. System components such as the RIB card are monitored. [Table 5-4](#) lists the parameters included in the Environment Polling settings.

**Table 5-4 Environment Polling—RIB Card Settings**

Parameters	Default Value
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive connectivity polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## External Polling

External Polling settings configure polling intervals used to monitor notifications from a server. [Table 5-5](#) lists the parameters included in the External Polling settings.

**Table 5-5 External Polling Settings**

Parameters	Default Value
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive connectivity polls. The default value is 10 seconds.
Server Name	Name of the server that clients contact for polling notifications. The default value is PollingServer. Do not change this value.

## Performance Polling—Disk Usage and Virtual Memory

Performance Polling—Disk Usage and Virtual Memory settings configure polling for monitoring disk usage and virtual memory. [Table 5-6](#) lists the parameters included in the Performance Polling—Disk Usage and Virtual Memory settings.

**Table 5-6 Performance Polling—Disk Usage and Virtual Memory Settings**

Parameter	Default Value
Analysis Mode	Enables or disables connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Performance Polling—CPU and Physical Memory (RAM)

[Table 5-7](#) lists the parameters included in the Performance Polling—CPU and Physical Memory settings.

**Table 5-7 Performance Polling—CPU and Physical Memory Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Performance Polling—DS1 Voice Port

Table 5-8 lists the parameters included in the Performance Polling—DS1 Voice Port settings.

**Table 5-8 Performance Polling—DS1 Voice Port Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Performance Polling—E1 Voice Port

Table 5-9 lists the parameters included in the Performance Polling—E1 Voice Port settings.

**Table 5-9 Performance Polling—E1 Voice Port Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Performance Polling—Inline Power Switch Ethernet Port

Table 5-10 lists the parameters included in the Performance Polling—Inline Power Switch Ethernet Port settings.

**Table 5-10 Performance Polling—Inline Power Switch Ethernet Port Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Performance Polling—Power Supply

Table 5-11 lists the parameters included in the Performance Polling—Power Supply settings.

**Table 5-11 Performance Polling—Power Supply Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Performance Polling—Interface

Table 5-12 lists the parameters included in the Performance Polling—Interface settings.

**Table 5-12 Performance Polling—Interface Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Voice Port to Cisco CallManager Connectivity Polling

Table 5-13 lists the parameters included in the Voice Port to Cisco CallManager Connectivity settings.

**Table 5-13 Voice Port to Cisco CallManager Connectivity Polling Settings**

Parameter	Default
Analysis Mode	Enable or disable connectivity or availability polling. The default is Enabled.
Polling Interval	The time between successive performance polls. The default value is 240 seconds.
Retries	The number of times to retry a failed poll request. The default value is 3.
Timeout	The amount of time allowed for the first poll request before it times out. The default value is 700 milliseconds.

## Setting Thresholds

You can set thresholds for media servers and SPE only using VHM. Thresholds for voice-enabled routers (Voice Gateways) and switches (Inline Power Switches) must be set using DFM. See the *Device Fault Manager User Guide* for instructions.

You can access or change the threshold settings on the Threshold tab of the Polling and Thresholds window. This window and its menus, buttons, and functions are all described in the *Device Fault Manager User Guide*. For instructions on starting the Polling and Thresholds window, see the “[Configuring Polling and Thresholds](#)” section on page 5-10.

These topics describe available threshold settings:

- [Threshold Setting—CallManager Application, page 5-19](#)
- [Threshold Setting—CPU and Physical Memory \(RAM\), page 5-19](#)
- [Threshold Setting—Disk Usage and Virtual Memory, page 5-20](#)
- [Threshold Setting—Environment: RIB Card, page 5-20](#)
- [Threshold Setting—Environment: Temperature Sensor, page 5-20](#)

### Threshold Setting—CallManager Application

The CallManager Application setting monitors the percentage of inactive phones connected to the CallManager. The available parameter setting is:

- **InActivePhoneThreshold**—Contains upper threshold for inactive phones expressed as a percentage of the total phones connected to the Cisco CallManager. The default value is 20.

### Threshold Setting—CPU and Physical Memory (RAM)

CPU and memory settings configure the performance monitoring of a system’s CPU and its associated memory elements. The available parameter settings are:

- **FreePhysicalMemoryThreshold**—Contains minimum acceptable free physical memory expressed as a percentage of the total amount of physical memory. The default value is 15.
- **ProcessUtilizationThreshold**—The upper threshold for processor utilization expressed as a percentage of the total capacity of the processor. The default value is 90.

### Threshold Setting—Disk Usage and Virtual Memory

Disk Usage and Virtual Memory settings monitor the performance of disk usage and virtual memory elements. Events such as high disk utilization and high virtual memory utilization are controlled by the following parameters:

- **FreeHardDiskThreshold**—Threshold for minimum amount of hard disk space expressed as a percentage of the total hard disk memory. The default value is 15.
- **FreeVirtualMemoryThreshold**—Threshold for minimum amount of free virtual memory expressed as a percentage of total virtual memory. The default value is 15.

### Threshold Setting—Environment: RIB Card

- **BatteryPercentChargedThreshold**—Low threshold setting, expressed as a percent of battery charge. The default value is 20.

### Threshold Setting—Environment: Temperature Sensor

- **TemperatureCelsiusThreshold**—Temperature threshold in degrees Celsius. The default value is 30.

# Scheduling Inventory Collection

You can schedule periodic inventory collection for VHM.

These topics explain the process:

- [Impact of Scheduling on VHM Inventory Collection, page 5-21](#)
- [How VHM Inventory Collection Works, page 5-22](#)
- [Ensuring Accurate VHM Inventory Collection, page 5-22](#)
- [Changing Inventory Collection Schedule, page 5-23](#)
- [Deleting Devices from Inventory, page 5-24](#)

## Impact of Scheduling on VHM Inventory Collection

During a scheduled VHM inventory collection run, the following sequence of events occur:

1. VHM synchronizes its inventory with DFM inventory. During synchronization only new voice enabled devices in DFM are imported in VHM.

**Note**

---

For VHM to synchronize with the most up-to-date DFM inventory, Network Administrators must set the DFM Rediscovery Schedule so that DFM rediscovery completes before VHM inventory collection starts.

---

2. A 15-minute delay ensues, to allow all new devices to be imported before VHM inventory collection starts.
3. VHM inventory collection starts. The order in which VHM devices are discovered is controlled so that registration relationships between Voice Gateways and CallManagers can be tracked by VHM. VHM rediscovers devices in the following order:
  - a. CallManager ICS 7750 and Media Servers are rediscovered.
  - b. A 5-minute delay allows time to put the CallManagers back in inventory after rediscovery.

- c. Voice Gateways and Inline Power Switches are rediscovered.
- d. Unsupported and undiscovered devices are rediscovered.

## How VHM Inventory Collection Works

During VHM inventory rediscovery, a device is deleted from the VHM repository and then rediscovered. If you look at the Real-Time Dashboard during rediscovery, you will see that the device is removed from the Real-Time Dashboard window and then added again when rediscovery completes.

## Ensuring Accurate VHM Inventory Collection

To ensure accurate VHM inventory collection:

- Schedule VHM inventory collection scheduling to start after DFM Rediscovery Schedule completes. This ensures that all the newest devices are available in the DFM inventory before VHM synchronizes its inventory with DFM.
- Use only VHM inventory collection scheduling, because its sequencing guarantees that the correct registration relationships are included in VHM inventory. Avoid using the Inventory Collect All menu option from the Administration Console. If you use the Inventory Collect All option, the sequence in which devices are discovered is not guaranteed. As a result, Voice Gateways may be discovered before CallManagers. For Voice Gateways that are registered to a CallManager, the registration relation between the two is created in the VHM repository if the sequence of the objects' creation is altered.

## Changing Inventory Collection Schedule

By default, inventory collection runs at 3:00 a.m every day.

To change the inventory collection schedule:

- 
- Step 1** From the CiscoWorks2000 desktop, select **Voice Health Monitor > Administration > Inventory Collection Scheduling**. The Inventory Collection Schedule window is displayed.
- Step 2** From the Inventory Collection Scheduling window, select values for the following parameters to change the current settings.

**Table 5-14** *Inventory Collection Scheduling Settings*

Parameter	Description
Start Date	Specifies the day, month, and year on which the first inventory collection will be scheduled.
Time	Specifies the hour and minute at which inventory collection will be triggered.
Frequency	Specifies the intervals at which inventory collection happens. The options are Weekly and Daily.

- Step 3** Click **OK**.
-

## Configuring the Timeout Interval and Retries for Device Discovery

If an SNMP query does not respond in time, VHM will timeout. It will then retry contacting the device for as many times as listed under the `snmpretries` attribute in the configuration file. The timeout period is doubled every subsequent retry. For example, if the timeout is 4 seconds and the retries are 3 (these are the default values), VHM waits for 4 seconds, then it waits for 8 seconds and in the third try it waits for 16 seconds.

You can configure the SNMP timeout interval and the number of retries used for VHM device discovery.

To configure the SNMP timeout interval and the number of retries:

- 
- Step 1** Using Windows Explorer on your VHM machine open the following folder: `cscopx\objects\vhm\inventorycollector` folder.
  - Step 2** Open the `InventoryConfig.conf` file using a text editor (notepad).
  - Step 3** Edit the value of the properties for `snmptimeout` (in seconds) and `snmpretries` to the desired values.
  - Step 4** Save the file.
  - Step 5** Stop and restart the CW2000 Daemon Manager through the Services window from the Windows 2000 desktop. This is required for the changes to take effect.

## Deleting Devices from Inventory

You can delete devices from inventory using the inventory view in the Administration Console. The general procedures for managing and unmanaging objects are described in the *Device Fault Manager User Guide*.

To delete a device from the VHM domain:

- 
- Step 1** Select a system level object from one of the following classes:
    - MediaServer
    - VoiceGateway
    - ICS

- InlinePowerSwitch

A system level object is the top level object within a class.



---

**Note** Do not select devices from the Composed Of list for any system level object.

---



---

**Note** Do not delete devices from the following classes: Voice Cluster, Voice Services, WorkFlowApp, or CiscoCallManager.

---

**Step 2** Right-click the object you want to delete, and select Delete from the menu.

---

## Configuring Trap Receiving

This topic explains how to change the default port number that VHM uses to receive traps. VHM is completely dependent on DFM to receive traps from voice-enabled devices. When you configure VHM trap receiving, you must also configure the DFM trapd.conf file to reflect the new port number so that VHM continues to receive traps from DFM.



---

**Note** The default value for the VHM trap port is 9009. The default value for the DFM trap port is 162. For trap port configuration scenarios in which both DFM and a Network Management System are in use, please refer to *Device Fault Manager User Guide*. See the [“Ports and Protocols Used by VHM and DFM” section on page 7-5](#) for a complete list of ports used by both products.

---

To configure the trap port number:

- 
- Step 1** Click **Voice Health Monitor > Administration > Trap Configuration > Trap Receiving**. The VHM Trap Receiving window appears.
- Step 2** Modify the port number.
- Step 3** Modify the DFM trapd.conf file with the new VHM trap receiving port number:

- If DFM is installed on the same machine:
  - You can select **Yes** for **Update the DFM trapd.conf file automatically?** and click **OK**
  - or
  - You can select **No**, click **OK**, and then manually update the DFM trapd.conf file
- If DFM is installed on another machine, you must manually update the trapd.conf file.

**Note**

---

The *Device Fault Manager User Guide* contains complete instructions for updating the DFM trapd.conf file.

---

## Configuring Fault Notification

You can configure fault notification adapters to forward event information to recipients on the network. VHM provides three types of fault notification adapters:

- **File Notifier Adapter**—Logs alarms detected by the VHM server and forwards them to a file. A file is the only valid recipient for this adapter. Use this adapter to create a historical file containing all alarms generated by VHM.
- **Mail Notifier Adapter**—Uses SMTP to send mail notifications to recipients. Like the Trap Notifier Adapter, you can specify the recipients—in this case, an email address. Use this adapter to generate asynchronous email notifications when one or more alarm conditions occur. For example, you could use the Mail Notifier Adapter to send an epage to a specified list of recipients. For less serious faults, you might want to forward the notifications to a list of email addresses.
- **Trap Notifier Adapter**—Converts alarms into SNMP trap messages and forwards the traps to recipients. You can specify the recipients, such as network management systems or other domain managers, using an IP address

or a system name. Use this adapter to send alarms to another application or NMS for additional processing or display. The format of the converted SNMP trap messages is provided in the *Device Fault Manager User Guide*.

**Note**

---

When you configure any adapter using the command line, if the adapter is running, you must stop and restart it for the new configuration file to take effect. You can do this by using the GUI to disable (stop) and enable (restart) the adapter.

---

## Using the GUI to Configure Adapters

Configuring an adapter using the GUI automatically restarts the CiscoWorks2000 process associated with the adapter.

Adapter	VHM GUI Choice	For more information, refer to...
File Notifier Adapter	<b>Voice Health Monitor &gt; Administration &gt; Fault Notification &gt; File Notifier</b>	<a href="#">Configuring the File Notifier Adapter, page 5-35</a>
Mail Notifier Adapter	<b>Voice Health Monitor &gt; Administration &gt; Fault Notification &gt; Mail Notifier</b>	<a href="#">Configuring the Mail Notifier Adapter, page 5-40</a>
Trap Notifier Adapter	<b>Voice Health Monitor &gt; Administration &gt; Fault Notification &gt; Trap Notifier</b>	<a href="#">Configuring the Trap Notifier Adapter, page 5-45</a>

A VHM adapter process starts when you enable the adapter from its GUI and stops when you disable it from the GUI.

When an adapter starts, its configuration information is loaded from a file. The configuration files have the extension .conf and are located in directories under the directory *NMSROOT*\objects\smarts\vhm-conf.



### Note

NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.



### Caution

Do not rename the configuration files or move them. Adapters that cannot find the required configuration file will not run.

## Using the Command Line to Configure Adapters

To change the configuration of an adapter using the command line:

- 
- Step 1** Locate the configuration file for the given adapter. The configuration files are located in the *NMSROOT*\objects\smarts\vhm-conf directory; the file names are listed in the sections that provide detailed information about the adapters.



---

**Note** NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

---



---

**Note** Save a copy of any configuration file you intend to change, and mark it as a backup file.

---

- Step 2** Use any text editor to change the parameters. Change only the parameters listed. To change notification adapter subscriptions, follow the instructions in the [“Changing Subscriptions for Notification Adapters”](#) section on page 5-29.
- Step 3** Save the edited configuration file.
- Step 4** Stop and restart the CiscoWorks2000 process that runs the adapter by disabling and enabling the adapter using the GUI.
- 

## Changing Subscriptions for Notification Adapters

The File Notifier, Mail Notifier, and Adapter Trap Notifier configuration files contain a *SubscribesTo* parameter that specifies the devices and notifications the adapter should monitor. This allows you to tailor the adapters to track only the information you want.

The following topics describe how to use subscriptions with notification adapters.

## Specifying a Notification Adapter's Subscription Profile

You can directly edit a notification adapter configuration file to specify a particular subscription profile (profileName), which identifies the events the adapter will track. (Creating subscription profiles is described in the *Device Fault Manager User Guide*.)



### Note

The profileName must match an existing VHM subscription profile.

```
SubscribesTo =
{
    GA_ProfileSubscription::Filelog-Default-Profile-Subscriptions
    {
        profileName = "default"
    }
}
```

## Specifying Particular Events to Be Tracked by a Notification Adapter

You can directly edit a notification adapter configuration file to specify the events to which a notification adapter will subscribe. The device parameters for subscriptions include:

className	Type of managed element (for example, Cisco CallManager).
instanceName	Objects that describe the managed element (for example, CCM—routers.cisco.com).
eventName	Name of compound or symptom to be reported for the managed element (for example, Power Supply Down).
aggregates	Compound events. If set to TRUE, sends a notification when the selected compound events occur.
symptoms	Symptomatic events. If set to TRUE, sends a notification when the selected symptomatic events occur.

A complete list of valid classes, instances, and events is provided in [Table 5-15](#). This method is normally used with the Mail Notifier Adapter and Trap Notifier Adapter. The File Notifier Adapter is ready to use; normally, you will want to enable only the File Notifier Adapter to create one repository for all generated alarms.

[Table 5-15](#) lists the classes, instances, and events supported by DFM.

**Table 5-15 Supported Subscription Classes, Instances, and Events**

<b>Class</b>	<b>Instance</b>	<b>Event (Symptom/Compound)</b>
VoiceGateway	.*	Unresponsive (S)
Processor	.*	HighUtilization (S)
DeviceMemory	.*	InsufficientFreeMemory (S)
DeviceTemperatureSensor	.*	TemperatureSensorDown (S)
DeviceTemperatureSensor	.*	TemperatureSensorDegraded (S)
Fan	.*	FanDown (S)
Fan	.*	FanDegraded (S)
PowerSupply	.*	PowerSupplyDown (S)
PowerSupply	.*	PowerSupplyDegraded (S)
InlinePowerSwitch	.*	Unresponsive (S)
VoiceInterface	.*	InterfaceAdministrativelyDown (S)
VoiceInterface	.*	InterfaceOperationallyDown (S)
VoicePort	.*	VoicePortOperationallyDown (S)
VoicePort	.*	VoicePortAdministrativelyDown (S)
VoiceCard	.*	CardDown (S)
RAM	.*	InsufficientFreePhysicalMemory (S)
VirtualMemory	.*	InsufficientFreeVirtualMemory (S)
HardDisk	.*	InsufficientFreeHardDisk (S)
SystemProcessor	.*	HighProcessorUtilization (S)
SystemPowerSupply	.*	PowerSupplyDown (S)
SystemPowerSupply	.*	PowerSupplyDegraded (S)

**Table 5-15 Supported Subscription Classes, Instances, and Events (continued)**

<b>Class</b>	<b>Instance</b>	<b>Event (Symptom/Compound)</b>
SystemFan	.*	FanDown (S)
SystemFan	.*	FanDegraded (S)
SystemTemperatureSensor	.*	TemperatureSensorDown (S)
SystemTemperatureSensor	.*	TemperatureSensorDegraded (S)
SystemInterface	.*	InterfaceOperationallyDown (S)
SystemInterface	.*	InterfaceAdministrativelyDown (S)
SystemTemperatureSensor	.*	TemperatureHigh (S)
CiscoCallManager	.*	CallManagerDown (S)
VoiceGateway	.*	ConnectivityException (C)
SkinnyVoiceGateway	.*	ConnectivityException (C)
SkinnyVoiceInterface	.*	InterfaceOperationallyDown (S)
WorkFlowApp	.*	ApplicationDown (S)
SNMPAgent	.*	Unresponsive (S)
MediaServer	.*	Unresponsive (S)
MRP	.*	Unresponsive (S)
MRP	.*	HighUtilization (S)
MRP	.*	InsufficientFreeMemory (S)
SSP	.*	Unresponsive (S)
SSP	.*	InsufficientFreeMemory (S)
SSP	.*	HighUtilization (S)
SPE	.*	Unresponsive (S)
ICSPowerSupply	.*	PowerSupplyDown (S)
ICSPowerSupply	.*	PowerSupplyDegraded (S)
ICS	.*	Unresponsive (S)
ICS	.*	EntityDown (S)
CiscoCallManager	.*	SyntheticPhoneRegistrationFailed (S)
CiscoCallManager	.*	SyntheticEmptyCallFailed (S)

**Table 5-15 Supported Subscription Classes, Instances, and Events (continued)**

Class	Instance	Event (Symptom/Compound)
CiscoCallManager	.*	SyntheticOffHookTransactionFailed (S)
CiscoCallManager	.*	SyntheticEndtoEndCallFailed (S)
CiscoCallManager	.*	SyntheticPhonetoGatewayCallFailed (S)
CiscoCallManager	.*	SyntheticPhonetoBridgeCallFailed (S)
VoiceServices	.*	SyntheticTransactionFailed (S)
VoiceServices	.*	ApplicationDown (S)
RIBCard	.*	BatteryDisconnected (S)
RIBCard	.*	BatteryFailed (S)
RIBCard	.*	BatteryLow (S)

In the following example, the Mail Notifier Adapter will report all Operational Exception aggregates (compound events) that occur on any voice gateway managed by VHM:

```
SubscribesTo =
{
    GA_ChoiceSubscription::Mail-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = "VoiceGateway"
        instanceName = ".*"
        eventName = "OperationalException"
        aggregates = TRUE
        symptoms = FALSE
    }
}
```

According to the following example, the Mail Notifier Adapter will report when the state of any power supply managed by VHM is not normal:

```
SubscribesTo =
{
    GA_ChoiceSubscription::Mail-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
```

```

        className = "PowerSupply_Fault.*"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    }
}

```

According to the following example, the Mail Notifier Adapter will report all interface performance events that occur on any interface managed by DFM:

```

SubscribesTo =
{
    GA_ChoiceSubscription::Mail-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = "Interface_Performance.*"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    }
}

```

According to the following example, the Mail Notifier Adapter will send a report when the state of any MediaServer class or VoiceCluster class managed by VHM is not normal:

```

SubscribesTo =
{
    GA_ChoiceSubscription::MediaServer-All-Subscriptions
    {
        className = "MediaServer"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    },
    GA_ChoiceSubscription::VoiceCluster-All-Subscriptions
    {
        className = "VoiceCluster"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    }
}

```

```
}

```

In the following example, the Mail Notifier Adapter will report all high utilization events that occur on any interface managed by VHM:

```
SubscribesTo =
{
    GA_ChoiceSubscription::Mail-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = ".*"
        instanceName = ".*IF-.*"
        eventName = "HighUtilization"
        aggregates = TRUE
        symptoms = TRUE
    }
}
```

## Configuring the File Notifier Adapter

The File Notifier can log alarms detected by the VHM server and store them in a file. You can use either the GUI or the command line to configure this adapter. The GUI lets you do essential configuration, while the command line lets you fine-tune the adapter. For more information, see the [“Using the Command Line to Configure the File Notifier Adapter”](#) section on page 5-36.

### Using the GUI to Configure the File Notifier Adapter

You can enable or disable logging alarms detected by VHM in a log file.

To configure the file notifier adapter:

- 
- Step 1** Click **Voice Health Monitor > Fault Notification > File Notifier**. The File Notifier window appears.
  - Step 2** In the Adapter field, select **ENABLED** or **DISABLED** to enable or disable event logging in the alarms file.
  - Step 3** Click **OK**.
-

This procedure does the following:

- Enables or disables the process with CiscoWorks2000.
- Creates a log file for the file notifier  
NMSROOT\objects\smarts\logs\vhm\_filelog\_notifier.log.
- Creates the alarm file NMSROOT\objects\smarts\logs\VHM-alarms.log.



**Note**

---

NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

---

You do not need to restart CiscoWorks2000 for your changes to take effect. The GUI does this for you automatically.

To specify the types of notifications that you want forwarded to the alarms file, use the command line (refer to the [“Using the Command Line to Configure the File Notifier Adapter”](#) section on page 5-36).

## Using the Command Line to Configure the File Notifier Adapter

This topic shows the contents of the file notifier adapter configuration file (NMSROOT\objects\smarts\vhm-conf\notifier\vhm\_filelog\_notify.conf).



**Note**

---

NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

---

[Table 5-16](#) lists the parameters that you can change using the command line. Additional configuration of this file is normally not required.

```
#
# This is a configuration file which contains objects for the
# file-log adapter.
#
# Based on GNA - the Generic Notification Adapter framework
#
# $Id: vhm_filelog_notify.conf,v 1.1 2000/11/30 22:14:19 svl Exp $
#
#
```

```

# The GNA notifier object.
#
GNA_Notifier::vhm-filelog-Notifier
{
    serverName = "VHM"

# How long to wait, in seconds, before beginning to send events.
# Default is 1 sec., to prevent a flood of notifications
# upon adapter startup.
    initialEventDelay = 0

    ProvidesAdditionalParams =
Filelog_AdapterParams::file_Notifier-Parameters
    {
    }

    ReadsInputFrom = GA_SubscriberFE::Filelog_Subscriber-FrontEnd
    {
        # How long an event must remain active before the adapter
        # sends a notification, in units of seconds.
        eventSmoothingInterval = 0

        # Notification threshold; discard notifications with a
        # certainty below this value.
        minimumCertainty = 0.01
        SubscribesTo =
        {
GA_ProfileSubscription::Filelog-Default-Profile-Subscriptions
            {
                profileName = "default"
            }
        }
    }

# No user-serviceable parts below here.
#
start_stopRuleSet = "filelog/filelogInit.asl"

    adapterRuleSet = "filelog/filelogNotify.asl"

    PerformsSend = FilelogAction::filelog_Interface
}

```

According to the following example, the File Notifier Adapter will report, to an alarm log file, when the state of any VoiceGateway or MediaServer class managed by VHM is not normal:

```
SubscribesTo
{
    #GA_ProfileSubscription::Filelog-Default-Profile-Subscriptions
    #{
        #           profileName = "default
    #}
    GA_ChoiceSubscription::All-Subscriptions1
    {
        className = "VoiceGateway"
        instanceName = ".*"
        eventName = ".*"
        # Include problems, but omit symptoms and aggregates.
        problems = TRUE
        aggregates = TRUE
        symptoms = TRUE
    },

    GA_ChoiceSubscription::All-Subscriptions2
    {
        className = "MediaServer"
        instanceName = ".*"
        eventName = ".*"
        # Include problems, but omit symptoms and aggregates.
        problems = TRUE
        aggregates = TRUE
        symptoms = TRUE
    }
}
```

## File Notifier Adapter Command Line Parameters

Table 5-16 lists the File Notifier Adapter parameters that you can change.

**Table 5-16 File Notifier Adapter Parameters**

Parameter	Description
serverName	Default name of the VHM server to connect to. Note that this is the name of the VHM server, not the name of the host it is running on. The default is VHM.
initialEventDelay	Time interval (in seconds) the adapter should wait before accepting events from the VHM server. The default value is 1.
eventSmoothingInterval	Time (in seconds) that an event must remain in its current state before the adapter sends a notification. If the event is cleared before the event smoothing interval expires, it is not sent. The default value is 0 seconds.
minimumCertainty	Threshold above which notifications are logged. Any notification with a certainty below the threshold is discarded. Values may range from 0.0 to 1.0. The default value is 0.01.
SubscribesTo	Devices and types of notifications an adapter subscribes to. The default is all notifications and devices. Refer to the <a href="#">“Changing Subscriptions for Notification Adapters”</a> section on page 5-29.

After you change the File Notifier Adapter file, you must stop and restart the adapter process by using the GUI to disable and then enable the adapter. See the [“Configuring the File Notifier Adapter”](#) section on page 5-35 for instructions.

## Alarm Log Example

The following is an example of the VHM alarm log file, *NMSROOT/objects/smarts/logs/VHM-alarms.log*:

```
06-Mar-2001 10:45 AM NOTIFY
RAM::RAM-vhm-ccm3.cisco.com::InsufficientFreePhysicalMemory 100%
Physical Memory(RAM) is insufficient.

06-Mar-2001 03:03 AM NOTIFY
SkinnyVoiceInterface::SVI-SkinnyVG-SDA00908F003434::InterfaceOperation
allyDown 100% Skinny Voice Interface is operationally down.
```

```
06-Mar-2001 12:37 PM NOTIFY
SkinnyVoiceInterface::SVI-SkinnyVG-SDA0001C9D8DD3A::InterfaceOperation
allyDown 100% Skinny Voice Interface is operationally down.

06-Mar-2001 10:56 AM NOTIFY
CiscoCallManager::CCM-vhm-ccm4.cisco.com/1::SyntheticEmptyCallFailed
100% The synthetic transaction to initiate a call failed.

05-Mar-2001 05:51 PM NOTIFY
CiscoCallManager::CCM-vhm-ccm4.cisco.com/1::SyntheticPhonetoGatewayCal
lFailed 100% The synthetic transaction to perform a Phone to Gateway
call failed.

05-Mar-2001 05:51 PM NOTIFY
CiscoCallManager::CCM-vhm-ccm4.cisco.com/1::SyntheticPhonetoBridgeCall
Failed 100% The synthetic transaction to perform a Phone to Conference
Bridge call failed.

05-Mar-2001 05:51 PM NOTIFY
CiscoCallManager::CCM-vhm-ccm4.cisco.com/1::SyntheticEndtoEndCallFaile
d 100% The synthetic transaction to perform an end to end call failed.
```

## Configuring the Mail Notifier Adapter

The Mail Notifier adapter sends email notifications to a specified list of recipients via SMTP. The email adapter is configured to subscribe to a list of notifications and to send those notifications to a specified mailbox or group of mailboxes.

You can configure the mail notifier using the GUI or the command line. The GUI lets you do essential configuration, while the command line lets you fine-tune the adapter.



---

**Note**

If you do not use the command line to fine-tune the adapter, you will receive email for all events.

---

For more information see the [“Using the Command Line to Configure the Mail Notifier Adapter”](#) section on page 5-42.

## Using the GUI to Configure the Mail Notifier Adapter

To notify other users of VHM alarms:

- 
- Step 1** Click **Voice Health Monitor > Fault Notification > Mail Notifier**. The Mail Notifier screen appears.
  - Step 2** In the Adapter field, select **ENABLED** or **DISABLED** to enable or disable mail notification.
  - Step 3** In the Add Recipient field, enter the username for the user you want to notify about VHM events and alarms.
  - Step 4** If you want to remove a recipient, select the recipient from the Remove Recipient field.
  - Step 5** In the SenderId field, enter the email address of the sender.
  - Step 6** In the MailServer field, enter the fully qualified domain name of the mail server.
  - Step 7** Click **OK**.
- 

This procedure does the following:

- Enables or disables the process and registers or unregisters the process with CiscoWorks2000.
- Updates the Mail Notifier Adapter configuration file  
*NMSROOT*\objects\smarts\vhm-conf\notifier\vhm\_mail\_notify.conf.

**Note**

*NMSROOT* is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

You do not need to restart CiscoWorks2000 for your changes to take effect. The GUI does this for you automatically.

To log all mail messages or specify the types of notifications that you want to monitor, use the command line (see the [“Using the Command Line to Configure the Mail Notifier Adapter”](#) section on page 5-42).

## Using the Command Line to Configure the Mail Notifier Adapter

Before editing the configuration file, disable the adapter. See the [“Configuring the Mail Notifier Adapter” section on page 5-40](#) for instructions.

This topic shows the contents of the mail notifier adapter configuration file (*NMSROOT\objects\smarts\vhm-conf\notifier\mail\_notify.conf*).



### Note

NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOpx.

[Table 5-17](#) lists the parameters that you can change using the command line.

```
#
# This is a configuration file which contains objects for the
# mail notification adapter.
#
# Based on GNA - the Generic Notification Adapter framework
#
# $Id: vhm_mail_notify.conf,v 1.1 2000/11/30 22:14:19 sv1 Exp $
#
#
# The GNA notifier object.
#
GNA_Notifier::vhm-mail-Notifier
{
    serverName = "VHM"

# How long to wait, in seconds, before beginning to send events.
# Default is 1 sec., to prevent a flood of notifications
# upon adapter startup.
    initialEventDelay = 0

# Additional parameters: A comma-separated list of recipients (who to
# send to); the email address of the sender; and the fully qualified
# domain name of the mail server.
    ProvidesAdditionalParams =
MailAdapterParams::mail_Notifier-Parameters
    {
# Recipients = "username@host.domain"
# SenderId = "daemon@localhost"
# MailServer = "mailhost.domain"

        Recipients = ""
```

```

        SenderId = ""
        MailServer = ""
    }

    ReadsInputFrom =
GA_SubscriberFE::mail_Notifier-Subscriber-FrontEnd
    {
# How long an event must remain active before the adapter sends a
# notification, in units of seconds.
        eventSmoothingInterval = 0

# Notification threshold; discard notifications with a certainty
# below this value.
        minimumCertainty = 0.01
        SubscribesTo =
        {
            GA_ChoiceSubscription::Mail-All-Subscriptions
            {
                className = ".*"
                instanceName = ".*"
                eventName = ".*"
                problems = TRUE
                aggregates = TRUE
                symptoms = TRUE
            }
        }
    }

    PerformsSend = MailAction::mail_NotifierInterface
    {
# Trace all outgoing email messages to stderr
        trace = FALSE
    }

# No user-serviceable parts below here.
#
        filterRuleSet = "mail-notify/mailFilter_Notify.asl"
        adapterRuleSet = "mail-notify/mail_Notify.asl"
    }

```

According to the following example, the Mail Notifier Adapter will send a report when the state of any MediaServer class or VoiceCluster class managed by VHM is not normal:

```
SubscribesTo =
{
    GA_ChoiceSubscription::MediaServer-All-Subscriptions
    {
        className = "MediaServer"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    },
    GA_ChoiceSubscription::VoiceCluster-All-Subscriptions
    {
        className = "VoiceCluster"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    }
}
```

## Mail Notifier Adapter Command Line Parameters

[Table 5-17](#) lists the Mail Notifier Adapter parameters that you can change.

**Table 5-17 Mail Notifier Adapter Parameters**

Parameter	Description
serverName	Default name of the VHM server to connect to. Note that this is the name of the VHM server, not the name of the host it is running on. The default is VHM.
initialEventDelay	Time interval (in seconds) the adapter should wait before accepting events from the VHM domain manager. The default value is 1.
Recipients	Comma-separated list of the recipients. The default is null.
SenderId	Address associated with the adapter.
MailServer	Fully qualified domain name for the mail server.

**Table 5-17 Mail Notifier Adapter Parameters (continued)**

Parameter	Description
eventSmoothingInterval	Time (in units of seconds) that an event must remain active before the adapter sends a notification. If the notification is cleared before the event smoothing interval expires, the notification is not sent. The smoothing interval also controls when notifications are changed. The default value is 0 seconds.
minimumCertainty	Threshold above which notifications are sent. Any notification with a certainty below the threshold is discarded. Values may range from 0.0 to 1.0. The default value is 0.1.
SubscribesTo	Devices and types of notifications an adapter subscribes to. The default is all devices and notifications. See the <a href="#">“Changing Subscriptions for Notification Adapters”</a> section on page 5-29.
trace	Setting for logging mail messages. The default is FALSE. If set to TRUE, log file is created in <i>NMSROOT</i> \objects\smarts\log\sm_mail_notifier.log.  <b>Note</b> NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOpX.

After you change the Mail Notifier Adapter file, you must stop and restart the adapter process by using the GUI to disable and then enable the adapter. See the [“Configuring the Mail Notifier Adapter”](#) section on page 5-40 for instructions.

## Configuring the Trap Notifier Adapter

You can use either the GUI or command line to configure the Trap Notifier Adapter. The GUI lets you do essential configuration, while the command line lets you fine-tune the adapter. For more information, see the [“Using the Command Line to Configure Adapters”](#) section on page 5-29.

## Using the GUI to Configure the Trap Notifier Adapter

The Trap Notifier adapter converts all VHM notifications into SNMP trap messages. The Trap Notifier sends the trap messages to specific recipients on the network.

To notify other hosts of VHM events and alarms:

- 
- Step 1** Click **Voice Health Monitor > Fault Notification > Trap Notifier**. The Trap Notifier window appears.
  - Step 2** In the Adapter field, select **ENABLED** or **DISABLED** to enable or disable trap notification.
  - Step 3** In the Add Recipient field, enter the hostname and port number of the machine you want to notify about VHM events and alarms.
  - Step 4** If you want to remove a recipient, select the recipient from the Remove Recipient field.
  - Step 5** Click **OK**.
- 

This procedure does the following:

- Enables or disables the process and registers or unregisters the process with CiscoWorks2000.
- Updates the Trap Notifier Adapter configuration file *NMSROOT\objects\smarts\vhm-conf\notifier\vhm\_trap\_notify.conf*.

**Note**

---

NMSROOT is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

---

You do not need to restart CiscoWorks2000 for your changes to take effect. The GUI does this for you automatically.

To save information about all handled traps in a log file, or specify the type of notifications that you want to listen for, use the command line (see the [“Using the Command Line to Configure the Trap Notifier Adapter”](#) section on page 5-47).

## Using the Command Line to Configure the Trap Notifier Adapter

This topic shows the contents of the Trap Notifier Adapter file (*NMSROOT*\objects\smarts\vhm-conf\notifier\vhm\_trap\_notify.conf).



### Note

*NMSROOT* is the directory where CiscoWorks2000 is installed on your machine. If you selected the default directory during installation, it is *C:\Program Files\CSCOPx*.

[Table 5-18](#) lists the parameters that you can change using the command line.



### Note

To create a log file for every trap handled by the adapter, set `dumpTrap` to `TRUE`. A log file is created in *NMSROOT*/objects/smarts/log/sm\_trap\_notifier.log.

```
#
# This is a configuration file which contains objects for the
# trap notification adapter.
#
# Based on GNA - the Generic Notification Adapter framework
#
# $Id: vhm_trap_notify.conf,v 1.1 2000/11/30 22:14:19 sv1 Exp $
#

#
# The GNA notifier object.
#
GNA_Notifier::vhm-trap-Notifier
{
    serverName = "VHM"

# How long to wait, in seconds, before beginning to send events.
# Default is 1 sec., to prevent a flood of notifications
# upon adapter startup.
    initialEventDelay = 0

# Additional parameters: a list of hosts (specified by host name,
# UDP ports and SNMP version ) to which the traps are sent.
# To add more hosts to the list, follow this format
# { {"host_name1", port_num1, "1"},
#   {"host_name2", port_num2, "2"} }
# Version number can only be 1 or 2. Currently only 1 is supported
```

```

ProvidesAdditionalParams =
Trap_AdapterParams::trap_Notifier-Parameters
{
recipients = { }
}

ReadsInputFrom = GA_SubscriberFE::trap_Subscriber-FrontEnd
{
# How long an event must remain active before the adapter sends a
# notification, in units of seconds.
eventSmoothingInterval = 0

# Notification threshold; discard notifications with a certainty
# below this value.
minimumCertainty = 0.01
SubscribesTo =
{
GA_ChoiceSubscription::Trap-All-Subscriptions
{
# Subscribe to events whose class, instance, and event
# names match the givent pattern.
className = ".*"
instanceName = ".*"
eventName = ".*"
# Include problems, but omit symptoms and aggregates.
problems = TRUE
aggregates = TRUE
symptoms = TRUE
}
}
}

# No user-serviceable parts below here.
#
filterRuleSet = "trap-notify/trapFilterNotify.asl"
adapterRuleSet = "trap-notify/trapNotify.asl"

PerformsSend = Trap_NotifierAction::trap_NotifierInterface {
dumpTrap = FALSE
}
}

```

According to the following example, the Trap Notifier Adapter will send a trap when the state of any MediaServer class or VoiceCluster class managed by VHM is not normal:

```

SubscribesTo =
{

```

```

GA_ChoiceSubscription::MediaServer-All-Subscriptions
{
    className = "MediaServer"
    instanceName = ".*"
    eventName = ".*"
    aggregates = TRUE
    symptoms = TRUE
},
GA_ChoiceSubscription::VoiceCluster-All-Subscriptions
{
    className = "VoiceCluster"
    instanceName = ".*"
    eventName = ".*"
    aggregates = TRUE
    symptoms = TRUE
}
}

```

## Trap Notifier Adapter Command Line Parameters

Table 5-18 lists the Trap Notifier Adapter parameters that you can change.

**Table 5-18** Trap Notifier Adapter Parameters

Parameter	Description
serverName	Default name of the server to connect to. Note that this is the name of the VHM server, not the name of the host it is running on. The default is VHM.
initialEventDelay	Time interval (in seconds) the adapter should wait before accepting events from the VHM. The default value is 1.
recipients	Table of addresses to send the SNMP traps to. Each row consists of three different values: host or IP address, socket number, and SNMP version (usually equal to 1). The values are separated by commas and enclosed in curly braces. In turn, the rows are also separated by commas and enclosed in curly braces. The default is null.
eventSmoothingInterval	Time (in seconds) that an event must remain in its current state before the adapter sends a notification. If the event is cleared before the event smoothing interval expires, it is not sent. The default value is 0 seconds.
minimumCertainty	Threshold above which events are logged. Any notification with a certainty below the threshold is discarded. Values may range from 0.0 to 1.0. The default value is 0.5.

**Table 5-18 Trap Notifier Adapter Parameters (continued)**

Parameter	Description
dumpTrap	If set to TRUE, causes information to be sent to the log file for every trap handled by the adapter. The default value is FALSE. If set to TRUE, log file is created in <i>NMSROOT\objects\smarts\log\sm_trap_notifier.log</i> .
SubscribesTo	Devices and types of notifications an adapter subscribes to. The default is all notifications and devices. Refer to the <a href="#">“Changing Subscriptions for Notification Adapters”</a> section on page 5-29.

After you change the Trap Notifier Adapter file, you must stop and restart the adapter process by using the GUI to disable and then enable the adapter. See the [“Using the GUI to Configure the Trap Notifier Adapter”](#) section on page 5-46 for instructions.

## Examples

These examples show how to configure the Trap Notifier Adapter so that VHM trap messages can be forwarded to a number of recipients (such as network management systems).

This code fragment shows you the format you should use:

```
# Additional parameters: a list of hosts (specified by host name,
# UDP ports and SNMP version ) to which the traps are sent.
# To add more hosts to the list, follow this format
# { {"host_name1", port_num1, "1"},
#   {"host_name2", port_num2, "2"} }
# Version number can only be 1 or 2. Currently only 1 is supported
```

```
ProvidesAdditionalParams =
Trap_AdapterParams::trap_Notifier-Parameters
{
recipients = { }
}
```

This example forwards trap messages to the recipient *host\_name1*:

```
#For case of one recipient:
ProvidesAdditionalParams =
Trap_AdapterParams::trap_Notifier-Parameters
{
recipients = {"host_name1", 162, "1"}
}
```

This example forwards VHM trap messages to the recipients *host\_name1* and *host\_name2*:

```
#For case of two recipients:
    ProvidesAdditionalParams =
    Trap_AdapterParams::trap_Notifier-Parameters
    {
    recipients = {"host_name1", 162, "1"},
    {"host_name2", port_num, "1" }
    }
```

This example forwards VHM trap messages to the recipients *host\_name1*, *host\_name2*, and *host\_name3*:

```
#For case of three recipients:
    ProvidesAdditionalParams =
    Trap_AdapterParams::trap_Notifier-Parameters
    {
    recipients = {"host_name1", 162, "1"},
    {"host_name2", port_num2, "1"},
    {"host_name3", port_num3, "1" }
    }
```

## Configuring ICS 7750 for Use with VHM

If you have an ICS 7750, you must enable minimal trace for each SPE CCM following the procedure in this topic. If trace is not enabled, VHM cannot obtain adequate information from the ccm Table in the CCM-MIB to monitor the health of the CCM.

To enable minimal trace on ICS 7750 SPE's Call Manager:

- Step 1** From the Cisco CallManager Administration pages in the Trace Configuration window:
- a. Select the Trace On check box to enable trace.
  - b. Configure SDI Trace settings with the following values.

Setting	Recommended Value
User Mask	11
Level	ERROR
Event	INFORMATION

- Step 2** From the Cisco CallManager Administration pages, enable SNMP in the Service Parameter window (EnableSNMP).

- Step 3** Restart the SPE through System Manager:

- a. From a command prompt, start the System Manager.  
For example:  
`\\<ip_address>\icsconfig`
- b. Click the shutdown/restart link.
- c. Click the restart button for the Primary SPE in the list.



**Note** In dual SPE systems, restarting the Primary SPE will trigger a failover. In dual SPE systems, repeat step 3 on the secondary SPE; restarting the secondary SPE switches back to the original Primary SPE.

# Configuring CCM for Use with VHM

For VHM to manage a CCM running on an MCS (Media Convergence Server), minimal trace must be enabled. It should be enabled by default in all CCMs running on an MCS.

If trace is not enabled, VHM cannot obtain adequate information from `ccmTable` in the CCM-MIB to monitor the health of the CCM.

To enable minimal trace on Cisco CallManager:

- 
- Step 1** Log into CCM:
- a. On your web browser's address line, enter the IP address of the CCM Administration page.  
For example enter:  
`http://ipaddressofccm/ccmadmin.`
  - b. Enter your username and password in the dialog box.  
The Cisco CallManager Administration window opens.
- Step 2** Select **Service** from the menu bar.
- Step 3** Select **Trace** from the drop-down menu.  
The Trace Configuration page opens.
- Step 4** From the CCM list on the left side of the page, click the IP address of the CCM you are configuring.  
The Configured Services dialog box opens.
- Step 5** Select Cisco CallManager from the list.  
The CallManager trace settings appear.
- Step 6** Set the trace settings:
- a. Verify that the Trace On check box is selected.
  - b. Set Level to ERROR.
  - c. Set User Mask to 11.
  - d. Set Event to INFORMATION.
- Step 7** Select **Service** from the menu bar.

- Step 8** Select **Service Parameters** from the drop-down menu.  
The Service Parameters Configuration page opens, listing the CCMs on the left side.
- Step 9** Click the IP address of the CCM you are configuring.  
The Configured Services box opens.
- Step 10** Select Cisco CallManager from the list.  
A window appears, displaying the Configured Service Parameters selection box.
- Step 11** Scroll down the list and select **EnableSnmp**.
- Step 12** Verify that the value is set to **T**.
- Step 13** Click **Update**.  
The snmp service on your CCM is updated.
-