



# Voice Health Monitor Overview

---

These topics provide an overview of the VHM application:

- [Overview of VHM, page 1-2](#)
- [How VHM Integrates with Third-Party NMSs, page 1-7](#)
- [Device Types that VHM Manages, page 1-7](#)
- [Locating the Supported Device List, page 1-9](#)
- [How VHM Works with the CiscoWorks2000 Server, page 1-9](#)
- [Starting the VHM Application, page 1-10](#)
- [Getting Started with VHM, page 1-10](#)

# Overview of VHM

VHM helps network administrators and network operators determine and maintain the stability of the VoIP network within their enterprise. VHM achieves this goal by using:

- A series of availability and health checks on the VoIP equipment in the network.
- A fault detection and escalation system to notify the users of any faults or exceptions detected.

VHM integrates with network management systems (NMSs) such as HP OpenView Network Node Manager.

With VHM, you can:

- Discover VoIP network devices and applications on a user-entered schedule
- Monitor faults in voice and data networks
- Run synthetic transaction tests, to check Cisco CallManager functions
- Check the availability and health of VoIP equipment and applications
- Obtain the status of each voice device group, such as Voice Cluster, Voice Gateway, Inline Power Switches, and Work Flow Apps

## How VHM Works

VHM manages the voice-specific devices in the network by polling information from managed devices, as well as processing SNMP Traps generated by the devices. VHM relies on DFM to receive the SNMP Traps. VHM does not duplicate queries for information collection, but shares the information collected by DFM.

Any polling analysis done in DFM can be leveraged by VHM. When polling devices, DFM polls generic parameters, while VHM polls voice-specific parameters. When VHM is used in conjunction with DFM, users can detect generic faults that are causing VoIP disruptions.

VHM correlates the collected information and generates events on voice components that can be viewed in alarm logs or on the Real-Time Dashboard. Users can also view device level faults in the DFM alarm log. Alarms for both VHM and DFM can be seen from the Monitoring Console.

VHM and DFM share many features as well as some components of their architectures. VHM and its commonality with DFM are described in more detail in the [“VHM and DFM Interdependencies” section on page 1-3](#).

## Event Correlation in VHM

Two types of events are generated by VHM: Compounds and Symptoms. One or more Symptoms generate compound or aggregated events. Symptoms are faults, such as Power Supply Down or Temperature Too High, which generate environment exceptions. Events are generated when fault conditions are detected and the event correlation cycle is reached. The event correlation cycle in VHM occurs every 30 seconds.

An example of an event correlation in VHM is TooManyInactivePhones. This event is generated when phones registered with call managers in a cluster become inactive and cross the InActivePhoneThreshold over a number of active phones. In this event, all the call managers in the cluster are monitored to find out the total number of phones that became inactive and compare that number with the total number of active phones in the cluster.

## VHM and DFM Interdependencies



### Note

---

For all DFM references in this guide, refer to the *Device Fault Manager User Guide* for more detailed information.

---

Device Fault Manager (DFM) and VHM both analyze Cisco device failures. The two products often identify problems before users of network services realize that a problem exists. Both VHM and DFM:

- Use a top-down approach that starts with users identifying problems and their symptoms:
  - Identify the problems affecting managed systems that are critical to correlate.
  - Describe the symptoms, developing a “problem signature” that specifies which conditions are present in a faulty element when the problem occurs.

- Create a causality mapping between the problems and the symptoms. Problems and symptoms are coded in correlation models that VHM and DFM use to:
  - Analyze network conditions.
  - Generate faults and exceptions.

The event information necessary to diagnose problems is present in the correlation model. Therefore, VHM and DFM monitor only the events necessary to diagnose problems.

Table 1-1 lists the interdependencies between VHM and DFM.

**Table 1-1 Interdependencies between VHM and DFM**

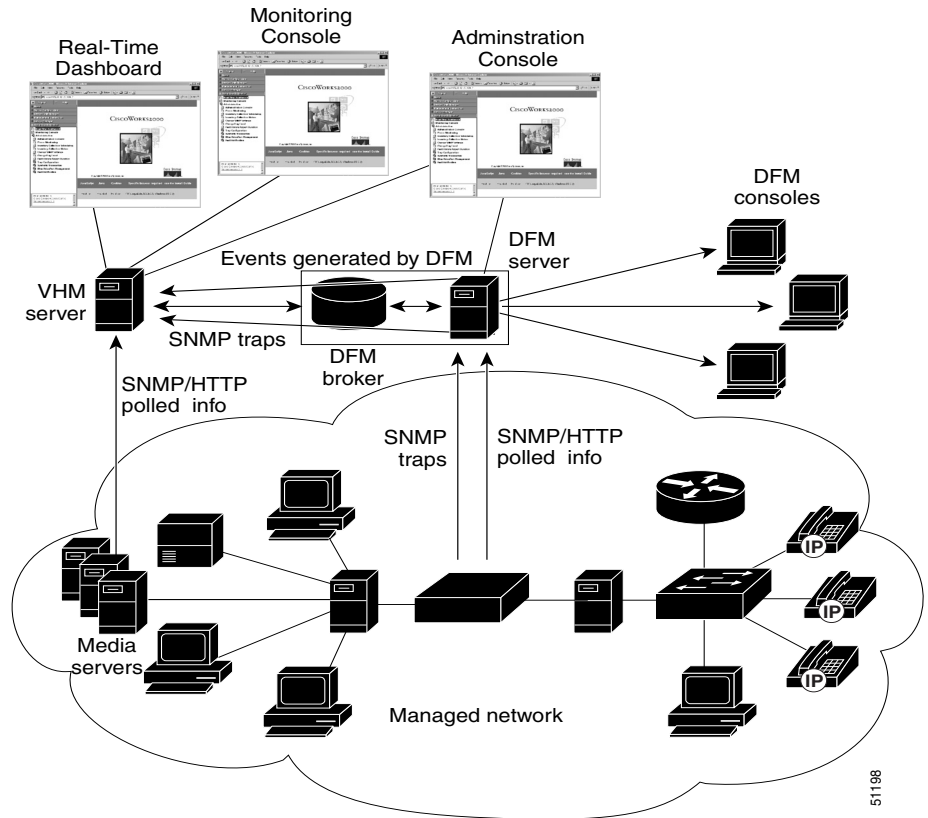
Component or Feature	Description of Dependency
DFM Installation	A DFM-compatible version of VHM must be installed either on the same machine as VHM or on a remote machine where it is network accessible to VHM. See <i>Installing and Setting Up Voice Health Monitor on Windows 2000</i> for server system requirements.
DFM Broker	<p>The DFM Broker maintains a list of active domain managers running on the network and registered with the DFM Broker. Domain managers are fault management server processes such as VHM and DFM. Each domain manager is identified by name and the IP address and port the domain manager is running on.</p> <p>The VHM installation process can find the DFM Broker if it is installed locally. If not, during installation, VHM prompts the user to enter the IP address and port for the DFM Broker. VHM then registers the VHM domain manager with the DFM broker.</p>
SNMP Trap Receiving	To receive SNMP traps for VoIP devices from DFM, VHM must update the trap forwarding filter in DFM. When DFM receives a trap, it forwards the trap based on the definition of the trap forwarding filter. The VHM trap receiver receives the trap and analyzes it to generate an event in VHM.

**Table 1-1 Interdependencies between VHM and DFM (continued)**

Component or Feature	Description of Dependency
Inventory Collection	<p>Inventory Collection performs two tasks at a user-scheduled time:</p> <ul style="list-style-type: none"> <li>• Synchronizes the VHM device list with DFM; during this process, voice-enabled devices that have been added to or deleted from DFM inventory will also be added to or deleted from VHM inventory.</li> <li>• Probes devices to find newly installed voice cards, ports, or voice applications.</li> </ul> <p>VHM also registers with DFM to receive device list update events. If any device is added or deleted, or becomes unresponsive, DFM sends an event alarm to VHM. VHM can process the event by, for example, starting to manage new voice-enabled devices.</p>
Alarm logs	<p>VHM generates voice faults and listens for element-level faults from DFM. If VHM receives an alarm for a device it manages, it uses the alarm in voice fault correlations. Alarms for devices that VHM does not manage are dropped.</p> <p>For more information about VHM fault browsers, see <a href="#">Chapter 2, “Monitoring Voice Network Health.”</a></p>
Device classification differences between VHM and DFM	<p>VHM and DFM classify devices differently. For example, Cisco routers and Catalyst switches are managed by both VHM and DFM. However, DFM classifies Cisco routers as Router class, while VHM classifies routers as Voice Gateways.</p> <p><b>Note</b> VHM manages only Cisco routers and Catalyst switches that have VoIP cards or ports. See the <a href="#">“Device Types that VHM Manages”</a> section on page 1-7 for more information.</p>
Polling and threshold parameters between VHM and DFM	<p>Threshold parameters for voice-enabled routers and switches must be set in DFM. However, threshold parameters for media servers must be set in VHM and are not shared with DFM.</p> <p>Polling parameters are not shared between VHM and DFM. However, it is best to synchronize them to avoid inconsistent polling of devices. Therefore, it is recommended that you set polling intervals the same in both VHM and DFM.</p>

Figure 1-1 illustrates the architecture that VHM shares with DFM.

**Figure 1-1 VHM Architecture**



# How VHM Integrates with Third-Party NMSs

VHM can be integrated with third-party vendors' NMSs such as HP OpenView Network Node Manager. VHM integrates with an NMS in two ways:

- Although VHM receives traps only from DFM, DFM can receive traps from an NMS or directly from devices. As a result, the traps DFM forwards to VHM may have come from an NMS or from a device.

See *Installing and Setting Up the Device Fault Manager on Solaris* for the default port numbers used by DFM and NMS and for example configuration scenarios to help you understand how DFM and NMSs can work together.

- VHM provides a trap notifier that allows you to:
  - Configure the port and IP address of the NMS that the trap notifier sends SNMP trap messages to.
  - Forward event notifications in the form of an SNMP trap to an NMS, when the NMS has been configured to listen on that port.

## Device Types that VHM Manages

The voice-specific devices managed by VHM are categorized by voice device group. [Table 1-2](#) lists the voice device groups and their descriptions.

**Table 1-2 Voice Device Groups**

Group	Description
VC (Voice Cluster)	All CallManagers in a voice cluster, and all the devices with voice cards that register with any CallManager in a cluster (including Voice Gateways and Skinny Voice Gateways).
WorkflowApplicationServer	Media servers that may be running workflow applications or Cisco voice applications.

**Table 1-2 Voice Device Groups (continued)**

Group	Description
InlinePowerSwitch	Catalyst switches that supply power to phones connected via Ethernet.
VoiceGateway	These include: <ul style="list-style-type: none"> <li>• Catalyst switches with:               <ul style="list-style-type: none"> <li>– Voice T1/E1</li> <li>– Transcoder</li> <li>– Conference bridge</li> <li>– Media termination points (MTPs)</li> <li>– Voice FXS</li> </ul> </li> <li>• IOS routers with:               <ul style="list-style-type: none"> <li>– FXS</li> <li>– FXO</li> <li>– T1 PRI/E1 PRI</li> </ul> </li> </ul>

For each voice device group, the following information is displayed on VHM Real-Time Dashboard:

- Number of devices in the group
- Number of devices that have a Critical level fault
- Number of devices that have a Warning level fault
- Number of devices whose status is Indeterminate

For further information on the Real-Time Dashboard and the individual information displayed for each voice device group, see the [“Using the Real-Time Dashboard”](#) section on page 2-1.

# Locating the Supported Device List

Device packages for all supported devices are installed when you install VHM. Information about devices installed with VHM can be found at:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/vhm/vhm1\\_0/supdv1\\_0.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/vhm/vhm1_0/supdv1_0.htm)

You can download device packages for new devices as they become available and find information about all supported devices from CCO at:

[www.cisco.com](http://www.cisco.com)

To find out which device packages are installed on your CiscoWorks2000 Server, select **Server Configuration > About the Server > Applications and Versions**.

## How VHM Works with the CiscoWorks2000 Server

VHM works in conjunction with the CiscoWorks2000 Server, which represents a common management foundation, providing a set of management services shared by multiple management applications. VHM uses these CiscoWorks2000 components:

- Desktop GUI
- Security
- Help Engine and Files
- Web Server/Servlet Engine
- User Accounts
- Widgets, Classes, and Libraries
- Java on SNMP Stack
- CMF Debugging Tools—LogMsg
- Process Management

# Starting the VHM Application

To start VHM from the CiscoWorks2000 desktop:

- 
- Step 1** Click the **Voice Health Monitor** drawer from the CiscoWorks2000 desktop.
- 

The following applications and folders are displayed:

- **Real-Time Dashboard**—Provides a summarized status of the voice network, grouping voice devices logically and allowing you to drill down into the details of each device and device group. See the [“Using the Real-Time Dashboard” section on page 2-1](#).
- **Monitoring Console**—Allows you to view the alarm logs that VHM and DFM have generated against devices. See the [“Using the Monitoring Console” section on page 2-14](#).
- **Administration**—Contains applications that users in administrative roles can use to configure and administer VHM. Users in operator roles may start and view the applications in the Administration folder but may not update any of the configuration data. See [Chapter 5, “Basic VHM Configuration.”](#)

## Getting Started with VHM

Table 1-3 contains the tasks necessary to use VHM to discover VoIP network devices and applications and to generate faults based on voice network events.

**Table 1-3** Getting Started Tasks

To perform this task...	Log in as this CiscoWorks2000 security role...	Then see...
Import voice network devices into VHM	Network Admin	<a href="#">“Managing and Unmanaging Voice Devices in VHM” section on page 5-4</a>
Adjust polling intervals and fault thresholds	Network Admin (Network Operator can view information only)	<a href="#">“Configuring Polling and Thresholds” section on page 5-10</a>

**Table 1-3 Getting Started Tasks (continued)**

<b>To perform this task...</b>	<b>Log in as this CiscoWorks2000 security role...</b>	<b>Then see...</b>
Configure VHM notifiers	Network Admin (Network Operator can view information only)	<a href="#">“Configuring Fault Notification” section on page 5-26</a>
Schedule inventory collection	Network Admin or Network Operator	<a href="#">“Scheduling Inventory Collection” section on page 5-21</a>
Configure synthetic transactions against CallManager	Network Admin or Network Operator	<a href="#">“Synthetic Transaction Overview” section on page 6-2</a>
Examine a Real-Time Dashboard Summary View of the voice network	Users in all five security roles may execute these tasks	<a href="#">“Using the Real-Time Dashboard” section on page 2-1</a>
Use the Real-Time Dashboard Status View for a voice device group	Users in all five security roles may execute these tasks	<a href="#">“Using the Status View” section on page 2-9</a>
Obtain device-specific information from the Real-Time Dashboard	Users in all five security roles may execute these tasks	<a href="#">“Using the Device Detail View” section on page 2-13</a>
View and respond to alarms	Users in all five security roles may execute these tasks	<a href="#">“Using the Monitoring Console” section on page 2-14</a>

