



VHM System Administration

These topics provide reference material for VHM system administrators and provide procedures for VHM system administration tasks.

VHM Administrator Reference

These topics contain no task-related information, but are provided for the reference of VHM system administrators:

- [Managing Client User Access, page 7-2](#)
- [Updating the VHM Host Server Name, page 7-5](#)
- [Updating the DFM Host Server Name, page 7-7](#)
- [Updating the DFM Username and Password, page 7-8](#)
- [Ports and Protocols Used by VHM and DFM, page 7-9](#)
- [Security Considerations, page 7-10](#)
- [How the DFM Broker Works, page 7-11](#)

Managing Client User Access

VHM gives you the ability to limit client user access to the Administration Console and Monitoring Console of VHM and DFM. Unauthorized users who try to access the Administration or Monitoring Console will get the following Console Load Error message:

```
Could not load console CustomizeAdminConsole.iccon
java.net.SocketException: Connection reset by peer: JVM_rcv in socket
input stream read
```

You cannot limit client user access to the Real-Time Dashboard, Inventory Collection Scheduling, Trap Configuration, Synthetic Transaction, or Fault Notification.

The following sections explain how to limit or view client user access to the Administration and Monitoring Consoles:

- [Updating Client User Access, page 7-2](#)
- [Updating Client User Access if DFM Is Not on the Local System, page 7-3](#)
- [Deleting Client User Access, page 7-4](#)
- [Viewing Client User Access, page 7-4](#)

Updating Client User Access

VHM uses the `aclupdate.exe` utility to update client user access.

To update client user access:

-
- Step 1** Install VHM.
- Step 2** After installation is completed and you have restarted the computer, open a DOS command prompt.
- Step 3** Use the `cd` command to access `NMSROOT\objects\vhm\bin` directory.



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

- Step 4** Enter the **aclupdate** command and the client user access.
- To give access to all client users, enter the following:
`aclupdate --default`
 - To limit access, enter the command **aclupdate** followed by the local host's IP address or server name and the list of users that you want to grant permission to (use the IP address or the server name of the systems, separated by commas).
For example, enter:
`d:\> aclupdate 172.22.125.33 vhm-dm1,172.22.125.40,vhm-tst2`

- Step 5** Press Enter.
The utility stops the CiscoWorks2000 Daemon Manager, updates the registry files, and then restarts the CiscoWorks2000 Daemon Manager.
-

Updating Client User Access if DFM Is Not on the Local System

If DFM and VHM are on separate systems, you must update the user access list on both systems.



Note

When setting the user access list, the list on the VHM server must contain the DFM IP address, and the list on the DFM server must contain the VHM IP address.

- To update the user access list on the VHM system, see the instructions in the [“Updating Client User Access” section on page 7-2](#).
- To update the user access list on the DFM system, either you can use the instructions listed in *User Guide for Device Fault Manager*, or you can use the same utility (aclupdate.exe) that you used on the VHM system.



Note

If you use the aclupdate.exe on the DFM system, you must first copy the utility from the VHM system to the DFM system.

Deleting Client User Access

You cannot delete individual client user access. You must delete the entire access list and create a new list.

To delete client user access:

Step 1 On your VHM system, open a command prompt and go to the directory where the `aclupdate.exe` utility is located. For instructions, see the [“Updating Client User Access” section on page 7-2](#).

Step 2 Enter the following command:

```
aclupdate --default
```

This command removes the old client user access list and gives access to all users. To limit client user access again, you must perform the steps in the [“Updating Client User Access” section on page 7-2](#).

Viewing Client User Access

You can view a list of the users who have client user access.

To view the Client User Access list:

Step 1 On your VHM system, open a command prompt and go to the directory where the `aclupdate.exe` utility is located. For instructions, see the [“Updating Client User Access” section on page 7-2](#).

Step 2 Enter the command:

```
aclupdate --show
```

This command displays a list of all users who belong to the client user access list. If access is set to default (all users), the client user access list does not appear; the statement `any host` appears instead.

Updating the VHM Host Server Name

If DFM is installed on the same system as VHM and the VHM host server name is changed, you must update the host server name in VHM.

To update the VHM host server name:

-
- Step 1** On the VHM system, open a DOS command prompt.
- Step 2** Add NMSROOT\objects\vhm\bin to the PATH Environment Variable
For example, enter:
- ```
set PATH=%PATH%;e:\progra-1\cscopx\objects\vhm\bin
```
- Step 3** Enter the **ServerNameChange** command.  
For example enter:
- ```
d:\> ServerNameChange
```
- Step 4** In the confirmation box that asks if you want to apply the name change to VHM, click **Yes**.
- Step 5** Click **OK** in the dialog box that reminds you to change the system name in the trapfilter.conf and trapd.conf files.
- Step 6** To reboot, click **Yes** in the confirmation dialog box.
- Step 7** Restart the DFM server so that your changes can take effect:
- On the VHM system, open a DOS command prompt.
 - In the DOS command prompt, enter

```
Set PATH=%PATH%;d:\progra-1\cscopx\objects\vhm\bin
```
 - Enter `pdterm DfmServer`.
 - Enter `pdexec DfmServer`.
-

Updating the VHM Host Server Name in the trapfilter.conf and trapd.conf Files

After you run the ServerNameChange utility, you need to manually update the trapfilter.conf and trapd.conf files with the new VHM host server name.

To update the trapfilter.conf and trapd.conf files:

-
- Step 1** On the VHM system, use a text editor to open the trapfilter.conf and trapd.conf files.

The trapfilter.conf file is located at NMSROOT\CSCOPx\cgi-bin\vhm.

The trapd.conf file is located at NMSROOT\CSCOPx\objects\smarts\conf\trapd.

- Step 2** In both files, remove the previous VHM host server name (old-pc) and enter the new name (new-pc).

For example:

Before:

```
MATCH:all
FORWARD:*. *.*.* .1.3.6.1.4.1.232 * * old-pc:9009
FORWARD:*. *.*.* .1.3.6.1.4.1.9.9.156.* * * old-pc:9009
FORWARD:*. *.*.* .1.3.6.1.4.1.2.6.159.* * * old-pc:9009
FORWARD:*. *.*.* .1.3.6.1.4.1.9.9.190.* * * old-pc:9009
```

After:

```
MATCH:all
FORWARD:*. *.*.* .1.3.6.1.4.1.232 * * new-pc:9009
FORWARD:*. *.*.* .1.3.6.1.4.1.9.9.156.* * * new-pc:9009
FORWARD:*. *.*.* .1.3.6.1.4.1.2.6.159.* * * new-pc:9009
FORWARD:*. *.*.* .1.3.6.1.4.1.9.9.190.* * * new-pc:9009
```

- Step 3** Save and close the file.
-

Updating the DFM Host Server Name

When DFM is installed on a remote system and it is moved or its host server name changes, you must update the DFM host server name in VHM.

**Note**

Make sure you sync the DFM username and password before you run the `ServerNameChange` command. If you are also changing the DFM username and password, you will need to update them in VHM. (See the [“Updating the DFM Username and Password”](#) section on page 7-8.)

To update the DFM host server name:

- Step 1** On the VHM system, open a DOS command prompt.
- Step 2** Enter the `ServerNameChange` command.
For example, enter:

```
d:\> ServerNameChange
```
- Step 3** In the confirmation message box that asks if you want to change the remote Broker information, click **Yes**.
- Step 4** The Brokers dialog box opens. Enter the new DFM host server name and port number.
If the broker is not running on the specified system, or if an invalid number is entered for the port number, a warning dialog box opens. Click **OK**, and enter the correct information.
- Step 5** A message appears, reminding you to append the contents of the `trapfilter.conf` file to the `trapd.conf` file in the DFM system. Click **OK**.
- Step 6** To reboot, click **Yes** in the confirmation message box.
- Step 7** Restart the DFM server so that your changes can take effect:
 - a. On the DFM system, open a DOS command prompt.
 - b. In the DOS command prompt, enter

```
Set PATH=%PATH%;d:\progra~1\cscopx\objects\vhm\bin
```

- c. Enter `pdterm DfmServer`.
 - d. Enter `pdexec DfmServer`.
-

Updating the DFM Host Server Name in the trapd.conf File

After you run the ServerNameChange utility, you need to manually update the trapd.conf file.

To update the trapd.conf file:

-
- Step 1** Using a text editor, open the trapfilter.conf file.
The trapfilter.conf file is located on the VHM system, at `NMSROOT\CSCOPx\cgi-bin\vhm`.
 - Step 2** Using a text editor, open the trapd.conf file.
The trapd.conf file is located on the DFM system, at `NMSROOT\CSCOPx\objects\smarts\conf\trapd`, on the DFM system.
 - Step 3** Copy the contents of the trapfilter.conf file and paste at the end of the trapd.conf file.
 - Step 4** Save the trapd.conf file.
 - Step 5** Close both files.
-

Updating the DFM Username and Password

When DFM is installed on a remote system and the DFM username and password are changed, you must update the DFM username and password in VHM. You must do this so that VHM can receive information from DFM.

**Note**

Updating the DFM username and password is required only when VHM and DFM are on separate systems. When they are on the same system, if the DFM username and password are changed, DFM automatically updates VHM with a new username and password.

To update the DFM username and password:

-
- Step 1** On the VHM system, open a DOS command prompt.
- Step 2** Open the NMSROOT/objects/vhm/bin directory.
- Step 3** Enter the **RemoteDFMConnect** command followed by the parameters **<username> <password> <host:port>**. The parameter **host:port** is the IP address and port number of the remote system where DFM is located.

For example, enter:

```
d:\> RemoteDFMConnect admin cisco 172.20.121.21:9002
```

The tool verifies the DFM version, and verifies that the username and password are correct.

When completed, a message appears stating the username and password have been updated.

- Step 4** On the VHM system, use the Services utility to stop and restart the CiscoWorks2000 daemon manger.
-

Ports and Protocols Used by VHM and DFM

VHM and DFM use the following ports and protocols.

- Ports:
 - 162—Default port number used by DFM for receiving traps.
 - 1099—Used by VHM for RMI.
 - 1775—Used by VHM to listen to the Synthetic Transaction server.
 - 43448—Used by AMA database engine
 - 42344—Used by AMA web service
 - 9000—Used by DFM for receiving traps if port 162 is occupied.
 - 9002—Used by the DFM Broker to listen to both the VHM server and the DFM server.
 - 9009—Default port number used by VHM for receiving traps from DFM

- Protocols:
 - SNMP
 - ICMP
 - TCP/IP
 - SMTP
 - RMI
 - HTTP

Security Considerations

Security for VHM files is based on the same standards used for CiscoWorks2000:



Caution

Do not change the protection of any file or directory to be less restrictive. You may, if you wish, make the protections more restrictive.

- File ownership and protection

All VHM files are installed with owner CASUSER. Only CASUSER can create, delete, or modify the files installed in *NMSROOT*.



Note

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



Note

File protections are not enforced on FAT partitions.

- Output Files

VHM is designed so that its output files can be written only to the VHM installation tree, which consists of the directories under *NMSROOT/objects/smarts*.

How the DFM Broker Works

The DFM Broker maintains information about domain managers such as the VHM server. Client applications, such as the Real-Time Dashboard, can determine where a domain manager is running by retrieving information from the DFM Broker. The DFM Broker works in the same way with both the VHM server and the DFM server.

See the *User Guide for Device Fault Manager* for more information about the DFM Broker, including:

- Information that the DFM Broker maintains
- How DFM (and VHM) clients find the DFM broker

VHM Administrator Tasks

VHM system administration can be performed only by the following types of users:

- Users in a CiscoWorks2000 System Admin role can perform system administration tasks that can be started from the CiscoWorks2000 desktop. These tasks include:
 - Backing up and restoring data
 - Starting and stopping CiscoWorks2000 processes
- Users who log on as local administrator to the system where VHM is installed can perform system administration tasks that can be started from the command line. These tasks include:
 - Viewing log files
 - Adjusting process file logging

Backing Up and Restoring VHM Data

A user logged on to CiscoWorks2000 in the System Admin role can back up CiscoWorks2000 data. CiscoWorks2000 uses a standard database structure for backing up all suites and applications. A sample directory structure for the CiscoWorks2000 Server (represented by the abbreviation vhms) follows.

Table 7-1 Sample VHM Backup Directory

Directory Path	Description	Usage Notes
/tmp/1	Number of backups	1, 2, 3...
/tmp/2/vhms	Application or suite	VHM backs up configuration files and log files.
/tmp/1/vhms/filebackup.tar	All CiscoWorks2000 server application tar files	Application data is stored in datafiles.txt and is compiled into a tar file.

The VHM backup files are stored in NMSROOT\backup\manifest\vhms\vhmserver\datafiles.txt.



Note

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

All files in the following directories are backed up:

- NMSROOT\objects\smarts\consoles
- NMSROOT\objects\smarts\repos
- NMSROOT\objects\smarts\logs
- NMSROOT\objects\smarts\vhm-conf\notifier
- NMSROOT\objects\smarts\vhm-conf\trapd

The VHM*.log files are backed up from the following directory:

- NMSROOT\log



Note

All VHM*.log files are backed up. There are no database files to back up.

Instructions for restoring data from a CiscoWorks2000 backup are included in CiscoWorks2000 data management online help.

Starting and Stopping VHM-Related CiscoWorks2000 Processes

The following table provides a complete list of VHM-related CiscoWorks2000 processes.

Table 7-2 VHM-Related CiscoWorks2000 Processes

Name	Description	Dependency
DfmBroker	<p>The DFM Broker maintains a registry about VHM and DFM domain managers. A domain manager registers the following information with the broker when its initialization is complete:</p> <ul style="list-style-type: none"> • Application name of the domain manager • Hostname where the domain manager is running • TCP port at which the HTTP server is listening <p>When a client needs to connect to the domain manager, it first connects to the broker to determine the hostname and TCP port where that server's HTTP service is listening. It then disconnects from the broker and establishes a connection to the domain manager.</p>	None

Table 7-2 VHM-Related CiscoWorks2000 Processes (continued)

Name	Description	Dependency
VHMServer	VHM domain manager; a VHM program that provides back-end services for VHM.	DfmBroker
VHMFileNotifier	Logs VHM analysis results into ASCII files (File Notifier Adapter).	VHMServer
VHMTrapNotifier	Converts VHM notifications into SNMP trap messages.	VHMServer
VHMMailNotifier	Monitors user-specified alarms and events and automatically emails notifications to specified recipients (Mail Notifier Adapter).	VHMServer
STServer ¹	Periodically runs synthetic transactions against Cisco CallManagers and provides real-time status updates to VHM.	AMADbEngine
AMADbEngine ¹	AMA Database Engine.	None
VHMSTIntegrator ¹	Integrates the VHM server with the ST server. Receives synthetic transaction messages from ST server and generates events to the VHM server.	STServer and VHMInventoryCollector
VHMDFMIntegrator	Integrates the DFM and VHM servers. Receives events and notifications from DFM and generates events on the VHM server.	VHMServer
VHMInventoryCollector	Synchronizes inventory with DFM. Handles all inventory events such as adding and deleting agents.	ESS
VHMInteractor	Provides inventory and device information to the Real-Time Dashboard; updates the Real-Time Dashboard with events.	VHMServer
VHMRMRegistry	Provides communication services for the VHMInteractor.	None

Table 7-2 VHM-Related CiscoWorks2000 Processes (continued)

Name	Description	Dependency
VHMPoller	<ul style="list-style-type: none"> Probes Digital Gateways and voice applications. Monitors connectivity between CallManager cluster and IP phones, Gateways and Gatekeepers. Provides suspect phone monitoring and ST results monitoring. 	VHMInventoryCollector

1. Throughout VHM, the terms Application Monitoring Appliance (AMA) and Synthetic Transaction (ST) are used interchangeably.

Stopping VHM-Related CiscoWorks2000 Processes

To stop CiscoWorks2000 processes:

-
- Step 1** To stop the VHMFileNotifier, VHMMailNotifier, and VHMTrapNotifier processes, disable them using the GUI. See the [“Using the GUI to Configure Adapters” section on page 5-37](#) for more information.
 - Step 2** To stop all other CiscoWorks2000 processes, log on to CiscoWorks2000 as an administrator.
 - Step 3** Select **Server Configuration > Administration > Process Management > Stop Process**. The Stop Process window opens.



Note If a process is not listed, it has not yet been started. In the Stop Process window, locate the process you want to stop in the Process drop-down list.



Note The VHM installation procedure sets VHMServer to start automatically, so it is normally listed. When you stop the VhmServer process, any users attached to VHM are detached. Use the Attach button to reattach when the VhmServer process is restarted.

Step 4 Select the process you want to stop and click the Finish button.

Restarting VHM-Related CiscoWorks2000 Processes

To restart CiscoWorks2000 processes:

-
- Step 1** To restart the VHMFileNotifier, VHMMailNotifier, and VHMTrapNotifier processes, enable them using the GUI. See the [“Using the GUI to Configure Adapters” section on page 5-37](#) for more information.
- Step 2** To restart all other CiscoWorks2000 processes, log on to CiscoWorks200 as an administrator.
- Step 3** Select **Server Configuration > Administration > Process Management > Start Process**. The Start Process window opens.
- Step 4** In the Start Process window, locate the process you want to start in the Process drop-down list.
- Step 5** Select the process you want to start and click the Finish button.
-

Viewing Log Files and Adjusting Process Logging

When troubleshooting a problem with the VHM system, Cisco TAC personnel may want to:

- View the contents of VHM log files.
- Adjust the trace level for a VHM process to increase the amount of information that is logged.

**Note**

Log files are for Cisco TAC use only.

To view VHM log files:

Step 1

From the CiscoWorks2000 desktop select, **Server Configuration > Administration > Log File**.

**Note**

Log files reflect the time zone in which the VHM server is located.

VHM processes that run on the server where VHM is installed write messages to the following files in the cscopx/log directory:

- VHMServer.log
- VHMInventoryCollector.log
- VHMInteractor.log
- VHMDFMIntegrator.log
- VHMSTIntegrator.log
- VHMPoller.log
- VHMDiscoveryJobCreate.log
- VHMDiscoveryJobDelete.log
- VHMDiscoveryJobSchedule.log
- VHMNotifier.log

Changing the Log Level

To change the logging level for VHM processes:

Step 1 From the CiscoWorks2000 desktop, select **Voice Health Monitor > Administration > Change Log Level**.

The Change Log Level screen appears.

Step 2 Check the check box next to the VHM process for which you want to change the log level. If you select All, the log level you select will apply to all VHM processes.

Step 3 Select the new log level from the drop-down menu.

The log levels to choose from are:

- Error
- Warning
- Trace
- Info

Step 4 Select **Apply**. If you want to see the default settings, select **Default**. The default settings will appear for all the VHM processes.

The log levels are set and the Log Level Settings window appears, showing the new settings.
