



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:

- [User Access, page 7-2](#)
- [Ports and Protocols Used by VHM and DFM, page 7-5](#)
- [Security Considerations, page 7-6](#)
- [How the DFM Broker Works, page 7-6](#)

User Access

VHM gives you the ability to limit 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_recv in socket
input stream read
```

You cannot limit 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 user access to the Administration and Monitoring Consoles:

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

Updating User Access

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

To update 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.
 - Step 4** Enter the `aclupdate` command and the user access.
 - To give access to all users, enter the following:

```
aclupdate --default
```

- To limit access, enter the command **aclupdate** followed by the local host's IP address or DNS name and the list of users that you want to grant permission to (use the IP address or the DNS name of the machines, separated by commas).

For example, enter:

```
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 User Access if DFM Is Not on the Local Machine

If DFM and VHM are on separate machines, you are required to update the user access list on both machines.



Note

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

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



Note

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

Deleting User Access

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

To delete user access:

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

Step 2 Enter the following command:

```
aclupdate --default
```

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

Viewing User Access

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

To view the User Access list:

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

Step 2 Enter the command:

```
aclupdate --show
```

This displays a list of all users who belong to the user access list.

If access is set to default (all users), the user access list does not appear; the statement `any host` appears instead.

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.
 - 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 machine. 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 *Device Fault Manager User Guide* 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 machine. 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
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
AMAServer	Periodically runs synthetic transactions against CCMs and provides real-time status updates to VHM.	None

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

Name	Description	Dependency
VHMAMAIntegrator	Integrates the VHM server with the AMA server. Receives synthetic transaction messages from AMA server and generates events to the VHM server.	None
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
VHMRMIRegistry	Provides communication services for the VHMInteractor.	None
VHMSkinnyGatewayPoller	Probes Skinny Gateways and voice applications.	VHMServer

To stop a CiscoWorks2000 process:

-
- Step 1** To stop (or start) the VHMFileNotifier, VHMMailNotifier, and VHMTrapNotifier processes, enable or disable them using the GUI. See the [“Using the GUI to Configure Adapters”](#) section on page 5-28 for more information.
- Step 2** To stop (or start) 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.

To restart a CiscoWorks2000 process:

Step 1 Select **Server Configuration > Administration > Process Management > Start Process**. The Start Process window opens.

Step 2 In the Start Process window, locate the process you want to start in the Process drop-down list.

Step 3 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.

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
- VHMAMAIntegrator.log
- VHM SkinnyGatewayPoller.log
- VHMInventoryCollectorSchedule.log
- VHMDiscoveryJobCreate.log
- VHMDiscoveryJobDelete

To set the logging level for VHM processes:

-
- Step 1** Use a text editor such as Notepad to open the `vhmproperty.conf` file in `cscopx\objects\vhm\config` directory.
- Step 2** In the `vhmproperty.conf` file, set `LoggingLevel` (by default, `LoggingLevel=1`) to one of the following values:
- 1—Log errors only
 - 2—Log errors and warnings
 - 3—Log errors, warnings, and trace messages
 - 4—Log errors, warnings, trace, and informational messages
- Step 3** Save the `vhmproperty.conf` file.
-

**Note**

Changes to the `vhmproperty.conf` file affect all VHM log files. After debugging a problem, remember to reset `LoggingLevel` to 1 to avoid accumulating large amounts of data in the log files.
