Avaya MultiVantage™ Fault and Performance Manager

Release 1.3
Installation and Configuration

555-233-138
Issue 4
May 2003

Notice
Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following website:

http://www.avaya.com/support

Preventing Toll Fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or working on your company's behalf). Be aware that there is a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention
If you s*uspect that you are being victimized* by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help
For additional support telephone numbers, go to the Avaya Web site:

http://www.avaya.com/support/

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional Centers of Excellence.

Providing Telecommunications Security
Telecommunications security of voice, data, and/or video communications is the prevention of any type of intrusion to, that is, either unauthorized or malicious access to or use of, your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Whereas, a "malicious party" is Anyone, including someone who may be otherwise authorized, who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company, including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security
The final responsibility for securing both this system and its networked equipment rests with you – an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

- Avaya provided telecommunications systems and their interfaces
- Avaya provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities
Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

To order copies of this and other documents

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
Fax 1.800.457.1764 or 1.207.626.7269

Write: GlobalWare Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

Email: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya Web site:

http:www.avaya.com/support/

Table of Contents

Preface

Purpose

This book explains how to install and set up Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager).

Prerequisites

Installing and configuring Fault and Performance Manager requires familiarity with network administration, knowledge of the Red Hat Linux operating system, and proficiency with Linux administration. This knowledge is not delivered in this book but is essential for a successful installation.

For this reason, we highly recommend that workstation or network administrators take the primary role in installation.

Intended Audience

We wrote this book for workstation or network administrators.

Conventions Used in This Book

In this book, we use the following typographical conventions:

- We use bold type for emphasis and for any information that you should type; for example: **save translation**.
- We use Courier font for any information that the computer screen displays; for example: `login`.
- We use arrows to indicate options that you should select on cascading menus; for example: "Select File>Open" means choose the "Open" option from the "File" menu.

Additional Resources

You may find the following additional resources helpful.

For help using Fault and Performance Manager, see the Fault and Performance Manager online help. It explains how to perform basic administration tasks. To access the online help, start Fault and Performance Manager and choose **Help>Help Topics.**

For help with complex administration tasks, use the *Administrator's Guide for Avaya MultiVantage™ Software*, which explains system features and interactions in detail. You can access this document from the VisAbility home page.

Tell Us What You Think!

Let us know how this book measured up to your expectations. Your opinions are crucial to helping us meet your needs! You can send us your comments by mail, fax, or e-mail, as follows:

Mail: Avaya, Inc.
Fault and Performance Manager Documentation Team
Room 3C-313
307 Middletown Lincroft Rd.
Lincroft, NJ 07738
USA

Fax: Fault and Performance Manager Documentation Team
+ 1 732 852-2469

E-mail: document@avaya.com

How to Get This Book (and Others) on the Web

You can view or download the latest version of this book from the Avaya, Inc. web site. You must have access to the Internet, an Internet browser, and Adobe Acrobat Reader (version 5.0 or later) with Search. Adobe Acrobat Reader is available from *http://www.adobe.com*.

To view or download the latest version of the Avaya VisAbility Management Suite documentation:

1. Access *http://www.avaya.com/support*.
2. Click **Product Documentation**.
3. Click **System and Network Management**.
4. Locate the heading "Avaya VisAbility Management Suite," and click the link corresponding to the software release.
5. Locate the title of the book, and click the link corresponding to the book.

How to Order More Copies of This Book

To order paper copies of this book, call or write us and request the following publication:

Order: Document Number: 555-233-138
Issue: Issue 4
Date: May 2003

Call: Avaya Publications Center
Voice: 1 800 457 1235
Fax: 1 800 457 1764

If you are calling from somewhere that cannot access US 1-800 numbers, then call:
Voice: + 1 207 866 6701
Fax: + 1 207 626 7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835
USA

1 Resources and Notices

Avaya provides a variety of planning, consulting, and technical services. The sections below briefly describe the resources and services that are available.

Client executives are your primary contact to obtain information and explore options to meet your specific business needs.

Avaya Technology and Consulting (ATAC)

ATAC works with client teams to develop detailed solutions for connectivity to MultiVantage™ solutions. The ATAC also designs network configurations to support Fault and Performance Manager, Avaya MultiVantage™ Proxy Agent (Proxy Agent), and Avaya MultiVantage™ Sub-Agent.

Avaya Remote Network Integration Services (RNIS)

For this product, RNIS offers customers the following services:

- Verify platform readiness
- Remotely install Fault and Performance Manager
- Configure the network management server for each voice system to be managed by Fault and Performance Manager
- Verify customer acceptance
- Custom on-site services

Avaya Technical Service Organization (TSO)

The TSO provides support for Fault and Performance Manager, MultiVantage Proxy Agent, and MultiVantage Sub-Agent to client teams, field technicians, and customers. The TSO will bill customers for support on a time and materials basis if the following conditions exist:

- Customers do not have a current maintenance agreement
- Customers do not procure and install the required systems and software as defined in the VisAbility Management Suite Services Support Plan
- Customers request support that is outside the purchase agreement

The TSO does not support hardware or software that customers purchase from third-party vendors.

Avaya Network Management Software Systems Support Group (NMSSS)

The Network Management Software Systems Support (NMSSS) group in Tampa Bay, Florida answers customer calls about applications in the VisAbility Management Suite. NMSSS will either answer your questions directly or connect you with an associate who can answer questions about your application.

Avaya Contact Information

You may find the following contact information helpful at various times during the process of installing and setting up this product This information was accurate at the time this book went to press. We update this information with each new release of Fault and Performance Manager.

Customers can access only the resources in Table 1 (not Table 2). To view Avaya web sites, Avaya recommends that you use Internet Explorer.

Table 1. Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://avaya.com/support/
Network Management Software Systems Support group	1-800-237-0016.
Remote Network Integration Services (RNIS)	http://www1.avaya.com/enterprise/brochures/svc1369.pdf
Toll Fraud Intervention	1-800-643-2353 prompt 1

Table 2. Avaya Internal Resources

Resource	Contact Information
Avaya Enterprise Management Support	http://aem-support.dr.avaya.com/
Avaya Technology and Consulting (ATAC)	Phone: 1-888-297-4700, prompt 2, 6 Main site (requires a password): http://forum.avaya.com
Remote Network Integration Services (RNIS)	http://associate2.avaya.com/sales_market/products/data-implementation-services/
VisAbility Management Services Support Plan	http://associate2.avaya.com/solution/support_plans/#Enterprise
VMS001 Form	http://associate2.avaya.com/sales_market/products/data-implementation-services/ Then click “Avaya VisAbility™ Management Suite Configuration Request Form #1.”

Third-Party Resources

The table below lists contact information for third-party vendors.

Table 3. Vendor web sites

Vendor	Web Sites
Hewlett-Packard	Main site: *http://www.openview.hp.com*
Microsoft	Main site: *http://www.microsoft.com*
Red Hat Linux	Main site: *http://www.redhat.com*
Peregrine	Main site: *http://www.peregrine.com* Scroll down to: action request system
Vytek	Main site: *http://www.vytek.com*
Versant	Main site: *http://www.versant.com*

System Security Notices

Customers are solely responsible for the security of their system, network, and access to hardware and software. The sections below define the precautions that all customers should take to maintain the security of their systems.

Network Security

Fault and Performance Manager uses the standard security features on the Red Hat Linux, Windows 2000, and Windows XP Professional operating systems.

Avaya strongly recommends that customers use passwords to prohibit access to their systems and to routinely change those passwords to maintain security.

SECURITY ALERT:

Customers should always change passwords immediately after external vendors have completed installation, maintenance, troubleshooting, or other tasks on their system.

Toll Fraud Security

Although Fault and Performance Manager is generally not at risk for toll fraud, customers are solely responsible for the security of their entire telecommunications system.

Toll Fraud is the unauthorized use of a company's telecommunications system by unauthorized parties. Unauthorized parties are persons other than the company's employees, agents, subcontractors, or persons working on behalf of the company. Toll fraud can result in substantial additional charges for the company's telecommunications services.

The company's system manager is responsible for the security of the company's system, which includes programming and configuring the equipment to prevent unauthorized use.

Avaya Disclaimer

Avaya does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunications services or facilities accessed through or connected to it. Avaya will not be responsible for any charges that result from such unauthorized use.

Toll Fraud Intervention

If customers suspect that they are a victims of toll fraud and need technical assistance, they should refer to the phone number listed for "Toll Fraud Intervention" on page 13.

2 Overview

Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager) together with Avaya MultiVantage™ Proxy Agent (Proxy Agent) and Avaya MultiVantage™ Sub-Agent provide a complete solution to fault and performance management of Avaya voice elements in the stand-alone mode as well as in an NMS integrated mode.

These products provide a view of the health and performance of your network systems. Fault and Performance Manager, MultiVantage Proxy Agent, and MultiVantage Sub-Agent work together as an integrated application.

Product Description

Fault and Performance Manager

Fault and Performance Manager provides graphical and tabular tools to monitor the status and performance of a network of supported systems and external devices.

Fault and Performance Manager collects configuration, fault, and performance data from MultiVantage Proxy Agent and MultiVantage Sub-Agent using SNMP and then displays the data in text, tables, and graphic formats.

The primary features of Fault and Performance Manager include:

- **Graphical User Interface (GUI)** -- The main window contains a navigation tree that lists all the supported systems and displays a colored alert symbol that indicates highest exception level. You can expand the list to view all of the configuration components and specific alert symbols for each component.
- **Configuration** -- You can view the configuration and administered properties of all supported systems (managed nodes) in both a graphic view and a table view.

- **Administration** -- You define the system-wide parameters for the features below:
  - **Data collection** -- You define the parameters for the data to be collected from each system, including the type of data, the schedule for collecting data, and the length of time to store the data.
  - **Exception logging** -- You define the conditions to log exceptions for performance thresholds, faults, and system errors.
  - **Exception alerting** -- You specify the alert levels for exceptions from each supported system. Alert levels may include exceptions that are critical, major, minor, or warning. The alert level and location of the exception appear in the main window as long as the exception exists.
- **Report Manager** -- You can define the parameters for individual reports for all or selected systems. The report options include:
  - Performance
  - Configuration
  - Exceptions

  You can view the reports on screen in both the table and chart formats or direct the reports to a printer, HTML file, GIF file, or ASCII file.
- **Scheduled Reports** -- You can schedule reports to run on a daily, weekly, or monthly basis, and edit and delete schedules as needed.

Supported Systems

Fault and Performance Manager Release 1.3 supports both SNMP V1 and V2c get and set requests and SNMP V1 alarm traps for the following systems:

- DEFINITY® ECS Releases 9.2 through 10.x
- Avaya MultiVantage™ Software
- Survivable Remote Processors (SRPs)
- Multipoint Conferencing Unit (MCU) Release 6.0 and later

- Avaya™ G600 Media Gateway
- Avaya™ CMC1 Media Gateway

Fault and Performance Manager treats SRPs and MCUs as MultiVantage solutions.

Fault and Performance Manager Release 1.3 supports only alarm traps for the following systems:

- DEFINITY AUDIX® Releases 3.1 through 4.0
- INTUITY AUDIX® Release 4.3 through 5.1 (with or without the remote maintenance board)
- Intuity™ Interchange Release 5.1 through 5.4
- Call Management System (CMS) R3V6 through R3V11
- CONVERSANT Release 9.0
- C-Hawk INTUITY AUDIX Release 1.0
- S8100 Media Server INTUITY AUDIX
- INTUITY AUDIX LX Release 1.0

System Requirements

Hardware

You should work with your Avaya client team to determine the hardware requirements that meet your business and performance specifications. Your client team has access to the VisAbility Management Suite Services Support Plan, which contains the information they need to help you determine hardware requirements in your situation. Your client team can download the package from the URL listed in Table 2 on page 13.

Hardware Certification

Avaya requires that Fault and Performance Manager hardware must be Red Hat Linux 7.3 and 8.0 certified. For the Red Hat URL, see "Third-Party Resources" on page 14.

⚠ CAUTION:

Customers are solely responsible for upgrading their network platforms to meet the NMS platform requirements for Fault and Performance Manager Release 1.3.

Software

Fault and Performance Manager Release 1.3 operates on Red Hat Linux 7.3. The optional NMSI component runs on Windows 2000 running HP OpenView 6.2 and Solaris 8.0.

Installation and Configuration Overview

The installation and configuration process will follow the basic steps listed below:

1. Customers complete the "Customer Pre-Installation Tasks" on page 21.
2. Customers communicate with RNIS to verify server readiness, finalize technical details, and confirm implementation schedule.
3. (For upgrades only:) Complete the procedure, "Backing up the Database" on page 39.
4. Installers complete "Installing on Linux" on page 22.
5. If you will be running Fault and Performance Manager with a Network Management System (NMS), then installers should:
   a. Complete the procedure, "Configuring Fault and Performance Manager to Integrate with HP OpenView" on page 23.
   b. Complete the procedure, "Installing Avaya NMSI Components on Windows" on page 26.
6. If you will be running Fault and Performance Manager “standalone,” the installers should complete the procedure, "Configuring Fault and Performance Manager for Stand-Alone Operation" on page 29.
7. Installers complete "Installing the Fault and Performance Manager Client on Windows" on page 30.
8. Installers complete "Administering Alarm Notification Services" on page 41.
9. If you will be running MultiVantage Sub-Agent, complete the procedures in "Configuring MultiVantage Sub-Agent" on page 49.
10. If you will be running Fault and Performance Manager with an NMS, then installers should complete"Executing Auto-Discovery" on page 70.
11. If you want to use Fault and Performance Manager to collect data, create and save report definitions, and schedule reports, then installers should complete "Starting the Administrative GUI" on page 63.

3 Installing and Upgrading Fault and Performance Manager

This chapter explains how to install Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager) Release 1.3 as a new or upgrade installation.

In this document, Proxy Agent refers to either DEFINITY Proxy Agent (DPA) or Avaya MultiVantage™ Proxy Agent (Proxy Agent).

Customer Pre-Installation Tasks

Before Fault and Performance Manager can be installed, customers must complete the several tasks that are defined in the VisAbility Management Suite Services Support Plan. Your client team can download the plan from the URL specified in Table 2 on page 13.

One of those tasks is to set up your Linux server. Instructions for doing so are in the Avaya VisAbility Management Suite Implementation Guidelines, which is available from your client executive. The instructions are also available in the Configuring Red Hat Linux document, which is available under the “VisAbility” heading of the System and Network Management area of the Support Centre web site. (see "How to Get This Book (and Others) on the Web" on page 9).

Completing the VMS001 Form

The VMS001 form stores information that an installer needs when installing and configuring Fault and Performance Manager. The form also stores information that Avaya would need when troubleshooting and or maintaining Fault and Performance Manager. Your client team has access to the form and may ask for your input in completing the form. The VMS001 form must be completed for new installations and for any upgrades or changes.

Installing on Linux

This section explains how to install Fault and Performance Manager. The installation script has been updated to simplify the process.

Required Materials

Assemble the following materials and information:

- This book
- "Avaya VisAbility Management Suite: Linux Server Installation" CD-ROM
- Completed VMS001 form
- Root name and password

*** Note:** You must reboot your system after installing Fault and Performance Manager.

Default options

The sections below describe the prompts in the order that they presented in the installation script. The default options help you to maintain consistency when upgrading to new releases. The installation script overwrites previous settings during the installation process.

Procedure

Complete the procedure below to install Fault and Performance Manager.

1. Ask all users to log off the system.
2. Close all open windows and applications.
3. At the login prompt, type **root** and press **ENTER.**
4. At the password prompt, type the root password and press **ENTER**.
5. Insert the "Avaya VisAbility Management Suite: Linux Server Installation" CD-ROM into the CD-ROM drive.
6. Open a terminal window.
7. Type **mount /dev/cdrom**.
8. Type **cd /mnt/cdrom**.

9. Type **vms_setup.bin** and press **ENTER**.

   The message “Initializing wizard.” appears followed by the Welcome screen.

10. Click **NEXT** and follow the prompts to complete the installation.

11. Do one of the following:

    — If you are installing a stand-alone system, go to "Configuring Fault and Performance Manager for Stand-Alone Operation" on page 29. or

    — If you are installing the HP OpenView integrated version, complete the next section.

Configuring Fault and Performance Manager to Integrate with HP OpenView

CAUTION:

To use the NMSI portion of the offer, before beginning the following configuration process, you must have HP OpenView for Windows NT/2000 Version 6.2 installed and running.

Complete the procedures below to configure Fault and Performance Manager to Integrate with HP OpenView.

1. At the login prompt, type **root** and press **ENTER**.

2. At the password prompt, type the root password and press **ENTER**.

3. Open a terminal window.

4. At the Linux prompt, type **/usr/sbin/mfpmconfig** and press **ENTER**.

   The system displays the prompt:

   ```
   Do you want to reconfigure the MultiVantage Fault and
   Performance Management software [yes]
   ```

5. Type **yes** and press **ENTER.**

   The system displays the prompt:

   ```
   Shutting down MFPM Server services:

   Configuring environment:

   MultiVantage Fault and Performance Management
   require a print command to be specified. This
   command will be used by the application when
   attempting to print reports to a printer. The
   keyword “%file” can be used in the print not
   appear here, the filename will be appended to the
   print command. Please enter a default print
   command to be used by the MFPM applications

   Enter printer command [ ]
   ```

6. Type the print command and press **ENTER.**

   The print command is on the VMS001 form.

   The system displays the message:

   ```
   MultiVantage Fault and Performance Management can
   integrate with an HP OpenView Network Node
   Manager system. It provides for MultiVantage
   System View which shows logical connectivity
   amongst MultiVantage IP telephony endpoints.
   Refer to the MultiVantage Fault and Performance
   Management documentation for more information
   about the HP OpenView NMS Integration.

   Do you want to integrate MFPM with an HP OpenView
   System[ ]?
   ```

7. Type **yes** and press **ENTER.**

   The system displays the message:

   ```
   In order for this capability to work, information
   regarding the IP connectivity with the HP
   OpenView server must be established.

   Enter the HP OpenView Server IP Address [  ]
   ```

8. Type the HP OpenView server IP address and press **ENTER.**

The system displays the message:

```
When the MultiVantage Fault and Performance Management
HP OpenView NMSI is installed, a service for the NMSI
SNMP Configuration service will be set up. The TCP
port number that this service is using on the HP
OpenView NMSI server must be entered at this time. If
you do not know the TCP port number yet, just select
the default and run mfpmconfig at a later time after
the NMSI HP OpenView Component has been installed on
the HP OpenView server.

Enter the HP OpenView Server Config Service TCP Port
Number you want to integrate MFPM with an HP OpenView
System [ ]?
```

9. Type the HP OpenView server config service TCP port number and press **ENTER**.

(This number is on the VMS001 form)

Avaya voice related objects will be placed on the HP OpenView maps. A specific map can be identified as the repository for where the Avaya objects will be placed. By default, HP OpenView's default map name is "default". If you use a different HP OpenView map, that map name needs to entered here. If you are not sure just accept the default setting.

```
Enter the HP OpenView Server Map Name [default]
```

10. Press **ENTER.**

The system displays the following messages:

```
Configuring MFPM Java Environment...

Configuring MFPM NMSI Environment...

Modifying MFPM Properties in Web Client JAR file...

Building environment file...

Platform configuration complete.

Starting MFPM Server services:

MultiVantage Fault and Performance Management
software configuration was successful.
```

11. At the Linux prompt, reboot the system by typing the shutdown command type **reboot** and press **ENTER.**

The system reboots. This takes several minutes.

Installing Avaya NMSI Components on Windows

Complete the procedure below if you plan to run Fault and Performance Manager integrated with an NMS.

1. Shut down all applications.
2. Insert the "Avaya VisAbility Management Suite: Windows Server Installation" CD into the CD-ROM drive.

   Wait a moment for the autorun application to appear automatically
3. Click **Install Network Management Products.**

   The installation program will display a welcome page.
4. At the Welcome page, click **Next.**

   The installation program displays a list of the applications that you can install. If HP OpenView is detected on the machine, the NMSI Components for HP OpenView check box will be enabled. Otherwise, it will be disabled.
5. Select **NMSI Components for HP OpenView,** along with any other programs you want to install.
6. Verify that you have enough available hard disk space on your PC to install the application.
7. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Finish.**

   A note advises you that if an installation wizard asks you if you want to reboot, you should NOT reboot until the final installation wizard has run. Click **OK.**

   Depending on which options you selected in Step 5, the master installation wizard launches one or more of the following installation wizards, in the following order:

   — Netscape installation wizard

   — Java Development Kit installation wizard

   — Apache Web Server installation wizard

   — Apache Tomcat installation wizard

— Avaya ATM WAN Survivable Processor Manager installation wizard

— VisAbility Management Home Page installation wizard

— Avaya VoIP Monitoring Manager installation wizard

— Avaya Directory Enabled Management installation wizard

— Adobe Acrobat Reader installation wizard

— Avaya MultiService Network Manager installation wizard (this will prompt for the MultiService Network Manager CD)

Installing the Java Development Kit

1. Read the terms and conditions of the Sun license agreement, and do one of the following:

   a. If you agree to the terms and conditions, click **Yes.**

   b. If you do not agree to the terms and conditions, click **Cancel.**

   Doing so will terminate the installation wizard for this application. The installation program will display the wizard for the next application that you selected (if any) in **Step 5** on page 26. In that event, refer to the installation document for that application and skip the rest of this procedure.

2. Specify the location where you want to install the JDK and click **Next.**

   To change the location, click **Browse** and navigate to where you want to install the JDK.

3. Specify the browser(s) that you want the JRE plug-in to work with and click **Next.**

   A list of options appears.

4. Leave everything selected (default) and click **Next.**

   The wizard installs the Java Runtime Environment.

5. Select **No, I will restart my computer later** and click **Finish.**

Installing Avaya NMSI Components

1. At the Welcome screen, click **Next.**
2. Specify the location where you want the files to be installed.

   Note: This is not the final location of the files. Files will be moved from the installation location into various areas of the HP OpenView product.
3. Enter the computer name or fully-qualified domain name (FQDN) of the Fault and Performance Manager server computer and click **Next.**

   The FQDN is the host name followed by the IP domain name. For example: `dnapc1.department.company.com`.
4. Enter the port number that the Fault and Performance Manager server expects to communicate to the NMSI components with and click **Next.**
5. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Finish.**

      A note advises you that if an installation wizard asks you if you want to reboot, you should NOT reboot until the final installation wizard has run. Click **OK.**

Finishing the Installation

After the final wizard runs, a message appears indicating that the installation is complete and that you can now reboot your computer (if any of the installation wizards indicated that this was necessary). To finish the installation, complete the following steps:

1. On the CD Browser screen, click **Exit.**
2. Remove the CD from the CD-ROM drive.
3. Reboot (if appropriate).

Configuring Fault and Performance Manager for Stand-Alone Operation

Complete the procedure below to configure Fault and Performance Manager for stand-alone operation. Skip this section if you do not plan to run Fault and Performance Manager standalone.

1. At the login prompt type **root** and press **ENTER.**
2. At the password prompt, type the root password and press **ENTER.**
3. Open a terminal window.
4. At the Linux prompt, type /**usr/sbin/mfpmconfig** and press **ENTER.**

   The system displays the prompt: `Do you want to reconfigure the MultiVantage Fault and Performance Management 1.3 software [yes]`
5. Type **yes** and press **ENTER.**

   The system displays the message:

   ```
   Shutting down MFPM Server services:

   Configuring environment:

   MultiVantage Fault and Performance Management require
   a print command to be specified. This command will be
   used by the application when attempting to print
   reports to a printer. The keyword “%file” can be used
   in the print not appear here, the filename will be
   appended to the print command. Please enter a default
   print command to be used by the MFPM applications

   Enter printer command [ ]
   ```
6. Type the print command and press **ENTER.**

   The system displays the message:

   ```
   MultiVantage Fault and Performance Management can
   integrate with an HP OpenView Network Node Manager
   system. It provides for MultiVantage System View which
   shows logical connectivity amongst MultiVantage IP
   telephony endpoints. Refer to the MultiVantage Fault
   and Performance Management documentation for more
   information about the HP OpenView NMS Integration.

   Do you want to integrate MFPM with an HP OpenView
   System[ ]?
   ```

7. Type **no** and press **Enter.**

   The system displays the messages:

   ```
   Configuring MFPM Java Environment...

   Configuring MFPM NMSI Environment...

   Modifying MFPM Properties in Web Client JAR
   file...

   Building environment file...

   Platform configuration complete.

   Starting MFPM Server services:

   MultiVantage Fault and Performance Management
   software configuration was successful.
   ```

8. At the Linux prompt, reboot the system by typing **cd/; /sbin/shutdown -r** and pressing **ENTER.**

   The system reboots. This takes several minutes.

Installing the Fault and Performance Manager Client on Windows

To install Fault and Performance Manager clients, you must use a Windows login that has Administrator privileges. Then, complete the following sections.

Starting the Installation

1. Shut down all applications running on the PC.
2. Insert the "Avaya VisAbility Management Suite: Windows Client Installation" CD into the CD-ROM drive.

   Wait a moment for the CD browser window to appear automatically.

3. Click **Install Network Management Client Products.**

   The installation program prepares the installation wizard and displays the Welcome page.

4. At the Welcome page, click **Next.**

   The installation program displays a list of the applications and shortcuts that you can install. By default, the option for Required Components is checked.

5. Select Shortcut for MultiVantage Fault and Performance Manager, along with any other programs or shortcuts you want to install.

6. Verify that you have enough available hard disk space on your PC to install the shortcut(s).

   a. If you don't, click **Cancel** to exit the installation program.

      Restart the installation at **Step 1** when you have made adequate hard disk space available.

   b. If you do, click **Next.**

      The installation program displays the summary page.

7. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Finish.**

      A note advises you that if an installation wizard asks you if you want to reboot, you should NOT reboot until the final installation wizard (in your situation) has run. Click **OK.**

*** Note:** If at any time during the installation you see a wizard that asks you if you want to reboot, **DO NOT SAY YES** until you are certain that the final installation wizard has run.

Depending on which options you selected in **Step 5**, the "master installer" program launches one or more of the following installation wizards, in the following order:

—Netscape installation wizard

—Java Runtime Environment (only if you select a shortcut, Directory Enabled Management, or VAL Manager)

—Required components installation wizard

—Avaya Site Administration installation wizard

—Avaya Terminal Emulation installation wizard

—VAL Manager installation wizard

—VoIP Monitor installation wizard

—System Management Client Shortcuts installation wizard.

—Adobe installation wizard

This book explains only the screens that appear if you select the Fault and Performance Manager shortcut option. If you select additional options, you may see other screens in between the ones described below.

Installing the Java Runtime Environment

First, The Java Runtime Environment installation wizard runs.

1. Read the terms and conditions of the Sun license agreement, and do one of the following:

   a. If you agree to the terms and conditions, click **Yes.**

      The installation wizard displays any Release Notes.

   b. If you do not agree to the terms and conditions, click **Cancel.**

      This will terminate the installation wizard for this application. The installation program will display the wizard for the next application that you selected (if any) in **Step 5**. In that event, **refer to the installation documentation for that application and skip the rest of this procedure.**

2. Specify the location where you want to install the JRE and click **Next.**

   To change the location, click **Browse** and navigate to where you want to install the JRE.

3. Specify the browser(s) that you want this JRE plug-in to work with and click **Next.**

   The installation wizard copies the necessary files to your computer, then displays a message and exits when the installation is complete.

   Then, the Required Components installation wizard runs.

Installing the Required Components

When you install the Required Components, the installation program sets up files so that you can launch applications from the VisAbility home page.

1. At the Welcome screen, click **Next.**
2. Specify the location where you want to install the Required Components and click **Next.**

   To change the location, click **Browse** and navigate to where you want to install the Required Components.
3. Enter the computer name or FQDN of the VisAbility Network Management Server.

   The VisAbility Network Management Server is either a Windows server or a Linux server. It is the location where this client PC will look for the VisAbility Management web page. If you have installed (or plan to install) both the Windows server and the Linux server, enter the Windows server information here. If you have installed (or plan to install) only the Linux server, then enter the Linux server information here.

   You can type the computer name or the FQDN. The FQDN is the host name followed by the IP domain name. For example: `dnapc1.department.company.com`.
4. Check the summary page and do one of the following:

   a. If it contains errors, click **Back** to correct the errors.

   b. If it is accurate, click **Next.**

      The installation wizard displays a message that the installation of Required Components is complete.
5. Click **Finish.**

Finishing the Installation

After the final wizard runs, a message appears indicating that the installation is complete and that you can now reboot your computer if any of the installation wizards indicated that this was necessary. To finish the installation, complete the following steps:

1. On the CD Browser screen, click **Exit.**
2. Remove the CD from the CD-ROM drive.
3. Reboot (if appropriate).

Repeat this process, starting at "Starting the Installation" on page 30, on all other Windows computers that you want to serve as Fault and Performance Manager clients.

Uninstalling Fault and Performance Manager

This section explains how to remove Fault and Performance Manager. This procedure contains only the basic steps. For more information on the Linux package uninstall, refer to the Linux system documentation.

CAUTION: **To preserve current data, back up data to a file or archive device.**

Procedure

Only root users should remove Fault and Performance Manager. The remove script prompts you to back up the database to a file or an archive device.

1. Close all windows and applications.
2. Log off the network server.
3. **Optional**. If you are backing up the database before you remove Fault and Performance Manager, connect the archive device.
4. At the login prompt, type **root** and press **ENTER.**
5. At the password prompt, type the root password and press **ENTER**
6. Open a terminal window

7. Type **cd/ usr/local/avaya/uninstall** and press **ENTER.**

   Doing so sets up the Fault and Performance Manager environment.

8. Type **. /uninstaller.bin** and press **ENTER.**

   The installation wizard appears followed by the Welcome screen.

9. Select the application to be removed

10. Click **NEXT** and follow the wizard prompts.

4 Customizing Fault and Performance Manager

Introduction

Only the system administrator or root user should edit the files that allow you to customize Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager).

The information in this chapter allows system administrators to manage the options below:

- Set up the MultiVantage Sub Agent on your MultiVantage software
- Control the NMSI polling of Proxy Agents
- Override the default location submaps that are administered on Proxy Agents
- Execute system commands to start and stop Fault and Performance Manager and to view the system health status
- Execute database commands
- Edit system configuration files to customize Fault and Performance Manager
- Integrate third-party products for alarm notification

Setting up Native Agent

For instructions on setting up the MultiVantage Sub Agent on your MultiVantage software, see the Administrator's Guide for Avaya MultiVantage Software, 555-233-506 Issue 6. The section is titled, "SNMP Agents" in Chapter 17, "Administering Media Servers."

System Commands

Start and Stop Commands

Fault and Performance Manager processes normally start from Linux inittab. The commands in the table below give the system administrator additional control of the Fault and Performance Manager processes.

Table 4. Start and Stop commands

Command	Description
service mfpm-server stop	Stops the Fault and Performance Manager system and prevents it from starting at system boot.
service mfpm-server start	Starts a stopped Fault and Performance Manager system and enables it to start at system boot.
service mfpm-server restart	Stops and immediately restarts the Fault and Performance Manager system.

System administrators can view a log of system startups and shutdowns from /var/avaya/mfpm/logs/MsgLog_[0-6]. The default number of MsgLog files is 6. You can change this value.

System Health Commands

The table below contains the system health commands.

Table 5. System Health commands

Command	Description
service mfpm-server status	Displays Fault and Performance Manager system process status
/usr/local/avaya/mfpm/bin/mfpm gui	Opens a graphical monitor of process status

Backing up the Database

Only the root user can execute the procedure to back up the database.

You can execute the BackupMFPM utility to back up the database during installation or at any time after the product is installed.

Required materials

You will need the following materials and information:

- Root login and password
- File name or device name to back up the database

Procedure

Complete the procedure below to back up the database.

1. Close all windows and applications.
2. **Optional**. Connect the archive device.
3. At the login prompt type root and press **ENTER**.
4. At the password prompt, type the root password and press **ENTER.**
5. Type **service mfpm-server stop** and press **ENTER.**

   This shuts down Fault and Performance Manager services.
6. Create a directory to store the backup and give it the correct permissions.

   For example, type **mkdir /var/backup** and press **ENTER**. Then type **chmod 777 /var/backup** and press **ENTER**.
7. Type **BackupMFPM output_file_path** or **output_device_path** and press **ENTER.**

   The system backs up the database and displays the message:

   ```
   Backup was completed successfully.

   Would you like to do another level of backup on
   database 'MFPM'? [default = no]
   ```
8. Press **ENTER**.

   Doing so selects "no."
9. Type **service mfpm-server start** and press **ENTER.**

   This restarts Fault and Performance Manager services.

Restoring the Database

Only the root user can execute the procedure to restore the database.

You can execute the RestoreMFPM utility to restore the database from the backup file or the archive device.

Required materials

You will need the following materials and information:

- Root login and password
- File name or device name to back up the database

Procedure

Complete the procedure below to restore the database.

1. Close all windows and applications.
2. **Optional**. Connect the archive device.
3. At the login prompt, type **root** and press **ENTER.**
4. At the password prompt, type the root password and press **ENTER.**
5. Type **service mfpm-server stop** and press **ENTER.**

   This shuts down Fault and Performance Manager services.
6. Type **RestoreMFPM input_file_path** or **input_device_path** and press **ENTER.**

   The system displays a series of messages, which takes several minutes. Then the system displays the prompt:

   ```
   During the roll forward, would you like to
   apply records from the database's current log
   file in addition to any archived records?
   [default = yes]
   ```
7. Type **N** (no) and press **ENTER.**

   The system restores the database and displays the message:

   ```
   Restore was completely successful.

   Would you like to do another level of restore on
   database 'MFPM'? [default = no]
   ```

8. Press **ENTER**.

   Doing so selects "no."

9. Type **service mfpm-server start** and press **ENTER.**

   This restarts Fault and Performance Manager services.

Administering Alarm Notification Services

Fault and Performance Manager offers a notification feature that, when used with third-party applications can (for example) page you when Fault and Performance Manager receives an alarm. Only a system administrator or a root user who knows Linux shell programming should perform this task.

Script directories

The /usr/local/avaya/mfpm/bin directory contains the sample scripts listed below:

- DEFINITY_ARS
- AUDIX_ARS
- CMS_ARS
- CONVERSANT_ARS

Alarm notification options

System administrators can choose to use the pager or email features in Fault and Performance Manager or edit the scripts to enable third-party products such as:

- Vytek, ***TeleAlert***
- Peregrine, ***Alarm Response Service (ARS)***

CAUTION: **Customers are solely responsible for the purchase, installation, and maintenance of third-party software products.**

Description of Alarm Notification Options

The tables below outline the alarm notification options that are available in Fault and Performance Manager or from third-party vendors.

Fault and Performance Manager options

The table below contains the description of product options within Fault and Performance Manager.

Table 6. Fault and Performance Manager notification options

Option	Description
CU Pager	Pages the system administrator and sends a code that identifies the type of alarm, alert, or error received from the managed system.
Email	Sends an email message to the system administrator that contains detailed information for the alarm, alert, or error received from the managed system.

TeleAlert options

The table below contains the descriptions of the notification options in Vytek's TeleAlert.

Table 7. Vytek notification options

Option	Description
Alpha Page	Pages the system administrator and sends a code that identifies the type alarm, alert, or error received from the managed system. The alpha page also confirms that the system administrator received the page. The page repeats until the system administrator responds to the page.
Voice Page	Sends a voice page to the system administrator and sends a code that identifies the type of alarm, alert, or error received from the managed system.
AUDIX	Calls the system administrator's AUDIX number and leaves a voice message that contains the detailed information for the alarm, alert, or error received from the managed system.

Peregrine option

The table below describes the notification options in Peregrine's ARS product. The sample script only supports ticketing. The Peregrine product supports voice page and email notification.

Table 8. Peregrine notification option

Option	Description
Ticket	Creates a trouble ticket that contains the historical information for the alarm, alert, or error received from the managed system.

DEFINITY_ARS Script

The MFPM looks for the DEFINITY_ARS script when one of the following events occur:

- MFPM receives an alarm trap from the managed nodes listed below:
  - MultiVantage solutions
  - MCU
- MFPM receives an exception event from Fault and Performance Manager for these managed nodes

Then the MFPM calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the MFPM assigns the alarm the string "NULL_FIELD."

Alarm notification values:

1. System name
2. Error description
3. New status severity
4. Old status severity
5. Product ID
6. Alarm sequence number
7. Alarming Port
8. Maintenance object name
9. On board fault

10. Type of alarm
11. Alternate name for the device
12. Describes the external device
13. Product Identifier of external device
14. Building location of external device
15. Address of external device
16. Restart date time
17. Restart level
18. Restart carrier
19. Restart craft demand
20. Restart escalated
21. Restart interchange
22. Restart unavailable
23. Restart cause
24. Restart speA release
25. Restart speB release
26. Restart speA update
27. Restart speB update

AUDIX_ARS Script

The MFPM looks for the AUDIX_ARS script when one of the following events occur:

- MFPM receives an alarm trap from the managed nodes listed below:
  - DEFINITY AUDIX
  - Intuity AUDIX
  - Intuity Interchange
- MFPM receives an exception event from Fault and Performance Manager for these managed nodes

Then the MFPM calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the MFPM assigns the alarm the string "NULL_FIELD."

Alarm notification values:

1. System name
2. Product ID
3. Alarm sequence number
4. Source of the alarm:
   - DEFINITY (for DEFINITY AUDIX)
   - Intuity Interchange
5. Error description
6. New status severity
7. Old status severity
8. Alarm location
9. Alarm date
10. Alarm time
11. Resource
12. Fault code
13. Module ID
14. Event number
15. Count number

CMS_ARS Script

The MFPM looks for the CMS_ARS script when one of the following events occur:

- MFPM receives an alarm trap from the Call Management System (CMS)
- MFPM receives an exception event from Fault and Performance Manager for the CMS

Then the MFPM calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the MFPM assigns the alarm the string "NULL_FIELD."

Alarm notification values:

1. System name
2. Product ID
3. Alarm sequence
4. Error description
5. New status severity
6. Old status severity
7. Product type
8. Version
9. ID value
10. Number
11. Name

CONVERSANT_ARS Script

The MFPM looks for the CONVERSANT_ARS script when one of the following events occur:

- MFPM receives an alarm trap from the CONVERSANT system
- MFPM receives an exception event from Fault and Performance Manager for the CONVERSANT system

Then the MFPM calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the MFPM assigns the alarm the string "NULL_FIELD."

Alarm notification values:

1. System name
2. Product ID
3. alarm number
4. Error description
5. New status severity
6. Old status severity
7. Location
8. Date
9. Time
10. Resource
11. Fault code
12. Module ID
13. Event number
14. Count number

5 Configuring MultiVantage Sub-Agent

MultiVantage Sub-Agent is a native Simple Network Management Protocol (SNMP) agent. This chapter describes how to configure MultiVantage Sub-Agent to work with Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager).

Recommended Software Requirements

We recommend the following software requirements for complete support and functionality:

- Avaya VisAbility Management Suite Release 1.3
- Avaya MultiVantage Release 1.3

Configuration Procedures

To configure MultiVantage Sub-Agent, you must perform the following procedures:

1. Verify the voice system login ("Procedure 1: Verify the Voice System Login" on page 50).
2. Launch the Maintenance web interface ("Procedure 2: Launch the Maintenance Web Interface" on page 52).
3. Turn on access for the SNMP ports ("Procedure 3: Turn on access for the SNMP Ports" on page 53). Perform this procedure only if you have an S8700 system.
4. Configure trap destinations ("Procedure 4: Configure Trap Destinations" on page 56).
5. Stop/start Master Agent ("Procedure 5: Stop/Start Master Agent" on page 58).
6. Administer SNMP agents ("Procedure 6: Administer SNMP Agents" on page 59).
7. Add the MultiVantage Sub-Agent ("Procedure 7: Add the MultiVantage Sub-Agent" on page 61).

Procedure 1: Verify the Voice System Login

The voice system login created automatically within the MultiVantage software for MultiVantage Sub-Agent is **acpsnmp**.

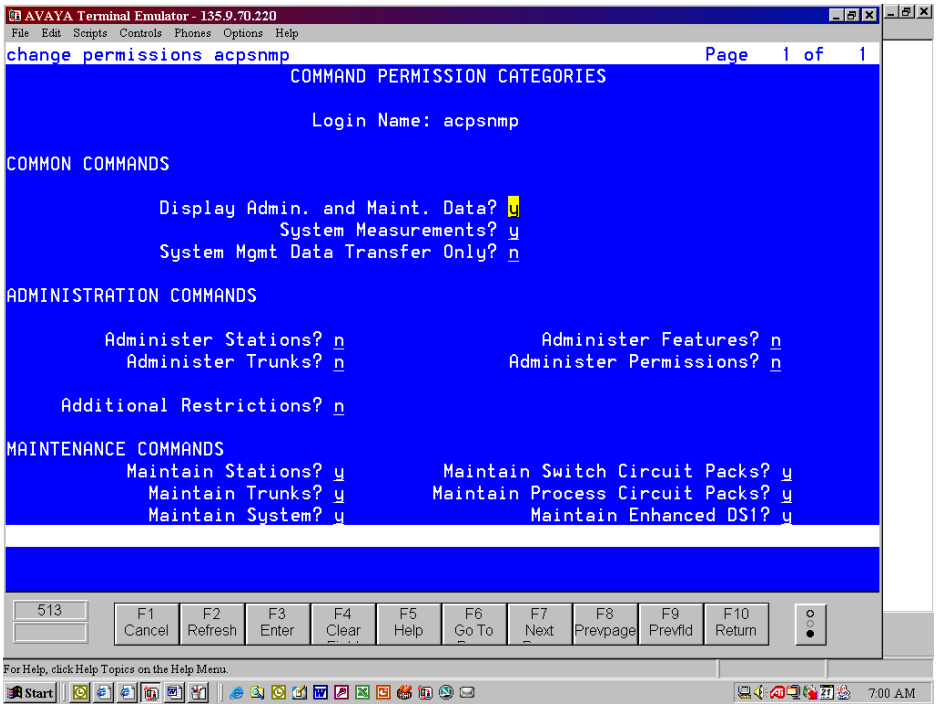
To verify the voice system login:

1. Verify the voice system login created for MultiVantage Sub-Agent to assure it has the correct permissions. The permissions for this login are the same as the permissions for the login used for the MultiVantage Proxy Agent. The **acpsnmp** login defaults with all permissions turned off. You must be able to perform maintenance commands.

   Use a tool such as Avaya Terminal Emulator or Avaya Site Administration to access the MultiVantage change permissions screen.

2. On the MultiVantage change permissions screen, set **Display Admin. and Maint. Data** to **y.**
   Set **System Measurements** to **y**. See the following screen.

*** Note:** If the customer is planning to use the BusyOut/Release feature, set the fields under MAINTENANCE COMMANDS to y. If the maintenance fields cannot be set to y, contact the TSO to activate the appropriate fields.

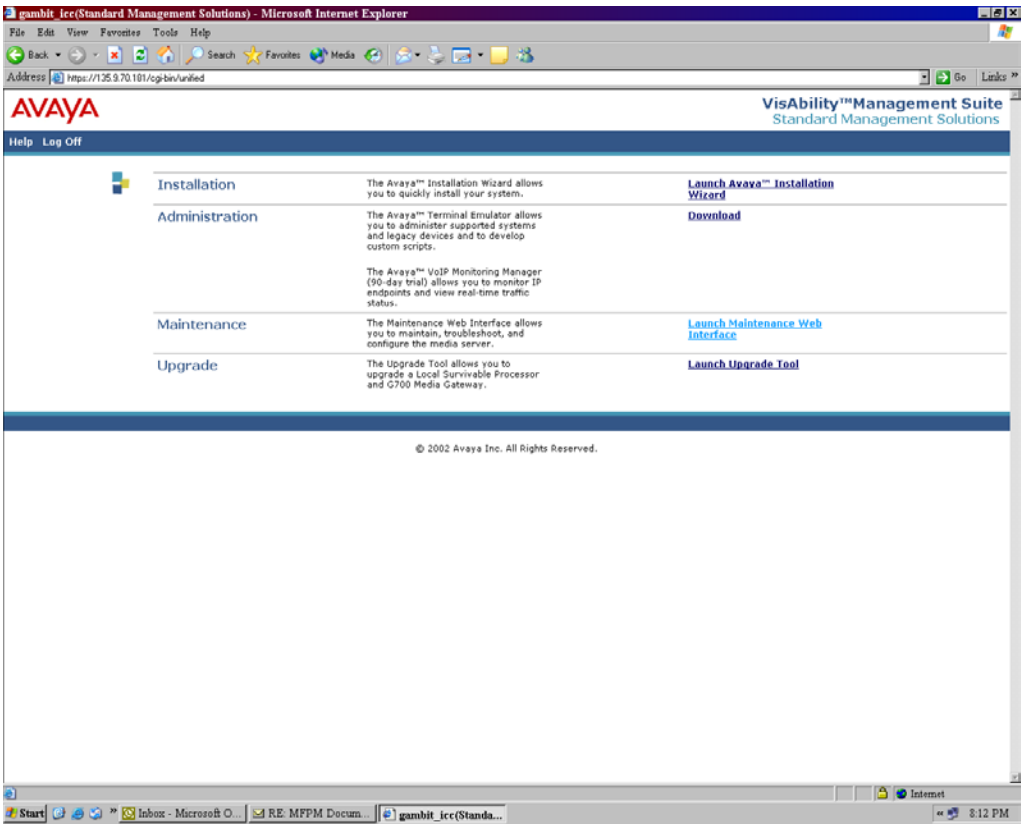


Go to "Procedure 2: Launch the Maintenance Web Interface" on page 52.

Procedure 2: Launch the Maintenance Web Interface

To launch the Maintenance web interface:

1. From the VisAbility™ Management Suite Standard Management Solutions page, **click Launch Maintenance Web Interface**.



2. Perform one of the following steps:

   — If you have an S8700 system, go to "Procedure 3: Turn on access for the SNMP Ports" on page 53.

   — If you do not have an S8700 system, go to "Procedure 4: Configure Trap Destinations" on page 56.

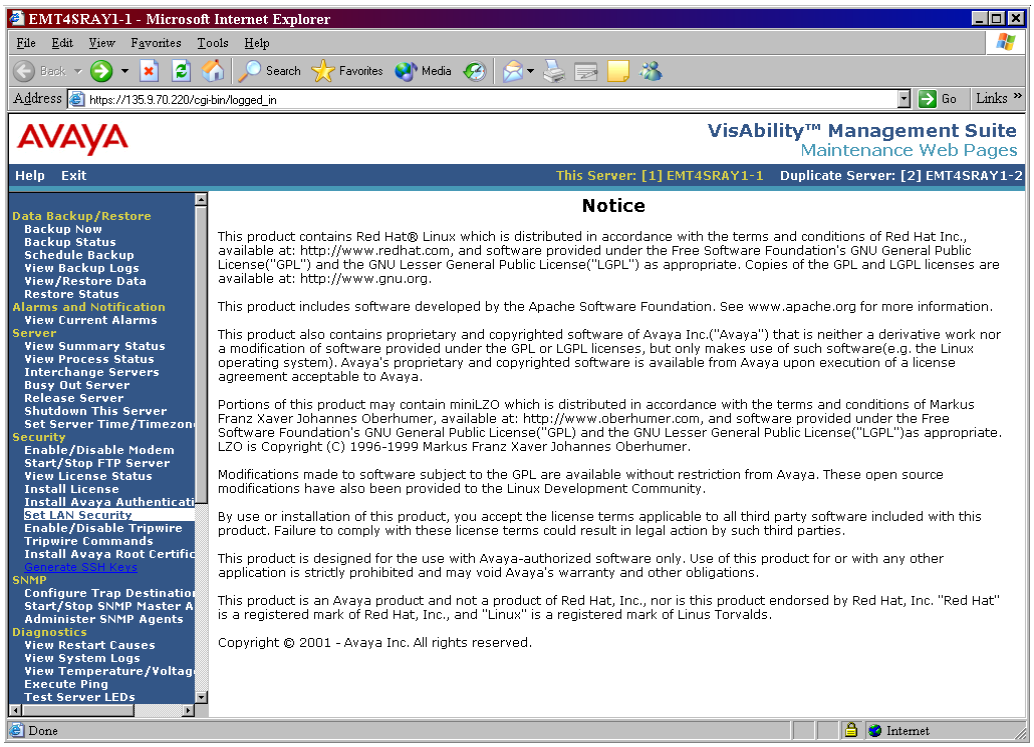
Procedure 3: Turn on access for the SNMP Ports

If you are using an S8700 system, you must complete the following steps before administering the agent on MultiVantage. This will allow the agent to properly pull performance or configuration data.

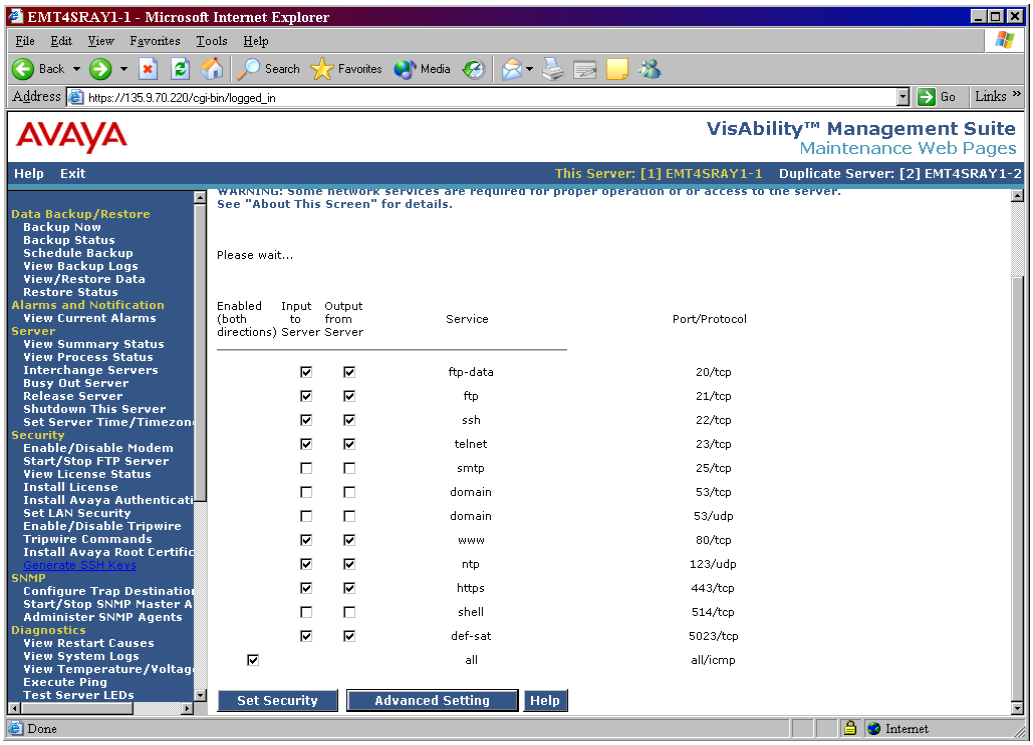
*** Note:** This procedure only applies to S8700 systems.

To turn on access for the SNMP ports:

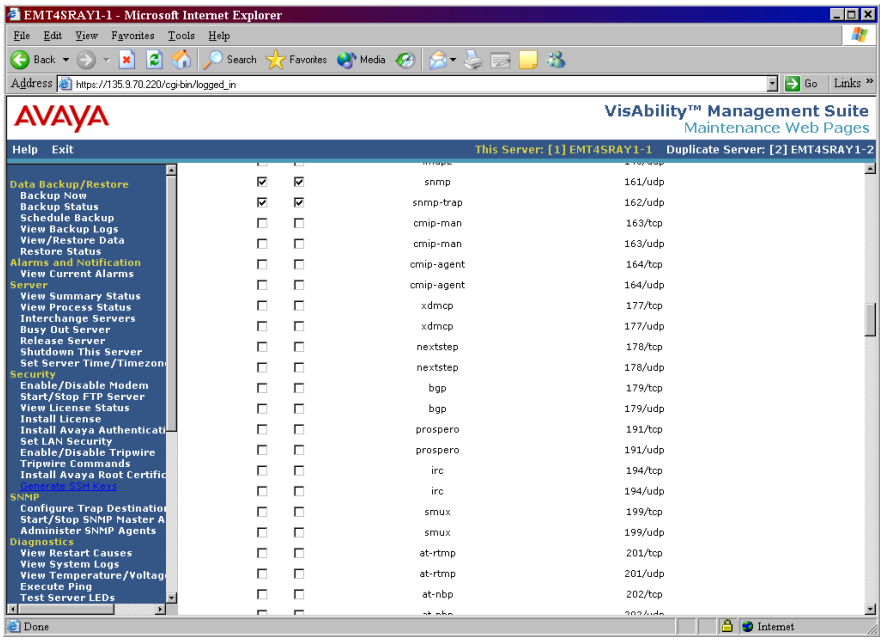
1. From the **Security** heading located on the navigation frame on the left side of this page, click **Set LAN Security**.



2. From the Set LAN Security page, click the **Advanced Setting** button.



3. Scroll down to the fields for SNMP (port 161) and snap-trap (port 162) and ensure that both the input and output boxes are checked as shown in the following screen. These ports are required and cannot be changed. (The ports are Industry Standard.)



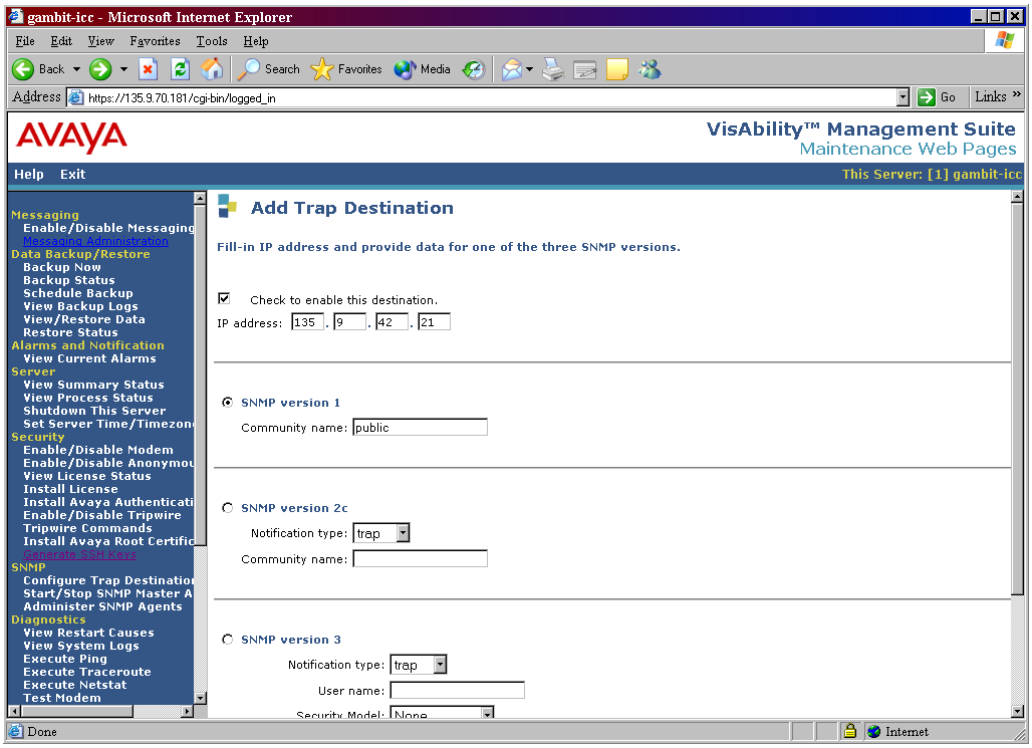
Go to “Procedure 4: Configure Trap Destinations” on page 56.

Procedure 4: Configure Trap Destinations

To configure trap destinations:

1. From the **SNMP** heading located on the navigation frame, click **Configure Trap Destinations**.

2. Click the **Add** button. The Add Trap Destination screen is displayed.

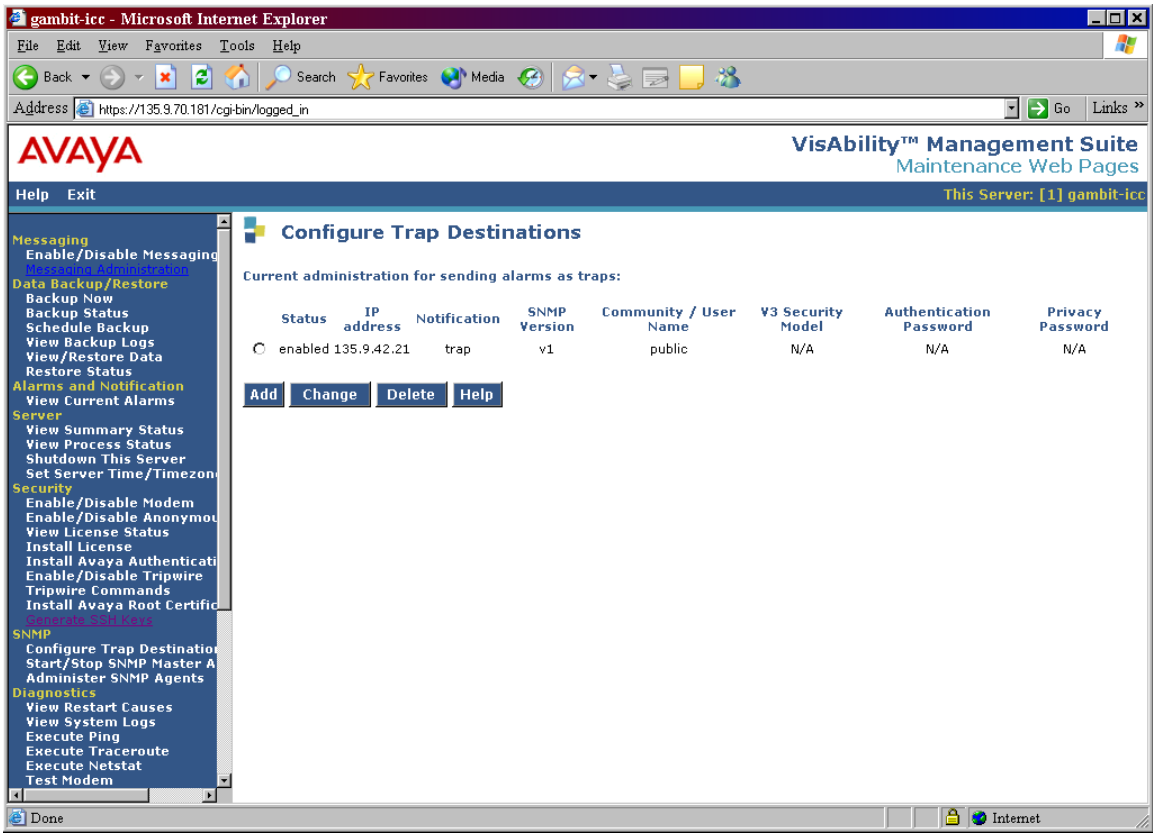


3. Check the box labeled **Check to enable this destination** and add the IP address of the MultiVantage Fault and Performance Manager. (If you are using MultiVantage Fault and Performance Manager, you must add the using MultiVantage Fault and Performance Manager IP address here.) This is where you setup the agent to distribute the SNMP traps to the proper destination.

4. Click the option button for **SNMP version 1** and enter the **read_community_name** in the Community name field.

5. Scroll down and click the **Add** button to add to the list of destinations.

6. Repeat steps 3 through 5 for every MultiVantage Fault and Performance Manager IP address you are adding to the list of destinations. After adding each destination you will see the following screen.



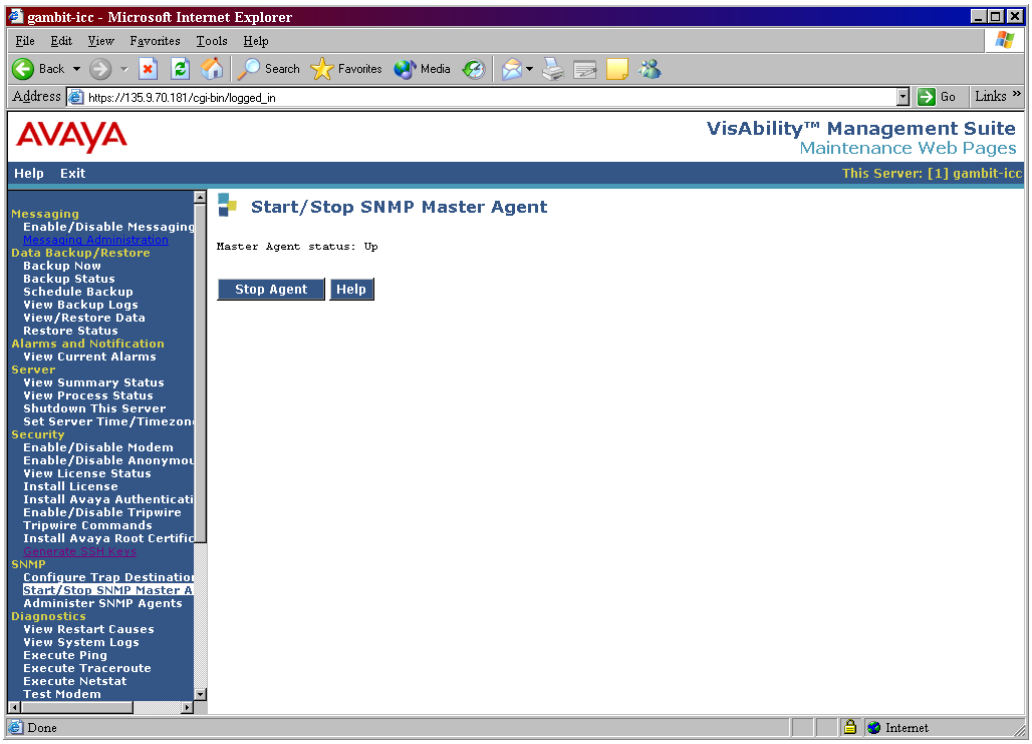
*** Note:** We do not recommend configuring multiple MFPM systems as a method of disaster recovery.

Go to "Procedure 5: Stop/Start Master Agent" on page 58.

Procedure 5: Stop/Start Master Agent

To stop/stop Master Agent:

From the **SNMP** heading located on the navigation frame, click the **Stop/Start Master Agent** link. The Start/Stop SNMP Master Agent web page appears. You can see the current state of the Master Agent. The default is **Up**. If it is not set to **Up**, then start it.

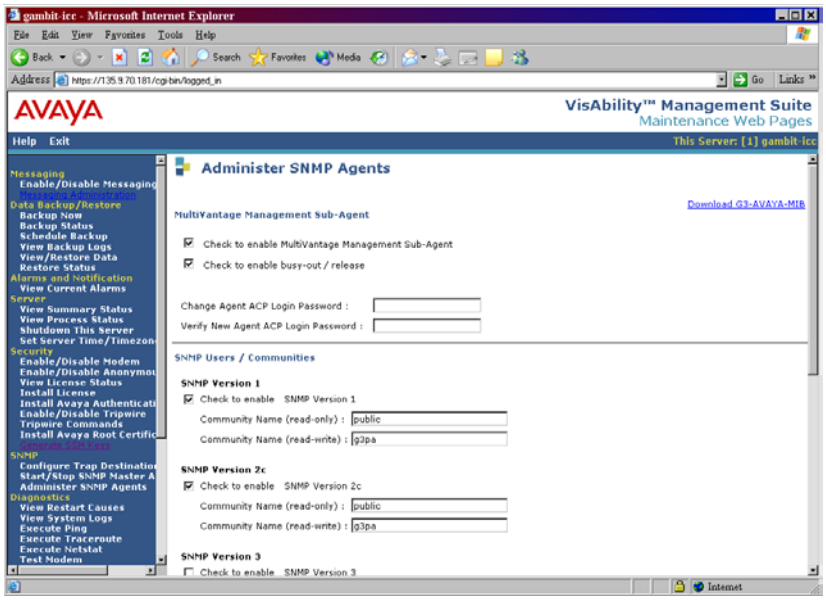


Go to "Procedure 6: Administer SNMP Agents" on page 59.

Procedure 6: Administer SNMP Agents

To administer SNMP agents:

1. From the **SNMP** heading located on the navigation frame, click **Administer SNMP Agents**. The Administer SNMP Agents page is displayed.



2. Select the first checkbox, **Check to enable MultiVantage Management Sub-Agent**.

3. If you want to use the busyout/release function in MFPM, select the second checkbox, **Check to enable busy-out / release**.

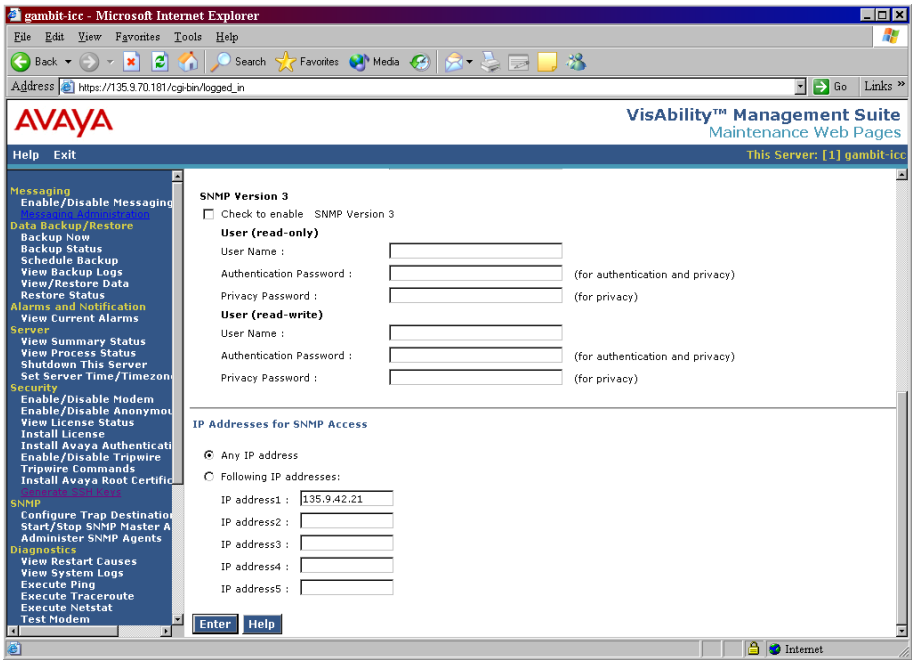
4. Enter the **`acpsnmp password`** in the **Change Agent ACP Login Password**. Enter the **`acpsnmp`** password again in the **Verify New Agent ACP Login Password**. The password defaults to a void state and if the password is *not* set, the agent will not be able to log in. It is very important that you enter the password twice.

5. Enable both **SNMP Version 1** and **SNMP Version 2**. Note that the read community name must match the information used in "Procedure 4: Configure Trap Destinations" on page 56.

   a. In the **SNMP Users / Communities** setup box, check the box below **SNMP Version 1** and enter the read community name AND the read/write community name, for example: `public for read-only and g3pa for read/write`

   b. In the **SNMP Users / Communities** setup box, check the box below **SNMP Version 2** and enter the read community name AND the read/write community name, for example: `public for read-only and g3pa for read/write`

6. Scroll down on this page and complete the form. Enter the IP address in the **IP Addresses for SNMP Access** setup box. Enter the IP addresses of all the MFPM servers you intend to send the data. You can select the radio button for **Any IP address** to allow access from any MultiVantage Fault and Performance Manager server.



7. Click the **Enter** button at the bottom of the page. The Administer the SNMP Agent setup is complete.

Go to "Procedure 7: Add the MultiVantage Sub-Agent" on page 61.

Procedure 7: Add the MultiVantage Sub-Agent

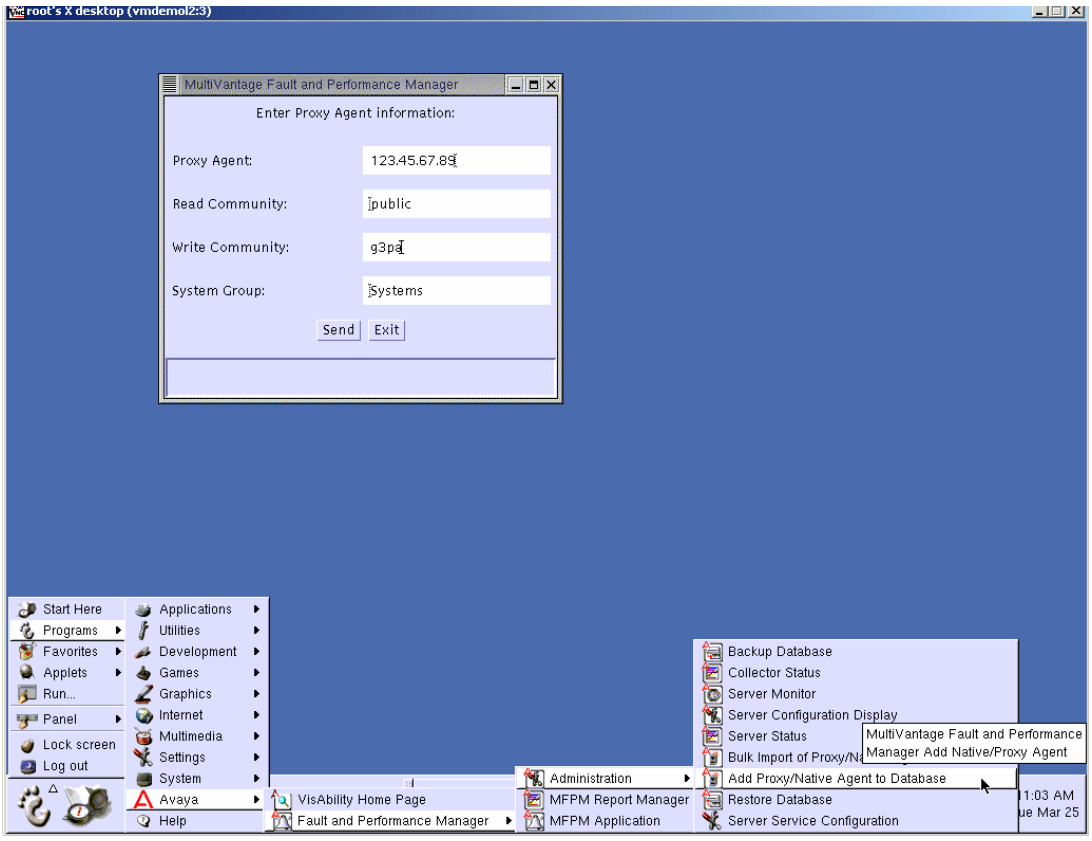
To add the MultiVantage Sub-Agent:

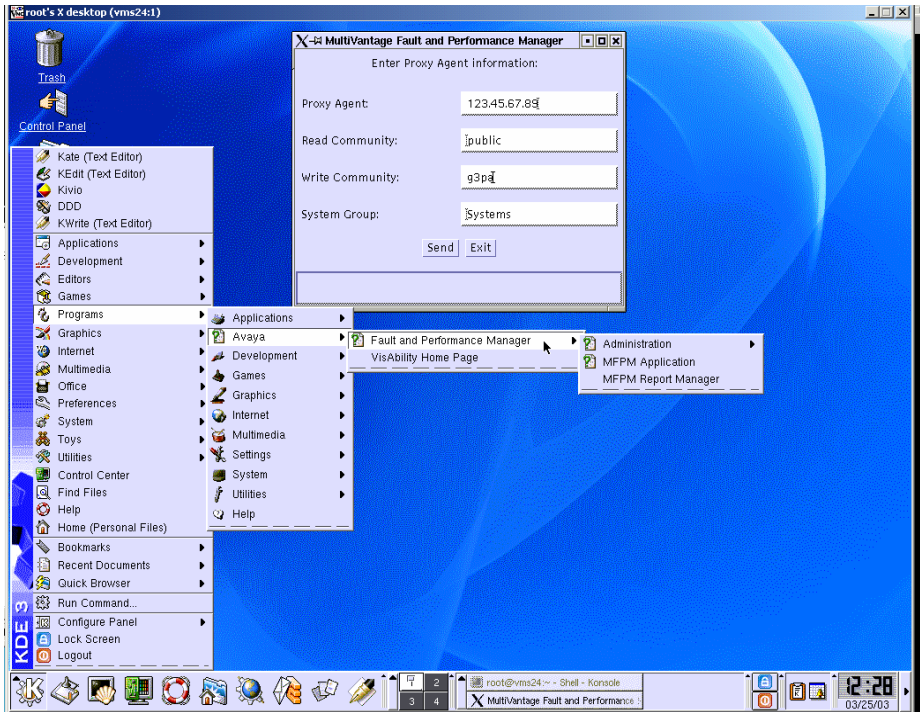
1. Log in to the VisAbility Linux server as root.
2. Perform one of the following steps:
   - If you are using Gnome, select **Foot icon>Programs>Avaya>Fault and Performance Manager>Administration>Add Proxy/Native Agent to Database>MultiVantage Fault and Performance Manager Add Native/Proxy Agent**.
   - If you are using KDE, select **K icon>Programs>Avaya>Fault and Performance Manager>Administration>Add Proxy/Native Agent to Database>MultiVantage Fault and Performance Manager Add Native/Proxy Agent**.
3. Enter the following information:
   - IP address of the Proxy Agent
   - Read community name
   - Write community name
   - System group

*** Note:** The read community name and the write community name *must* match *exactly* to the community names that were previously used in setting up the Sub-Agent in the web pages. (See "Procedure 6: Administer SNMP Agents" on page 59.)

This will allow the MultiVantage Sub-Agent to connect to the MultiVantage Fault and Performance Manager application. The following will occur:

- An entry will be added to the MultiVantage Fault and Performance Manager database.
- An icon will be created on the MultiVantage Fault and Performance Manager tree.
- The configuration information will be updated.





4. To verify that this is fully functional, go to the MultiVantage Fault and Performance Manager application and run a Refresh Alarms/Errors from the System Status screen of the node.

6 Getting Started

This chapter describes the purpose of and navigational instruction for the windows within Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager). In this chapter you will learn about the following windows and processes:

- Executing auto discovery on Fault and Performance Manager HP OpenView system
- Executing auto discovery on Fault and Performance Manager stand-alone system
- Starting the Fault and Performance Manager client from the Linux server
- Exiting the Fault and Performance Manager client from the Linux server
- Starting the Fault and Performance Manager client from a web browser
- Exiting the Fault and Performance Manager client from a web browser
- NMS maps
- Map commands
- Online Help system

Starting the Administrative GUI

The Fault and Performance Manager Administrative GUI lets you specify data collection parameters, create and save report definitions, and schedule reports. You must start this GUI to perform any of these tasks.

Procedure

Complete the procedure below to log in and exit Fault and Performance Manager, and to log off the NMS from the root map.

1. At the login prompt, type **root** and press **ENTER**.

2. At the password prompt, type the root password and press **ENTER.**

3. Open a terminal window.

   The system displays the Linux prompt.

4. At the Linux prompt, type **. /etc/avaya/mfpm/ENV** and press **ENTER.**

5. Type: **cd /usr/local/avaya/mfpm/bin/ and press ENTER.**

6. Execute one of the following scripts to access the information.

   — . /MFPMgui - launches Fault and Performance Manager. Add a voice system name at the end of the command to launch the application for a specific voice system.

   — . /PAdiscovery - launches Fault and Performance Manager to add new Proxy Agents.

   — . /MFPMgui_RM - launches the Fault and Performance Manager Report Manager.

   — . /MFPMgui_Exc - launches the Fault and Performance Manager Exception Report for all MultiVantage solutions registered in Fault and Performance Manager. Optionally, add the voice system name at the end of the command for the MultiVantage solution Exception Report for a specific voice system.

Starting the Fault and Performance Manager Client from a Web Browser

When you start the Fault and Performance Manager client from a web browser, you can only view; you can not make changes. You can start the client from a browser only if the browser meets the requirements specified in the VisAbility Management Suite Services Support Plan. Contact your client executive for the requirements.

*** Note:** You cannot perform administration functions or save reports created from the browser.

Procedure

Complete the procedure below to start the Fault and Performance Manager client from a web browser.

1. Open a supported browser.
2. At the URL address line, type the IP address for the Linux server where Fault and Performance Manager is installed and press **ENTER.**

   The system displays the VisAbility home page.
3. Click on **Products.**

   The Product page appears.
4. Read the installation information.
5. Click **Download.**

   A dialog box displays the progress of the download.
6. Click **Open.**

   A dialog box displays vms_client_cdexe file downloading.

   The WinZip Self-Extractor dialog box appears.
7. Click **Setup** to unzip the file.

   The system displays the Avaya VisAbility Management Suite Network Management Client for Window screen.
8. Click **Install Network Management Client Products.**

   The system indicates that it is preparing the wizard and then displays the Welcome screen.
9. Click **Next** and follow the prompts.
10. At the URL address line:

    a. Type the IP address for the Linux server where Fault and Performance Manager is installed and at the end of the address.

    b. Type **/mfpm**.

    c. Press **ENTER**.

    The Java Plugin Security Warning appears.
11. Click **Grant this Session**.

    The Avaya VisAbility Management Suite screen displays and Fault and Performance Manager launches.

Starting the Online Help

To start the online help, with Fault and Performance Manager open, choose **Help>Help Topics** or **Help>Current Panel**.

The online help system replaces the user guide for Fault and Performance Manager. The help screens contain the information listed below:

- Description and purpose of the screen
- Procedure to complete appropriate tasks on the screen
- Links to Related topics for more information

Help button

A Help button is also available on many tabs, panels, and dialog boxes. Clicking the Help button displays the help topic for the current screen.

Exiting the Fault and Performance Manager Client from a Web Browser

To exit the Fault and Performance Manager client from a web browser, choose **File>Exit.**

Fault and Performance Manager Integration with NMS

Before you integrate Fault and Performance Manager with the NMS, you must have installed the Fault and Performance Manager client on the HP OpenView Windows 2000 server. After installing the client, you must run mfpmconfig again to configure the HP OpenView server config service TCP port number.

Understanding the NMS Maps

The Network Management System Integration (NMSI) is one of the programs in Fault and Performance Manager, and is intended to integrate Fault and Performance Manager into the HP OpenView network management application.

This capability does not exist for Linux systems. Linux users execute a Linux command in the command prompt line to integrate Fault and Performance Manager into their own existing application.

This integration allows you to monitor your Avaya telecommunication elements and data networks from the same workstation.

NMS maps

NMSI uses the Auto-Discovery program to find and transmit system data from the managed nodes (supported systems) to the NMSI programs.

The NMSI uses the data received from Auto-Discovery to create and update the NMS maps, which include:

- NMS Root map
- VisAbility Fault and Performance Manager submap
- VisAbility USA and state submaps
- VisAbility custom submaps

The sections below describe the objects (system icons and connection lines) that display on the map and the color schemes that indicate the current status of the objects.

Root Map

The root map on the Network Management System (NMS) name "default" is the initial user interface to the various VisAbility submaps mentioned in the previous section.

NMSI places "explodeable" icons representing the various VisAbility submaps on the root map. The VisAbility submap icons lead to submaps that contain Proxy Agents and Managed Nodes that have been administered by the user in MFPM. The Voice System icons on these submaps are also explodeable icons that lead to submaps that show the various IP devices managed by each Voice System.

The icon names that display on the root map are:

- VisAbility Fault and Performance Manager MAP identifies a Generic submap.
- VisAbility USA MAP identifies the USA map and associated state submaps.

- VisAbility custom submaps will be used if defined by the user. Custom submaps need not have an associated icon, however, if an icon is used, be aware that the Custom submap is found by using the submap name, not the icon title. During discovery if a Custom submap is not found on which a object is to be placed the object will be placed on the Generic submap.

Proxy Agent icon colors

The table below contains Proxy Agent icon colors that display on HP OpenView maps. The colors indicate whether or not Proxy Agent is responding to requests.

Table 9. Proxy Agent Icon colors

Object	HP OpenView Color
Proxy Agent icon	**Dark Blue** = Unknown. Proxy Agent is not responding **Green** = Normal **Cyan** = Warning. Proxy Agent is responding, but is not honoring SNMP requests. Indicates that the SMNP community string for the NMS is incorrect. **Red** = Major. Proxy Agent failed to forward an alarm to INADS on its last try.

Fault and Performance Manager icon colors

Fault and Performance Manager maintains a list of active exceptions for the systems listed below:

- MultiVantage solutions
- Multipoint Conferencing Unit (MCU)

Fault and Performance Manager treats the MCUs as MultiVantage solutions.

The table below contains the MultiVantage solution icon colors and Proxy Agent line connections that display on the Fault and Performance Manager maps.

Table 10. MultiVantage Solution icon colors

Object	HP OpenView Color
MultiVantage solution icon MCU	**Dark Blue** = Unknown. Proxy Agent is not responding **Green** = Normal **Cyan** = Warning **Yellow** = Minor **Orange** = Major **Red** = Critical
Line connections to MultiVantage solution icons	**Black** = Up **Red** = Down or Other **Yellow** = Init (initiating) **Cyan** = Off **Salmon** = Idle for dynamic connection
NOTE: The "Dispatch Alert" text string and the flashing LSP icons are visible only when you are working in the NMS console. (This information will not appear in the NMS browser.)	

Other system icon colors

The NMSI only supports alarm traps from Proxy Agent for the systems below:

- DEFINITY AUDIX releases 3.1 through 4.0
- Intuity AUDIX release 4.3 through 5.1 (with or without the remote maintenance board)
- Intuity Interchange release 5.1 through 5.3
- Call Management System (CMS) R3V6 through R3V8
- CONVERSANT release 7.0

The Fault and Performance Manager maps provide only telnet support to the products above.

The table below contains the other system icon colors and Proxy Agent line connections that display on the Fault and Performance Manager maps.

Table 11. Other system icon colors

Object	HP OpenView Color
Other system icons for: DEFINITY AUDIX Intuity AUDIX Interchange CMS CONVERSANT	**Dark Blue** = Unknown. Proxy Agent is not responding **Green** = Normal **Cyan** = Warning **Yellow** = Minor **Orange** = Major
Line connections to other system icons	**Black** = Up. Proxy Agent is running and available to receive alarm traps. **Red** = Proxy Agent is stopped and cannot receive alarm traps.

Executing Auto-Discovery

This section is for NMSI Fault and Performance Manager systems only.

Auto-Discovery is a feature of your NMS that automatically gathers information about the managed nodes (voice elements) in your telecommunications system, and presents that information graphically using icons and maps. Auto-Discovery creates and updates the icons and submaps from data received from Proxy Agents that are connected to the managed nodes.

To execute Auto-Discovery, complete the following steps.

1. From the Linux server, type PAdiscovery
2. Enter the IP address of the Proxy Agent computer.
3. Enter the read and write community strings.

*** Note:** It will take some time for any new managed nodes to be discovered by MFPM and configuration data collection to take place. Only then will there be meaningful information on the NMS maps for these nodes.

4. From the HP OpenView server, click VisAbility>System View>Refresh Entire Map,

Executing Commands from NMS Maps

The NMS Integration (NMSI) program allows users to execute various commands from any of the NMS maps. Most of the commands perform operations on the systems that display on the selected map.

Users can execute the commands in two ways:

- Select a command from a menu
- Right-click the mouse on the object, and select the appropriate command from the popup menu

You cannot run MFPM-type commands from HP OpenView on a Solaris server unless the interface to HP OpenView is displayed in a web browser.

The sections below explain the commands and the execution options.

Description of Commands

The table below lists the commands that users can execute from any NMS map. The Description column describes the result of the command.

Depending on which NMSI command is selected and run, icons on the NMS maps can change status, be added or removed from the map, etc.

MultiVantage Configuration Manager, Avaya Site Administration, VAL Manager, Avaya Terminal Configuration, Avaya Terminal Emulator, MG Device Manager, VMON, Proxy Status, Proxy Cache Status, and Proxy Incoming AlarmLog applications and commands can also be launched out of the NMS.

Table 12. NMS Map commands

Command	Description
Network Management Application (Fault and Performance Manager product)	This command displays the main window, which contains the systems group navigation tree and configuration and status window. If you execute this command for a specific MultiVantage solution on the NMS map, then the command opens the main window with focus on the selected MultiVantage solution.
Report Generator	This command displays the Report Generator window of the Fault and Performance Manager.
Exception Report	This command displays the results of a Fault and Performance Manager Exception report. You can only execute this command for a specific MultiVantage solution on the map. The report shows exceptions only for the selected MultiVantage solution.
	1 of 4

Table 12. NMS Map commands (Continued)

Command	Description
Refresh Entire Map	The Refresh Entire Map process is primarily driven by the Fault and Performance Manager database and collection process. The database is used because not all Avaya products that Fault and Performance Manager deals with are IP based. Only IP Phones are exclusively obtained from the set of objects that HP OpenView has discovered. Therefore, the Refresh Entire Map process will place icons on one of the submaps and show connectivity between that device and others without regard to whether HP OpenView can discover that device, except for IP phones. Because the Refresh Entire Map process is driven by the Fault and Performance Manager database, it works primarily in a top down manner; that is, from Proxy Agents out to managed nodes, managed nodes out to boards, boards out to IP Phones. The case where IP Phones connect directly to a voice system refresh works in the reverse order, that is from the IP Phones to the voice system. A Refresh Entire Map must be performed to discover new Proxy Agents and new managed nodes. Each time a Refresh Entire Map is performed, the icons for all objects placed on NMS maps by NMSI will be removed, and the underlying HP OpenView object will remain in the database. During the Refresh Entire Map process, the text message “synchronizing” is shown at the bottom left of the HP OpenView GUI. (This is also true for other System View commands.) At the end of the Refresh Entire Map process, this text message disappears to denote that the command has completed. The time needed to perform a Refresh Entire Map depends primarily on the size of your network. For the Refresh Entire Map command to run, the following conditions must be met: • The MFPM server must be operational. • HP OpenView must have a Read-Write map open. • A connection must be established between HP Open View and the Fault and Performance Manager server process, NmsiServer. • Media Gateways and IP phones must be SNMP manageable from HP OpenView.
	2 of 4

Table 12. NMS Map commands (Continued)

Command	Description
Re-register with Server	The Re-register with Server establishes a connection between the Fault and Performance Manager server and HP OpenView. A Re-register with Server is done automatically when the HP OpenView GUI is started. However, if the Fault and Performance Manager server is brought down while the HP OpenView GUI is running, a connection can be established using the Re-register with Server command. You can run the Re-register with Server command even if a session already exists; this does not cause problems. In fact, running the Re-register with Server command is the simplest way to verify that a connection exists between HP OpenView and the Fault and Performance Manager server. If a connection cannot be established, an error message pops up on the screen. If the connection between HP Open View and the Fault and Performance Manager server is lost, all interaction between HP OpenView and the Fault and Performance Manager server is lost as well.
Refresh Voice System	Once a voice system is selected, if not an ICC voice system, the Refresh Voice System command works just like the Refresh Entire Map command, only on a per-voice system basis. Also see the Refresh Entire Map command. You can select one or more voice systems with this command.
Refresh C-LAN	This command is only available on a C-LAN. Once a C-LAN is selected, the Refresh C-LAN command is enabled. This command works just like the Refresh Entire Map command, only on a per-C-LAN basis. Also see the Refresh Entire Map command. You can select one or more C-LAN with this command.
Cleanup DB	The Cleanup DB command removes objects created by the Refresh Entire Map command, as long as the object has no associated icon.
Telnet to Proxy Agent	This command displays the telnet window to Proxy Agent. From the telnet window, users can log in to Proxy Agent and initiate an emulation session to cut-through to the managed node.
	3 of 4

Table 12. NMS Map commands (Continued)

Command	Description
Telnet to Managed Node	This command is for IP-connected nodes associated with a Proxy Agent. Users can telnet directly to the node rather than going through Proxy Agent.
Update System View Status	This command retrieves and displays the current status of the Managed Nodes in the NMS.
Update Voice System Status	For each Voice System that is selected on the NMS map, this command retrieves and updates the current status of the Voice System and the IP devices contained in it. You can select one or more voice systems with this command.
Update CLAN Status	For each CLAN that is selected on the NMS map, this command retrieves and updates the current status of the CLAN and the IP devices registered with it. You can select one or more CLAN with this command.
Acknowledge Active LSP	When an LSP is found to be "Active" by the NMS, it begins to flash on the NMS map. For each "flashing" LSP that is selected on the NMS map, the flashing stops. If you perform a "Refresh" involving "Active" but non-flashing LSPs, the "Active" but non-flashing LSPs will begin flashing again. You can select one or more LSPs with this command.
	4 of 4

Exiting the Fault and Performance Manager Client from the Linux Server

Clicking the “X” box in the upper right corner results in unpredictable behavior. To exit the application, follow the steps below:

1. To exit Fault and Performance Manager, from the menu bar on any screen, click **File > Exit.**

   The system exits the product and displays the Root map.

2. To log off the NMS, click **Map > Exit.**

   The system displays the Linux login prompt.

Glossary and Abbreviations

A

ATAC
See “Avaya Technology and Consulting (ATAC)” on page 11.

M

managed node
In this document, a managed node is any system (voice system or otherwise) that can be viewed and monitored using Fault and Performance Manager and Proxy Agent.

MultiVantage software
The call processing software that runs on MultiVantage solutions. Formerly known as DEFINITY software.

MultiVantage solution
Any of the products that run MultiVantage software. Formerly known as DEFINITY system, DEFINITY ECS, switch, PBX, or voice system.

N

Network Management Server
This is the Windows box that you can install Windows-based VisAbility Management applications on.

Network Management System
A system that lets you monitor the health and status of devices on your data network. For example, HP OpenView.

R

RNIS
See “Avaya Remote Network Integration Services (RNIS)” on page 11.

S

supported systems
In this document, a “supported system” is any of the voice systems or adjuncts that Proxy Agent works with. See “Supported Systems” on page 18.

SNMP
Simple Network Management Protocol.

System Management Server
This is the Linux box that you install Fault and Performance Manager or Proxy Agent on.

T

TSO
See “Avaya Technical Service Organization (TSO)” on page 12.

Index