



# **Avaya MultiVantage™ Fault and Performance Manager**

Release 1.0  
Installation and Configuration

555-233-138  
Issue 2  
August 2002

**Copyright 2002, Avaya Inc.  
All Rights Reserved**

### **Notice**

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

### **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 is not working on your company’s behalf). Be aware that there may be 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 suspect 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 is not 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 - Avaya’s customer 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
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

### **Voice Over Internet Protocol (VoIP)**

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya’s recommendations for configuration, operation and use of the equipment. **YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.**

### **Standards Compliance**

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user’s authority to operate this equipment.

The equipment described in this manual complies with standards of the following organizations and laws, as applicable:

- Australian Communications Agency (ACA)
- American National Standards Institute (ANSI)
- Canadian Standards Association (CSA)
- Committee for European Electrotechnical Standardization (CENELEC) – European Norms (EN’s)
- Digital Private Network Signaling System (DPNSS)
- European Computer Manufacturers Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- FCC Rules Parts 15 and 68
- International Electrotechnical Commission (IEC)
- International Special Committee on Radio Interference (CISPR)
- International Telecommunications Union - Telephony (ITU-T)
- ISDN PBX Network Specification (IPNS)
- National ISDN-1
- National ISDN-2
- Underwriters Laboratories (UL)

## Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Laser products, equipment classification and requirements:

- IEC 60825-1, 1.1 Edition
- Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition
- Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997
- One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

## Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

## Federal Communications Commission Statement

### Part 15:

**Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.**

**Part 68: Answer-Supervision Signaling.** Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

This equipment complies with Part 68 of the FCC Rules. On the rear of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

## Means of Connection

Connection of this equipment to the telephone network is shown in the following table.

Manufacturer's Port Identifier	FIC Code	SOC/REN/A.S. Code	Network Jacks
Off/On premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
CO trunk	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN, 1KN, 1SN	6.0F	RJ48C, RJ48M
120A2 channel service unit	04DU9-DN	6.0Y	RJ48C

If the terminal equipment (for example, the MultiVantage™ Solution equipment) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

### Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This digital apparatus does not exceed Class A limits for radio noise emission set out in the radio interference regulation of the Canadian Department of Communications.

Le Présent Appareil Numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils maniques de la class A prescrites dans le règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

### DECLARATIONS OF CONFORMITY

#### United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site:

[http://support.avaya.com/elmodocs2/DoC/SDoC/index.jhtml/](http://support.avaya.com/elmodocs2/DoC/SDoC/index.jhtml)

All MultiVantage™ system products are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at:

<http://www.part68.org/>

by conducting a search using "Avaya" as manufacturer.

### European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Européenne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) signed by the Vice President of MultiVantage™ Solutions research and development, Avaya Inc., can be obtained by contacting your local sales representative and are available on the following Web site:

<http://support.avaya.com/elmodocs2/DoC/IDoC/index.jhtml/>

### Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

### Network Connections

Digital Connections - The equipment described in this document can be connected to the network digital interfaces throughout the European Union.

Analogue Connections - The equipment described in this document can be connected to the network analogue interfaces throughout the following member states:

Belgium	Germany	Luxembourg
Netherlands	Spain	United Kingdom

### LASER Product

The equipment described in this document may contain Class 1 LASER Device(s) if single-mode fiber-optic cable is connected to a remote expansion port network (EPN). The LASER devices operate within the following parameters:

- Maximum power output -5 dBm to -8 dBm
- Center Wavelength 1310 nm to 1360 nm
- CLASS 1 LASER PRODUCT IEC 60825-1: 1998

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure. Contact your Avaya representative for more laser product information.

### To order copies of this and other documents:

Call: Avaya Publications Center

Voice 1.800.457.1235 or 1.410.568.3680

FAX 1.800.457.1764 or 1.410.891.0207

Write: Globalware Solutions

200 Ward Hill Avenue

Haverhill, MA 01835 USA

Attention: Avaya Account Management

E-mail: [totalware@gwsmail.com](mailto:totalware@gwsmail.com)

# Table of Contents

---

<b>Preface</b> .....	<b>7</b>
Purpose .....	7
Prerequisites .....	7
Intended Audience .....	7
Conventions Used in This Book .....	7
Additional Resources .....	8
Tell Us What You Think! .....	8
How to Get This Book (and Others) on the Web .....	9
How to Order More Copies of This Book .....	10
<b>Chapter 1 — Resources and Notices</b> .....	<b>11</b>
Avaya Technology and Consulting (ATAC) .....	11
Avaya Remote Network Implementation Services (RNIS) .....	11
Avaya Technical Service Organization (TSO) .....	12
Avaya Network Management Software Systems	
Support Group (NMSSS) .....	12
Avaya Contact Information .....	12
Third-Party Resources .....	14
System Security Notices .....	14
Network Security .....	14
Toll Fraud Security .....	15
<b>Chapter 2 — Overview</b> .....	<b>17</b>
Product Description .....	17
Supported Systems .....	18
System Requirements .....	19
Installation and Configuration Overview .....	20
<b>Chapter 3 — Installing and Upgrading Fault and Performance Manager</b> .....	<b>21</b>
Customer Pre-Installation Tasks .....	21
Completing the VMS001 Form .....	21
Installing on Linux .....	22
Configuring Fault and Performance Manager to Integrate with	
HP OpenView .....	23
Installing Avaya NMSI Components on Windows .....	26
Installing the Java Development Kit .....	27
Installing Avaya NMSI Components .....	28

---

Finishing the Installation .....	28
Configuring Fault and Performance Manager for Stand-Alone Operation .....	29
Moving the DNM 3.0 or 4.0 Database to Fault and Performance Manager .....	30
Installing the Fault and Performance Manager Client on Windows	31
Starting the Installation .....	31
Installing the Java Runtime Environment .....	33
Installing the Required Components .....	33
Finishing the Installation .....	34
Uninstalling Fault and Performance Manager .....	35
<b>Chapter 4 — Customizing Fault and Performance Manager .....</b>	<b>37</b>
Introduction .....	37
System Commands .....	38
Start and Stop Commands .....	38
System Health Commands .....	38
Backing up the Database .....	39
Restoring the Database .....	40
Administering Alarm Notification Services .....	41
Description of Alarm Notification Options .....	41
DEFINITY_ARS Script .....	43
AUDIX_ARS Script .....	44
CMS_ARS Script .....	45
CONVERSANT_ARS Script .....	46
<b>Chapter 5 — Getting Started .....</b>	<b>49</b>
Executing Auto-Discovery .....	49
Executing Auto-Discovery on Public Networks .....	50
Executing Auto-Discovery on Private Networks .....	50
Starting the Administrative GUI .....	52
Exiting the Fault and Performance Manager Client from the Linux Server .....	53
Starting the Fault and Performance Manager Client from a Web Browser .....	53
Starting the Online Help .....	54
Exiting the Fault and Performance Manager Client from a Web Browser .....	55
Fault and Performance Manager Integration with NMS .....	55
Understanding the NMS Maps .....	55
Root Map .....	56
Executing Commands from NMS Maps .....	59
Description of Commands .....	59
<b>Glossary and Abbreviations .....</b>	<b>65</b>
<b>Index .....</b>	<b>67</b>

# 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 B3-H25  
1300 W. 120th Ave.  
Denver, CO 80234-2726  
USA

Fax: Fault and Performance Manager Documentation Team  
+ 1 303 538 1741

E-mail: [document@avaya.com](mailto:document@avaya.com)

---

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

To view or download the latest version of this book, complete the following steps:

1. Install your internet browser.

Most computers are sold with browsers already installed.

2. Get access to the Internet.

If you do not already have access to the Internet, contact an Internet Service Provider (ISP) and set up an account.

3. Set up your browser preferences.

Refer to the documentation that came with your browser.

4. Install Adobe Acrobat Reader with Search, version 5.0 or later.

This is available on your CD-ROM or from: <http://www.adobe.com>.

5. Access <http://www.avaya.com/support>

6. Click `Online Services`.

7. Click `Documentation`.

8. Click `System and Network Management`.

9. Under the heading “VisAbility Management Suite,” click the link `MultiVantage Fault and Performance Manager 1.0`.

10. Locate the title of the book you want and then click it.

## 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 2  
Date: August 2002

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: + 1 410 568 3680  
Fax: + 1 410 891 0207

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 and Avaya MultiVantage™ Proxy Agent (Proxy Agent).

## Avaya Remote Network Implementation Services (RNIS)

For this product, RNIS offers customers the following services:

- Verify platform readiness
- Remotely install Fault and Performance Manager
- Connect and configure voice systems to work with Fault and Performance Manager
- Verify customer acceptance

## Avaya Technical Service Organization (TSO)

The TSO provides support for Fault and Performance Manager and Proxy 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*

<b>Resource</b>	<b>Contact Information</b>
Avaya Support Center	<a href="http://support.avaya.com/">http://support.avaya.com/</a>
Network Management Software Systems Support group	1-800-237-0016.
Avaya Technical Services Organization (TSO)	For calls about Avaya Site Administration: 1-800-242-2121 extension 15312.
Remote Network Implementation Services (RNIS)	<a href="http://www1.avaya.com/enterprise/who/docs/dataimplementation/fullprodinfo.html">http://www1.avaya.com/enterprise/who/docs/dataimplementation/fullprodinfo.html</a>
Toll Fraud Intervention	1-800-643-2353 prompt 1

*Table 2. Avaya Internal Resources*

<b>Resource</b>	<b>Contact Information</b>
Avaya Enterprise Management Support	<a href="http://aem-support.dr.avaya.com/">http://aem-support.dr.avaya.com/</a>
Avaya Technology and Consulting (ATAC)	Phone: 1-888-297-4700, prompt 2, 6 Main site (requires a password): <a href="http://forum.avaya.com">http://forum.avaya.com</a>
Remote Network Implementation Services (RNIS)	<a href="http://associate2.avaya.com/sales_market/products/data-implementation-services/">http://associate2.avaya.com/sales_market/products/data-implementation-services/</a>
VisAbility Management Services Support Plan	<a href="http://associate2.avaya.com/solution/support_plans/#Enterprise">http://associate2.avaya.com/solution/support_plans/#Enterprise</a>
VMS001 Form	<a href="http://associate2.avaya.com/sales_market/products/data-implementation-services/">http://associate2.avaya.com/sales_market/products/data-implementation-services/</a> 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: <a href="http://www.openview.hp.com">http://www.openview.hp.com</a>
Microsoft	Main site: <a href="http://www.microsoft.com">http://www.microsoft.com</a>
Red Hat Linux	Main site: <a href="http://www.redhat.com">http://www.redhat.com</a>
Peregrine	Main site: <a href="http://www.peregrine.com">http://www.peregrine.com</a> Scroll down to: action request system
Vytek	Main site: <a href="http://www.vytek.com">http://www.vytek.com</a>
Versant	Main site: <a href="http://www.versant.com">http://www.versant.com</a>

## 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 and Windows 2000 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 "Avaya Contact Information" on page 12 for the Toll Fraud Intervention phone number.



# 2 Overview

---

Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager) together with Avaya MultiVantage™ Proxy Agent (Proxy 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 and Proxy 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 Proxy 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 1.1 supports both SNMP V1 and V2c get and set requests and SNMP V1 alarm traps for the following systems:

- DEFINITY<sup>®</sup> ECS Releases 9.2 through 10.x
- Avaya MultiVantage<sup>™</sup> Software
- Survivable Remote Processors (SRPs)
- Multipoint Conferencing Unit (MCU) Release 6.0 and later
- Avaya<sup>™</sup> G600 Media Gateway
- Avaya<sup>™</sup> CMC1 Media Gateway

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

---

Fault and Performance Manager Release 1.1 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 5.3
- Call Management System (CMS) R3V6 through R3V8
- CONVERSANT Release 7.0

## 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 certified. For the Red Hat URL, see "Third-Party Resources" on page 14.



**Customers are solely responsible for upgrading their network platforms to meet the NMS platform requirements for Fault and Performance Manager Release 1.1.**

### Software

Fault and Performance Manager Release 1.1 operates on Red Hat Linux 7.3. The optional NMSI component runs on Windows 2000 running HP OpenView 6.2.

# 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.** (For upgrades only:) Complete the procedure, "Backing up the Database" on page 39.
- 3.** Installers complete "Installing on Linux" on page 22.
- 4.** 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.
- 5.** 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.
- 6.** Installers complete "Moving the DNM 3.0 or 4.0 Database to Fault and Performance Manager" on page 30.
- 7.** Installers complete "Installing the Fault and Performance Manager Client on Windows" on page 31.
- 8.** Installers complete "Administering Alarm Notification Services" on page 41.
- 9.** If you will be running Fault and Performance Manager with an NMS, then installers should complete "Executing Auto-Discovery" on page 49.
- 10.** 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 52.
- 11.** Customers meet with RNIS or the TSO (as appropriate) to complete a Technical Verification Checklist and a Customer Acceptance checklist.

# 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 1.1 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.

## 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
- Avaya TSO number: 1-800-242-2121, ext. 4-1080 or 720-444-1080

**\* 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 **cd /mnt/cdrom**

8. Type `vms_setup.bin` and press `ENTER`.

The message "Initializing wizard." appears followed by the Welcome screen.

9. Click `NEXT` and follow the prompts to complete the installation.

10. 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 be 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 `cd;/sbin/shutdown -r` 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 1.0
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.

## Moving the DNM 3.0 or 4.0 Database to Fault and Performance Manager

Only the root user should execute the procedure to move the database. You must back up the database before moving it to Fault and Performance Manager and then restore it after moving it to Fault and Performance Manager.

To move the database, there must be TCP/IP connectivity between the DNM 4.0 server and the Fault and Performance Manager server.

Users can execute the MigrateMFPM utility to migrate the database to the Fault and Performance Manager server after Fault and Performance Manager 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 move the database.

1. Close all windows and applications.
2. At the login prompt, type **root** and press **ENTER**.
3. At the password prompt, type the root password and press **ENTER**.
4. Type **MigrateMFPM** and press **ENTER**.

The system prompts you for information related to the migration. At the end, it displays the message:

```
Database migration was completed successfully.
```

# 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**.

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: `dnapcl.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 31, 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.



**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:

- 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

# 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 mfpd-server stop	Stops the Fault and Performance Manager system and prevents it from starting at system boot.
service mfpd-server start	Starts a stopped Fault and Performance Manager system and enables it to start at system boot.
service mfpd-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/mfpd/logs/MsgLog_[0-2]`

## System Health Commands

The table below contains the system health commands.

*Table 5. System Health commands*

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

---

# Backing up the Database

Only the root user should 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. 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]
```

7. Press ENTER.

Doing so selects “no.”

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

This restarts Fault and Performance Manager services.

# Restoring the Database

Only the root user should 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`
- `TT_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:

- Vyteck, *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 Vytex's TeleAlert.

*Table 7. Vytex 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 NMSI looks for the DEFINITY\_ARS script when one of the following events occur:

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

Then the NMSI calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the NMSI 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 NMSI looks for the AUDIX\_ARS script when one of the following events occur:

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

Then the NMSI calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the NMSI 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 NMSI looks for the CMS\_ARS script when one of the following events occur:

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

Then the NMSI calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the NMSI 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 NMSI looks for the CONVERSANT\_ARS script when one of the following events occur:

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

Then the NMSI calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then the NMSI 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 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

## 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, you must log in to the NMS network server and execute it through the NMS user interface.

## Executing Auto-Discovery on Public Networks

To execute Auto-Discovery on the public networks, complete the following steps.

1. At the Root map, select HP OpenView:
  - Click **Configuration > MFPM > Execute Auto-Discovery**
  - The system executes Auto-Discovery and logs the events in the Events Categories window.
2. To view the events In the Events Categories window,
  - Click **All Events**
  - Scroll down the list to find the message: Auto-Discovery Completed Successfully.
3. If appropriate, complete the procedure to "Executing Auto-Discovery on Private Networks" on page 50.
4. Verify that the Fault and Performance Manager installation and the NMS integration were successful. Refer to "Getting Started" on page 49.

## Executing Auto-Discovery on Private Networks

The procedure in this section is optional. For private networks, you must manually administer the fields in the Simple Network Management Protocol (SNMP) configuration file. Auto-Discovery uses these fields to access the SNMP data from the Proxy Agent.

### Required materials

You will need the completed VMS001 form. Refer to the Proxy Agent section and the fields listed below:

- Proxy Agent IP network address
- SNMP Get Community String
- SNMP Set Community String

---

**Procedure**

Complete the procedure below to execute Auto-Discovery on private networks.

1. Access the SNMP Configuration window from the NMS user interface.
2. If selected, turn off the button: **Use Proxy to access Target**
3. In the SNMP Configuration window, enter the data from the VMS001 form in the fields below. Do not change any other fields:

This information is listed in the "Network Managers" fields in the "Proxy Agent" section of the VMS001 form.

- a. In the Target field, type **IP address** for the Proxy Agent
- b. In the Community String field, type **private "get" name**
- c. In the Set Community String field, type **private "set" name**
- d. Click: **ADD**
- e. Click: **OK**

The system updates the fields and displays the Root map.

4. At the Root map, select HP OpenView from the menu bar
5. Select **Configuration > MFPM > Execute Auto-Discovery**

The system executes Auto-Discovery and logs the events in the Events Categories window.

6. To view the events In the Events Categories window, Click **All Events**

Scroll down the list to find the message:

Auto-Discovery Completed Successfully.

7. Verify that the Fault and Performance Manager installation and the NMS integration were successful. Refer to "Getting Started" on page 49.

# 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 the login name and press **ENTER**.
2. At the password prompt, type the 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.

---

## Exiting the Fault and Performance Manager Client from the Linux Server

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 **File > Close**.

The system displays the Linux login prompt.

## 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.

### 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>Contents**.

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 `mfpconfig` 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/Avaya Root map
- Avaya Fault and Performance Manager submap
- Avaya USA and state submaps
- 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 Fault and Performance Manager. Fault and Performance Manager creates additional submaps on only one NMS map.

### Proxy Agent submaps

NMSI places executable icons for the new maps on the root map. These icons represent the default location submaps that you administered on Proxy Agent for the managed nodes. The submaps options include: Generic, USA and associated State maps, and Custom.

The icon names that display on the root map are:

- Avaya Fault and Performance Manager MAP identifies a Generic submap.
- Avaya USA MAP identifies the USA map and associated state submaps.
- 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 Fault and Performance Manager 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	<p><b>Dark Blue</b> = Unknown. Proxy Agent is not responding</p> <p><b>Green</b> = Normal</p> <p><b>Cyan</b> = Warning. Proxy Agent is responding, but is not honoring SNMP requests. Indicates that the SMNP community string for the NMS is incorrect.</p> <p><b>Red</b> = Major. Proxy Agent failed to forward an alarm to INADS on its last try.</p>

## 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)
- Survivable Remote Processor (SRP)

Fault and Performance Manager treats the MCUs and SRPs 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*

<b>Object</b>	<b>HP OpenView Color</b>
MultiVantage solution icon MCU SRP	<b>Dark Blue</b> = Unknown. Proxy Agent is not responding <b>Green</b> = Normal <b>Salmon</b> = Dispatched <b>Cyan</b> = Warning <b>Yellow</b> = Minor <b>Orange</b> = Major <b>Red</b> = Critical
Line connections to MultiVantage solution icons	<b>Black</b> = Up <b>Red</b> = Down or Other <b>Yellow</b> = Init (initiating) <b>Cyan</b> = Off <b>Salmon</b> = Idle for dynamic connection

**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:	<b>Dark Blue</b> = Unknown. Proxy Agent is not responding
DEFINITY AUDIX	<b>Green</b> = Normal
Intuity AUDIX	<b>Salmon</b> = Dispatched
Interchange	<b>Cyan</b> = Warning
CMS	<b>Yellow</b> = Minor
CONVERSANT	<b>Orange</b> = Major
Line connections to other system icons	<b>Black</b> = Up. Proxy Agent is running and available to receive alarm traps. <b>Red</b> = Proxy Agent is stopped and cannot receive alarm traps.

## Executing Commands from NMS Maps

\* **Note:** Linux users execute the Fault and Performance Manager GUI script to launch the Fault and Performance Manager interface.

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 three ways:

- Select a command from a menu
- Double-click an object on the map
- Select objects from the third mouse button

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.

Based on the result of the command, the NMSI updates the NMS maps, changes the color of the status, and displays the appropriate NMS and Fault and Performance Manager windows.

*Table 12. NMS Map commands*

<b>Command</b>	<b>Description</b>
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 only for the selected MultiVantage solution.
Report Generator	This command displays the Report Generator window in Fault and Performance Manager.
Exception Report	This command displays the results of a Fault and Performance Manager Exception report.  If you execute this command for a specific MultiVantage solution on the map, then the report shows exceptions only for the selected MultiVantage solution.
	1 of 5

Table 12. NMS Map commands

Command	Description
Discovery	<p>The Discovery 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 Discovery 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.</p> <p>Because the Discovery 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 discovery works in the reverse order, that is from the IP Phones to the voice system. A Discovery must be performed to discover new Proxy Agents and new managed nodes. When the Discovery command is repeated, the icons for all objects discovered by Fault and Performance Manager will be removed, the underlying HP OpenView object will remain in the database.</p> <p>During the Discovery process, a flag is shown on the bottom of the HP OpenView display. At the end, a dialog box indicates that the Discovery is complete. The time needed to perform a Discovery depends primarily on the size of your network. For the Discovery command to run, the following conditions must be met:</p> <ul style="list-style-type: none"> <li>• The Fault and Performance Manager server must be operational.</li> <li>• HP OpenView must have a Read-Write map opened.</li> <li>• A connection must be established between HP Open View and the Fault and Performance Manager server process, NmsiServer. Refer also to the Fault and Performance Manager Login, Rediscover C-LAN, and Rediscover DEFINITY commands.</li> <li>• Media Gateways and IP phones must be SNMP manageable from HP OpenView.</li> </ul>
	2 of 5

*Table 12. NMS Map commands*

<b>Command</b>	<b>Description</b>
Login	<p>The Login establishes a connection between the Fault and Performance Manager server and HP OpenView. A login 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 Login command.</p> <p>You can run the Login command even if a login already exists; this does not cause problems. In fact, running the Login 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.</p>
Rediscover DEFINITY	<p>This command is not supported for Avaya S8300 voice systems. Once a voice system is selected, if not an ICC voice system, the Rediscover DEFINITY command works just like the Discovery command, only on a per-voice system basis. Also see the Discovery command.</p>
Rediscover C-LAN	<p>This command is only available on a C-LAN. Once a C-LAN is selected, the Rediscover C-LAN command is enabled. This command works just like the Discovery command, only on a per-C-LAN basis. Also see the Discovery command.</p>
Cleanup DB	<p>The Cleanup DB command removes objects created by the Discover command, as long as the object has no associated icon.</p>
Acknowledge Alert	<p>This command turns off alerting for a selected system icon and changes the color status to normal.</p>
	3 of 5

Table 12. NMS Map commands

Command	Description
Set Alert to Minor	<p>This command sets the alert level to Minor for the managed nodes listed below:</p> <ul style="list-style-type: none"> <li>• DEFINITY AUDIX</li> <li>• Intuity AUDIX</li> <li>• Intuity Interchange</li> <li>• Call Management System (CMS)</li> <li>• CONVERSANT</li> <li>• Avaya legacy system</li> </ul>
Show Managed Nodes	<p>This command displays the Managed Nodes list for a Proxy Agent. The list contains the current settings for all the managed nodes administered on the specific Proxy Agent, including:</p> <ul style="list-style-type: none"> <li>• Node Type and Node Name</li> <li>• Connection Type (static or dynamic), Connection Status, and Timeout minutes for dynamic connections</li> <li>• Submap type</li> <li>• Object Label which is the Node Name</li> </ul>
Connection Status	<p>This command displays the Connection Status window for a MultiVantage solution, MCU, or Survivable Remote Processor (SRP). The title bar on the window contains the name of the managed node.</p> <p>The Connection Status list contains the information below:</p> <ul style="list-style-type: none"> <li>• Connection Type (static or dynamic)</li> <li>• Connection State (Up, Off, etc.)</li> <li>• Counters for connection statistics</li> <li>• Alarm Forward Status</li> </ul>
Show MIB Values	<p>This command displays screens for viewing configuration, fault and performance information via the NMS platform menus.</p>
Start Connection	<p>This command instructs the Proxy Agent to start a connection to a MultiVantage solution, MCU, or SRP.</p> <p>The NMSI sets the connection state to init (initiating), which signals the Proxy Agent to connect to the managed node. The NMSI also changes the color of the connection line to the init color to indicate the current status.</p>
	4 of 5

*Table 12. NMS Map commands*

Command	Description
Stop Connection	<p>This command drops the connection between a Proxy Agent and a MultiVantage solution, MCU, or SRP.</p> <p>The NMSI sets the connection state to off, which signals Proxy Agent to drop the connection. The NMSI changes the color of the connection line to warning or unknown.</p> <p>When Proxy Agent drops the connection, NMSI again changes the color of the connection line to off.</p>
Telnet to Proxy Agent	<p>This command displays the telnet window to Proxy Agent.</p> <p>From the telnet window, users can log in to Proxy Agent and initiate an emulation session to cut-through to the managed node.</p>
Telnet to Node	<p>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.</p>
Refresh Alarms and Errors	<p>This command retrieves the status of systems that have dynamic connections to the Proxy Agent.</p> <p>The NMSI requests that Fault and Performance Manager update exception data for alarms and errors for selected MultiVantage solutions, MCU, and SRP systems. After Fault and Performance Manager updates the alarm and error data, the NMSI updates the system icons on the NMS maps.</p> <p>In addition, the NMSI adds an item called G3 MIB Values to the HP OpenView Fault menu.</p> <ul style="list-style-type: none"> <li>• When users select a MultiVantage solution icon from a map and the G3 MIB Values from the menu, the NMSI displays a list of MultiVantage solution MIB groups.</li> <li>• When users select one of the MultiVantage solution MIB groups from the list, the NMSI displays the values of the objects in the MIB group for the selected MultiVantage solution.</li> </ul>
	5 of 5

# 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 Implementation 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

---

## Symbols

>, meaning of 7

## A

ATAC 13

Auto-Discovery

execute on public networks 50

integration function 55

on private networks 50

Avaya Support Center web site 13

Avaya Technology and Consulting (ATAC)  
11

## B

backup, database 39

boldface, meaning of 7

books

giving feedback on 8

on the web 9

ordering 10

## C

CE marks 4

commands 38

system health 38

configuring FP Mgr for stand-alone 29

contact information

for Avaya 12

third party 14

## D

database

backup 39

restoring 40

definitions

FQDN 34

VisAbility Network Management Server 34

Discovery

introduction 61

documentation

giving feedback on 8

on the web 9

ordering 10

## E

editing system files 41

electromagnetic compatibility standards 3

Enterprise Management Support 13

## F

feedback, giving us your 8

FQDN, defined 34

## H

Hewlett-Packard web site 14

HP OpenView, integrating FP Mgr with 23

## I

installation

services 11

installing

FP Mgr client on Windows 31

integrating FP Mgr with HPOV 23

## M

Microsoft web site 14

## N

network

security 14

Network Management System (NMS)

integration process 55

## O

OpenView, integrating FP Mgr with 23

## P

passwords, changing 14

Peregrine web site 14

## R

Red Hat web site 14

requirements 19

restore database 40

RNIS 11

**S**

security

Avaya disclaimer 15

for networks 14

network 14

notices 14

toll fraud 15

toll fraud intervention 15

Services Support Plan, VisAbility Management 13

stand-alone configuration 29

standards

electromagnetic compatibility 3

system commands 38

system files, editing 41

system health 38

system requirements 19

**T**

Technical Service Organization 12

Technical Services Organization 12

toll fraud 15

Avaya disclaimer 15

intervention 15

Toll Fraud Intervention phone number 13

TSO 12

phone numbers 13

typographical conventions 7

**U**

Uninstalling FP Mgr 35

**V**

Versant web site 14

VisAbility Management Services Support Plan 13

VisAbility Network Management Server, defined 34

Vytek web site 14

**W**

web sites

Avaya 12

third-party 14