Avaya Integrated Management Release 3.0 Fault and Performance Manager Configuration

555-233-138
Issue 7
June 2005

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.

Warranty

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

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or 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.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Contacts* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Contacts* link. Then click the *International Services* link that includes telephone numbers for the international 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

TCP/IP Facilities

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

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.

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, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

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.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

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

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

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

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.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover 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.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that 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 tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	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	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) 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.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. 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 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.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect 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://www.avaya.com/support.

All Avaya media servers and media gateways 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 Europeénne*) 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).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

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。

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

Preface

Purpose

This book explains how to configure Avaya Fault and Performance Manager (Fault and Performance Manager).

Prerequisites

Configuring Fault and Performance Manager requires familiarity with network administration and knowledge of the Red Hat Linux operating system. 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 Avaya Fault and Performance Manager, see the Avaya Fault and Performance Manager online help. It explains how to perform basic administration tasks. To access the online help, start Avaya Fault and Performance Manager and choose **Help>Help Topics.**

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

Tell Us What You Think!

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

Mail:

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

Fax:

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

E-mail: document@avaya.com

How to Access Books on the Web

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

To view or download the latest version of the *Avaya Integrated Management* documentation:

1. Access http://www.avaya.com/support.
2. In the left column, click **System and Network Management**.
3. Scroll to **Integrated Management,** locate the product name, and click the link corresponding to the software release to display a list of available books for that product.

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 7
Date: June 2005

Call:

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

If you are calling from somewhere that cannot access US 1-800 numbers, then call:

Voice: + 1 207 866 6701
Fax: + 1 207 626 7269

Write:

Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835
USA

Chapter 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)

Avaya Technology and Consulting (ATAC) works with client teams to develop detailed solutions for connectivity to Avaya Communication Manager solutions. The ATAC also designs network configurations.

Communications, Solutions, and Integration (CSI) Group of Software Services

Avaya Communications, Solutions, and Integration (CSI) Group of Software Services offers customers the following services:

- Platform readiness verification
- Remote implementation and installation
- Network management server configuration
- Customer acceptance verification
- Custom on-site services

The CSI Group consists of the following two teams:

- **Converged Solutions Implementation Engineering**

  The Converged Solutions Implementation Engineering (CSIE) team implements multi-site media gateway (G350/G650/G700) deployment projects for both voice and data design. The overall direction of the CSIE team is to bring the correct methodology to these complex deployments that span various regions and to provide continuity to the overall project from the voice and data implementation standpoint.

- **Data Network Implementation Engineering (formerly RNIS)**

  The Data Network Implementation Engineering team implements and/or upgrades existing or new data networks. This team analyzes the customer’s network design requirements and performance expectations, and then creates the hardware and software installation specification used to implement data devices including Cajun, VPN, Wireless LAN, Secure Gateways, Extreme, and multi-vendor data equipment.

The CSI Group provides support on a contract basis. You can purchase various implementation offers from the CSI Group in Tampa, Florida. See Table 1: Customer-Accessible Resources on page 16 for contact information.

Avaya Technical Service Organization (TSO)

The Avaya Technical Service Organization (TSO) provides support to the Avaya Integrated Management 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 provide remote access.
- Customers do not have a current maintenance agreement.
- Customers do not procure and install the required systems and software as defined in the Integrated Management 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 Avaya Network Management Software Systems Support (NMSSS) group in Tampa Bay, Florida answers customer calls about applications in Avaya Integrated Management. NMSSS will either answer your questions directly or connect you with an associate who can answer questions about your application.

Customized Management Solutions for Avaya Integrated Management

The Integrated Management Product Team understands customer's needs and is focused on customer satisfaction. See Table 1: Customer-Accessible Resources on page 16 for contact information. The Product Team will assist customers with Avaya Integrated Management projects and will provide:

- **Project Management** — An Integrated Management project person will work with the customer to access configuration and customization requirements for any or all applications within each Avaya Integrated Management offer. If custom work is required, the evaluation will include a proposed statement of work and price. Note that this offer is *not* intended to provide installation for customers that choose to implement Integrated Management applications using Avaya Services or third-party implementation services.
- **Training** — Basic training can be performed remotely using an interactive medium to display the applications and a conference bridge for audio. On-site training can be customized to meet the customer's needs. Customized training will focus on application functionality that is relevant to the customer and provide focused knowledge transfer to facilitate application-specific training.

Avaya Contact Information

Table 1 and Table 2 provide contact information that you may use if you need assistance during the process of installing and setting up Avaya Integrated Management. To access the links in Table 2, you must be able to access the Avaya intranet.

Table 1: Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://www.avaya.com/support
Network Management Software Systems Support (NMSSS)	+1 800 237-0016
Communications, Solutions, and Integration (CSI) Group of Software Services	+1 800 730-9108, prompt 3
Integrated Management Product Team	Send email to: AIMtraining@avaya.com
Toll Fraud Intervention	+1 800 643-2353, prompt 1

Table 2: Avaya Internal Resources

Resource	Contact Information
Avaya System Management Support	http://aem-support.dr.avaya.com
Avaya Technology and Consulting (ATAC)	+1 888 297-4700, prompt 2,6 http://forum.avaya.com (requires a password)
Communications, Solutions, and Integration (CSI) Group of Software Services	http://associate2.avaya.com/sales_market/products/data-implementation-services/
Integrated Management Services Support Plan	http://associate2.avaya.com/solution/support_plans/#Enterprise

Third-Party Resources

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

Table 3: Vendor web sites

Vendor	Web Sites
Microsoft	Main site: http://www.microsoft.com
Red Hat Linux	Main site: http://www.redhat.com

System Security Notices

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

Network Security

Fault and Performance Manager uses the standard security features on the Red Hat Linux.

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

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

Toll Fraud Security

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

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

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

Avaya Disclaimer

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

Toll Fraud Intervention

If customers suspect that they are a victims of toll fraud and need technical assistance, they should refer to the phone number listed in Customer-Accessible Resources on page 16.

Chapter 2: Overview

Avaya Fault and Performance Manager (Fault and Performance Manager or FPM), Avaya Proxy Agent (Proxy Agent or PA), and Avaya Communication Manager Sub-Agent (Sub Agent or CMSA) provide a complete solution to fault and performance management of Avaya voice elements in both stand-alone mode and in NMS integrated mode.

FPM, PA, and CMSA work with the Integrated Management Database (IMD) to keep information together for all Integrated Management applications, to simplify data collection, to simplify data update, and to ensure database consistency.

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

Product Description

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 DEFINITY Proxy Agent or directly from an IP enabled voice system using OSSI, 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 provides the following views of the managed nodes in your network:
  - System Groups, which 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.
  - DCS Trunk Connectivity, which shows the DCS connectivity between the selected nodes.
  - IP Trunk Connectivity, which shows the IP trunk connectivity between the selected nodes.
  - Clusters, which shows the ESS clusters and LSP clusters.
- **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 filtering** -- You specify the filters for exceptions from each supported system. Filters can be configured based on any combination of the following parameters: Severity, Category, Maintenance Object Type and/or Maintenance Object Location. Additionally, you can configure filters to perform any combination of the following actions: Email, Trap, Alert, and/or ARS Script.
  - **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 3.0 supports both SNMP V1 and V2c get and set requests and SNMP V1 alarm traps for the following systems:

- DEFINITY® ECS Releases 9.5 through 10.x
- Survivable Remote Processors (SRPs)
- Multipoint Conferencing Unit (MCU) Release 7.2
- Avaya G250, G350 and G700 Media Gateways
- Avaya Communication Manager (Linux) Release 2.1 and 3.0
- Avaya Communication Manager Release 9.5 through 11
- Converged Communications Server (CCS) Release 1.0 and later.
- Interactive Response (IR) Releases 1.0 through 1.2
- Modular Messaging Release 1.0 and later

Fault and Performance Manager treats SRPs and MCUs as Communication Manager Feature Servers.

Fault and Performance Manager Release 3.0 supports only alarm traps for the following systems:

- DEFINITY AUDIX® Releases 3.1 through 4.0
- INTUITY AUDIX® Release 5.1 (with or without the remote maintenance board)
- INTUITY™ AUDIX® on S8100 Media Server
- INTUITY™ AUDIX® LX Release 1.0 through 17.X
- Modular Messaging Release 1.0 and later
- Call Management System (CMS) R3V8.3 through R3V11
- S8100 Media Server INTUITY AUDIX
- INTUITY™ Interchange Release 5.1 through 5.4
- CONVERSANT® Release 7.0 through 9.0
- IA770 INTUITY AUDIX® Option for S8300 ICC Release 1.0 through 2.0

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 Integrated Management 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: Avaya Internal Resources on page 16.

Hardware Certification

Avaya requires that Fault and Performance Manager hardware must be Red Hat Enterprise Linux AS R3.0 certified or Red Hat Enterprise Linux ES 3.0 or 2.1 certified. For the Red Hat URL, see Third-Party Resources on page 17.

⚠ **CAUTION:**

Customers are solely responsible for upgrading their network platforms to meet the NMS platform requirements for Fault and Performance Manager Release 3.0.

Software

Fault and Performance Manager Release 3.0 operates on:

- Red Hat Enterprise Linux AS R3.0
- Red Hat Enterprise Linux ES R3.0
- Red Hat Enterprise Linux ES 2.1 (upgrades only)

The optional NMSI component runs on:

- Windows 2003 Server running HP OpenView 7.5
- Windows 2000 Server running HP OpenView 7.0.1 or 7.5
- Solaris 9.0 running HP OpenView 7.0.1 or 7.5

Configuration Overview

The configuration process will follow the basic steps listed below:

1. During the software installation, perform one of the following steps:
   - If Fault and Performance Manager runs with a Network Management System (NMS), complete the procedures in Configuring Fault and Performance Manager to Integrate with HP OpenView on page 25.
   - If Fault and Performance Manager runs “standalone,” complete the procedures in Configuring Fault and Performance Manager for Stand-Alone Operation on page 29.
2. Complete the procedures in Administering Alarm Notification Services on page 34.
3. If you will be using SNMP traps, complete the procedures in Configuring SNMP Traps on page 41.
4. If you will be running Fault and Performance Manager with an NMS, complete Executing Auto-Discovery on page 56.
5. If you want to use Fault and Performance Manager to collect data, create and save report definitions, and schedule reports, complete the procedures in Starting the Administrative User Interface on page 50.

Chapter 3: Configuring Fault and Performance Manager

This chapter explains how to configure Avaya Fault and Performance Manager during the software installation.

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

If you are installing the HP OpenView integrated version, go to Configuring Fault and Performance Manager to Integrate with HP OpenView on page 25.

Configuring Fault and Performance Manager to Integrate with HP OpenView

To use the NMSI portion of the offer, before beginning the following configuration process, you must have HP OpenView for Windows NT/2000 Version 7.0.1 or 7.5 installed and running. When installing over version 7.5, you must download and install *Update 1 for Integrated Management 3.0* which is available on the Avaya Support Web site.

Note:

To use the OpenView Web client, the user must properly install and configure an appropriate web server (Apache, IIS, etc.). HP OpenView documentation should be consulted for information on setting up the web server and using OpenView Web.

Note:

To setup HP OpenView for System View, select the following options from within OpenView:

- Map>Properties...>View> Show Connection Labels
- Map>Properties...>Status Propagation>
  Propagate Most Critical

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

After installing Fault and Performance Manager, complete the following steps:

1. Logon to the Linux system as *root*.
2. At the Linux prompt type **/usr/sbin/mfpmconfig** and press **ENTER**.

   The system displays an explanation of the reasons to enable (default) or disable SNMP Polling. Then, the system displays the current setting and the prompt:

   ```
   Do you want to reconfigure the Avaya Fault and Performance Manager
   3.0 software [yes]?
   ```
3. Type **yes** and press **ENTER**.

   The system displays the prompt:

   ```
   Enter FPM server IP/FQDN: [ ]?
   ```
4. Type the IP address or fully qualified domain name (FQDN) of the FPM server, and press **ENTER**.

   The system displays the prompt:

   ```
   Shutting down FPM Server services:

   Configuring environment:

   Avaya Fault and Performance Manager provides for the capability of a
   distributed Data Collection Network of servers. This server is
   currently configured as a Primary data collection server. There may
   only be 1 Primary collection server in a network of FPM servers, and
   any number of Secondary data collection servers.

   Configure this server as the Primary Data Collection Server [yes]?
   ```
5. Type **yes** and press **ENTER**.

   The system displays the message:

   ```
   Avaya Fault and Performance Manager requires 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 command to represent the temporary filename
   created for printing purposes. If “%print” does not appear here, the
   filename will be appended to the print command.

   Please enter a default print command to be used by the FPM
   applications

   Enter printer command [ ]?
   ```

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

   The system displays the message:

   ```
   Avaya Fault and Performance Manager has been configured as a Primary
   Data Collection Server.

   Enter the FQDN of this server to be used by the Integrated
   Management Database to locate this FPM application server

   Enter the FQDN for FPM-computername [fqdn of computer]?
   ```

7. Type the FQDN, and press **ENTER**.

   The system displays the message:

   ```
   Avaya Fault and Performance Manager 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 Avaya Fault and Performance
   Manager documentation for more information about the OpenView NMS
   Integration.

   Do you want to integrate FPM with an HPOV System [yes]?
   ```

8. Type **yes** and press **ENTER**.

   The system displays the message:

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

   Enter the HPOV Server IP Address [ ]?
   ```

9. Type the IP address of the HPOV server, and press **ENTER**.

   The system displays the message:

   ```
   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 OpenView map, that map
   name needs to be entered here. If you are not sure just accept the
   default setting.

   Enter the HPOV Server Map Name [default]?
   ```

10. Press **ENTER**.

    The system displays the following messages:

    ```
    IMDAddApp Info: FPM successfully updated in IMD
    Configuring FPM Java Environment...
    Configuring FPM NMSI Environment...
    Modifying FPM Properties in Web Client JAR file...
    Building environment file...
    Platform configuration complete.
    Starting FPM Server services: [OK]
    ```

    Once FPM is configured for HP OpenView, the system displays the following message:

    ```
    Avaya Fault and Performance Manager software configuration was
    successful.
    ```

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.

After installing Fault and Performance Manager, complete the following steps:

1. Logon to the Linux system as *root*.
2. At the Linux prompt type **/usr/sbin/mfpmconfig** and press **ENTER**.

   The system displays an explanation of the reasons to enable (default) or disable SNMP Polling. Then, the system displays the current setting and the prompt:

   ```
   Do you want to reconfigure the Avaya Fault and Performance Manager
   3.0 software [yes]?
   ```
3. Type **yes** and press **ENTER**.

   The system displays the prompt:

   ```
   Enter FPM server IP/FQDN: [ ]?
   ```
4. Type the IP address or fully qualified domain name (FQDN) of the FPM server, and press **ENTER**.

   The system displays the prompt:

   ```
   Shutting down FPM Server services:

   Configuring environment:

   Avaya Fault and Performance Manager provides for the capability of a
   distributed Data Collection Network of servers. This server is
   currently configured as a Primary data collection server. There may
   only be 1 Primary collection server in a network of FPM servers, and
   any number of Secondary data collection servers.

   Configure this server as the Primary Data Collection Server [yes]?
   ```
5. Type **yes** and press **ENTER**.

   The system displays the message:

   ```
   Avaya Fault and Performance Manager requires 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 command to represent the temporary filename
   created for printing purposes. If “%print” does not appear here, the
   filename will be appended to the print command.
   ```

```
Please enter a default print command to be used by the FPM
applications
```

```
Enter printer command [ ]?
```

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

   The system displays the message:

   ```
   Avaya Fault and Performance Manager 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 Avaya Fault and Performance
   Manager documentation for more information about the OpenView NMS
   Integration.
   ```

   ```
   Do you want to integrate FPM with an HPOV System [yes]?
   ```

7. Type **no** and press **ENTER**.

   The system displays the following messages:

   ```
   IMDAddApp Info: FPM successfully updated in IMD
   ```

   ```
   Configuring FPM Java Environment...
   ```

   ```
   Configuring FPM NMSI Environment...
   ```

   ```
   Modifying FPM Properties in Web Client JAR file...
   ```

   ```
   Building environment file...
   ```

   ```
   Platform configuration complete.
   ```

   ```
   Starting FPM Server services: [OK]
   ```

   Once FPM is configured, the system displays the following message:

   ```
   Avaya Fault and Performance Manager software configuration was
   successful.
   ```

Chapter 4: Customizing Fault and Performance Manager

Introduction

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

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

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

Setting up Communication Manager Sub Agent

For instructions on setting up the Avaya Sub Agent on your Communication Manager, see the Administrator’s Guide for Avaya Communication Manager, 555-233-506, Issue 7. The section is titled, “SNMP Agents” in Chapter 17, “Administering Media Servers.”

System Commands

Start and Stop Commands

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

Table 4: Start and Stop commands

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

System administrators can view a log of system startups and shutdowns from /var/avaya/mfpm/logs/MsgLog_[0-30]. The default number of MsgLog files is 30. You can change this value.

System Health Commands

The table below contains the system health commands.

Table 5: System Health commands

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

Backing up the FPM Database

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

You can 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

Please refer to the Linux backup procedure in the *Avaya Integrated Management Release 3.0 System Management Installation and Upgrade*.

Restoring the FPM Database

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

You can 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

Please refer to the Linux restore procedure in the *Avaya Integrated Management Release 3.0 System Management Installation and Upgrade*.

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 /opt/avaya/mfpm/bin directory contains the sample scripts listed below:

- DEFINITY_ARS
- AUDIX_ARS
- CMS_ARS
- CONVERSANT_ARS

Alarm notification options

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

- Vytek, TeleAlert
- Remedy, Action Request System (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 specified address that contains detailed information for the alarm, alert, or error received from the managed system. Individual email addresses can be set by voice system and by type of alert.

TeleAlert options

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

Table 7: Vytek notification options

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

Peregrine option

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

Table 8: Peregrine notification option

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

DEFINITY_ARS Script

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

- FPM receives an alarm trap from the managed nodes listed below:
  - Communication Manager Feature Servers
  - MCU
- FPM receives an exception event from Fault and Performance Manager for these managed nodes

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

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

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

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

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

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

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

Alarm notification values:

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

CONVERSANT_ARS Script

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

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

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

Chapter 5: Configuring SNMP Traps

Communication Manager 3.0 provides a method for sending traps to Avaya Fault and Performance Manager. This chapter describes how to configure traps to be send to FPM.

Recommended Software Requirements

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

- Avaya Integrated Management Release 3.0
- Avaya Communication Manager Release 3.0

Configuration Procedures

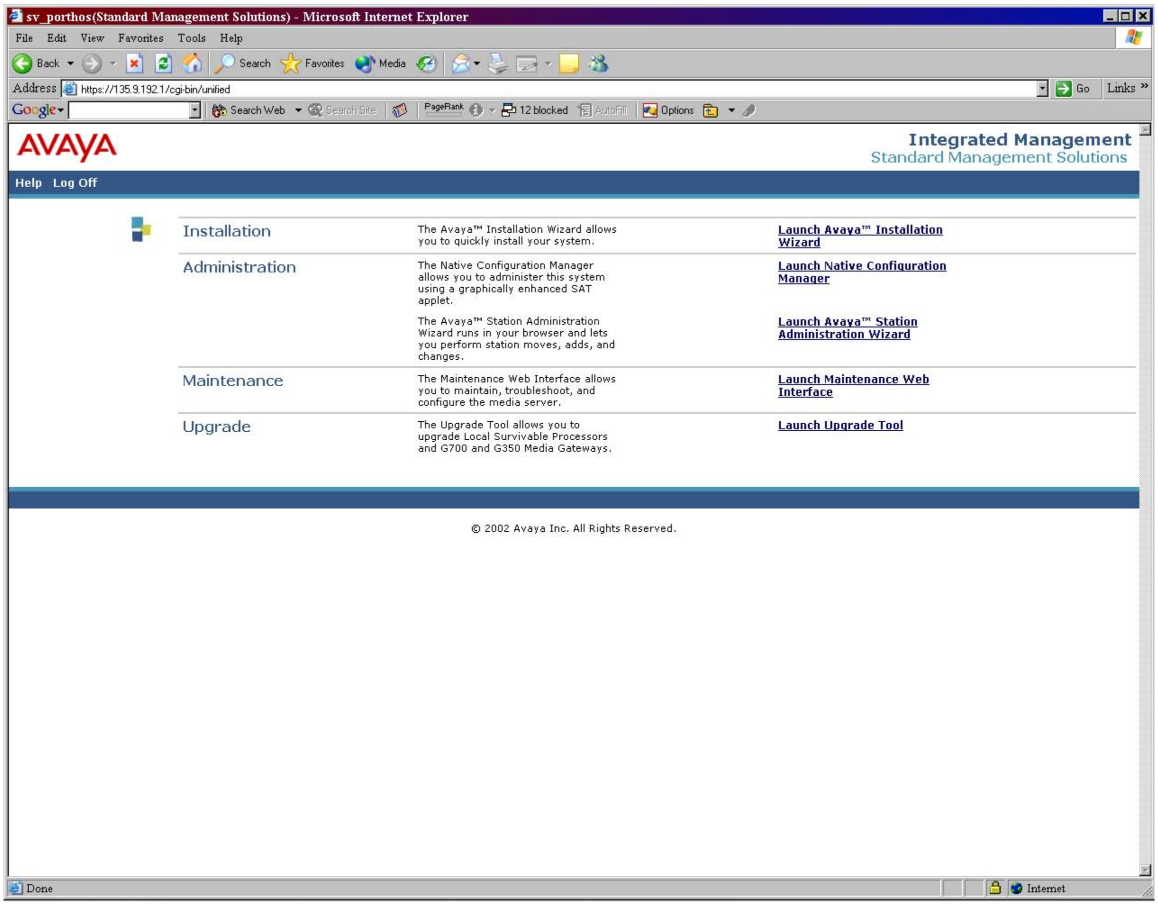
To configure traps for FPM, you must perform the following procedures:

1. Launch the Maintenance web interface (Procedure 1: Launch the Maintenance Web Interface on page 42).
2. Configure trap destinations (Procedure 2: Configure Trap Destinations on page 43).
3. Add nodes (for example, voice systems and adjuncts) you want to manage.

Procedure 1: Launch the Maintenance Web Interface

To launch the Maintenance web interface:

1. From the Integrated Management Standard Management Solutions page, click **Launch Maintenance Web Interface**.


sv_porthos(Standard Management Solutions) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://135.9.192.1/cgi-bin/unified
Go Links
Google Search Web Search Site PageRank 12 blocked AutoFill Options
AVAYA
Help Log Off
Done
Internet

Integrated Management
Standard Management Solutions

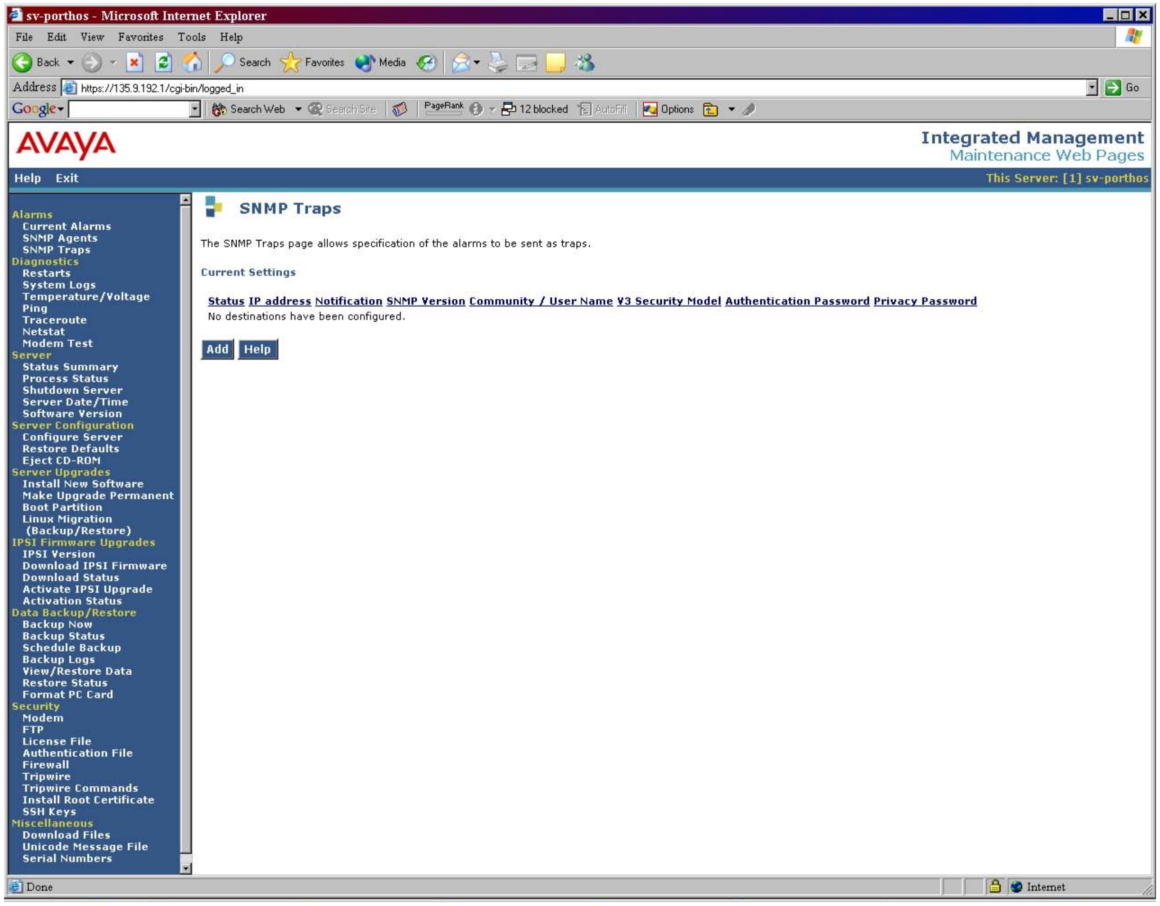
Installation	The Avaya™ Installation Wizard allows you to quickly install your system.	Launch Avaya™ Installation Wizard
Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
	The Avaya™ Station Administration Wizard runs in your browser and lets you perform station moves, adds, and changes.	Launch Avaya™ Station Administration Wizard
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade Local Survivable Processors and G700 and G350 Media Gateways.	Launch Upgrade Tool

© 2002 Avaya Inc. All Rights Reserved.

Procedure 2: Configure Trap Destinations

To configure trap destinations:

1. From the Alarms heading located on the navigation frame, click **SNMP Traps**. The SNMP Traps screen appears.



SNMP Traps

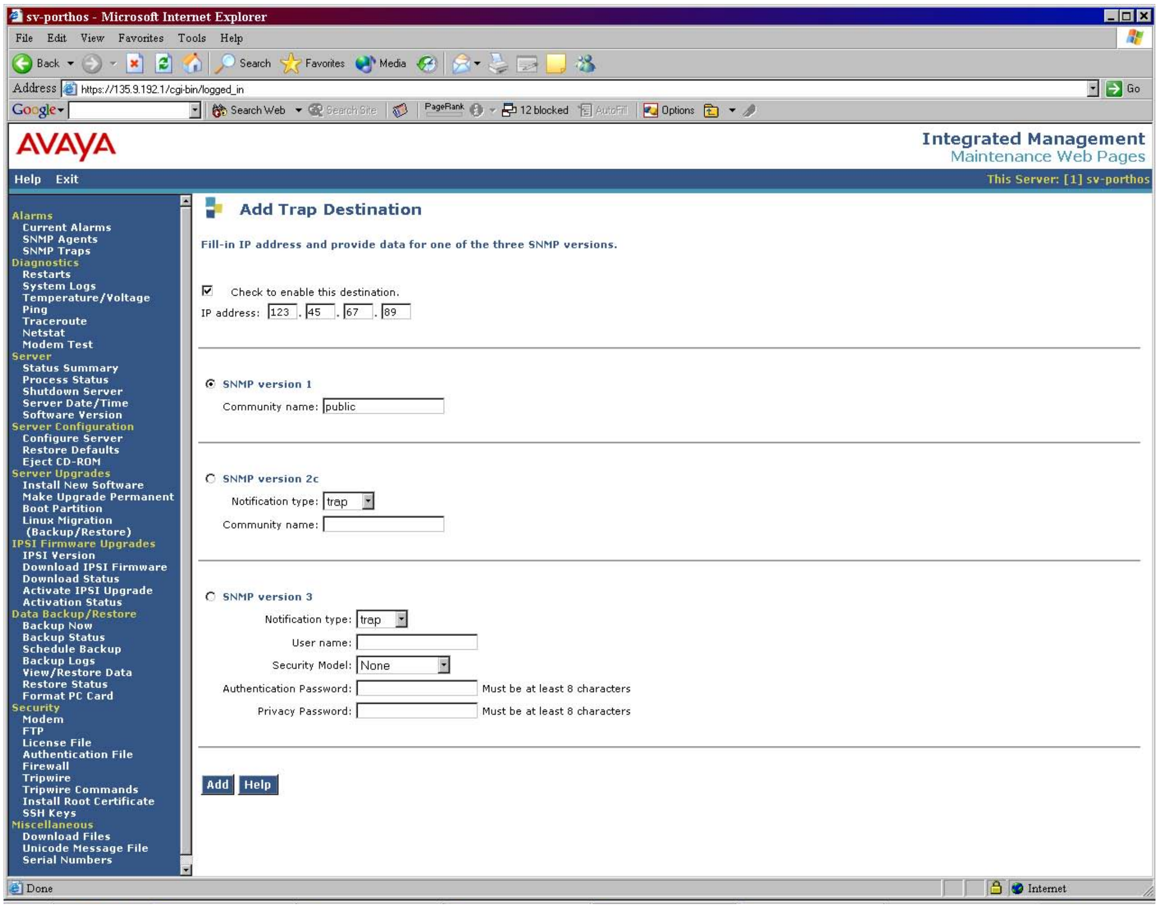
The SNMP Traps page allows specification of the alarms to be sent as traps.

Current Settings

Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password

No destinations have been configured.

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



Add Trap Destination

Fill-in IP address and provide data for one of the three SNMP versions.

☑ Check to enable this destination.

IP address: 123 . 45 . 67 . 89

● SNMP version 1

Community name: public

○ SNMP version 2c

Notification type: trap

Community name:

○ SNMP version 3

Notification type: trap

User name:

Security Model: None

Authentication Password: Must be at least 8 characters

Privacy Password: Must be at least 8 characters

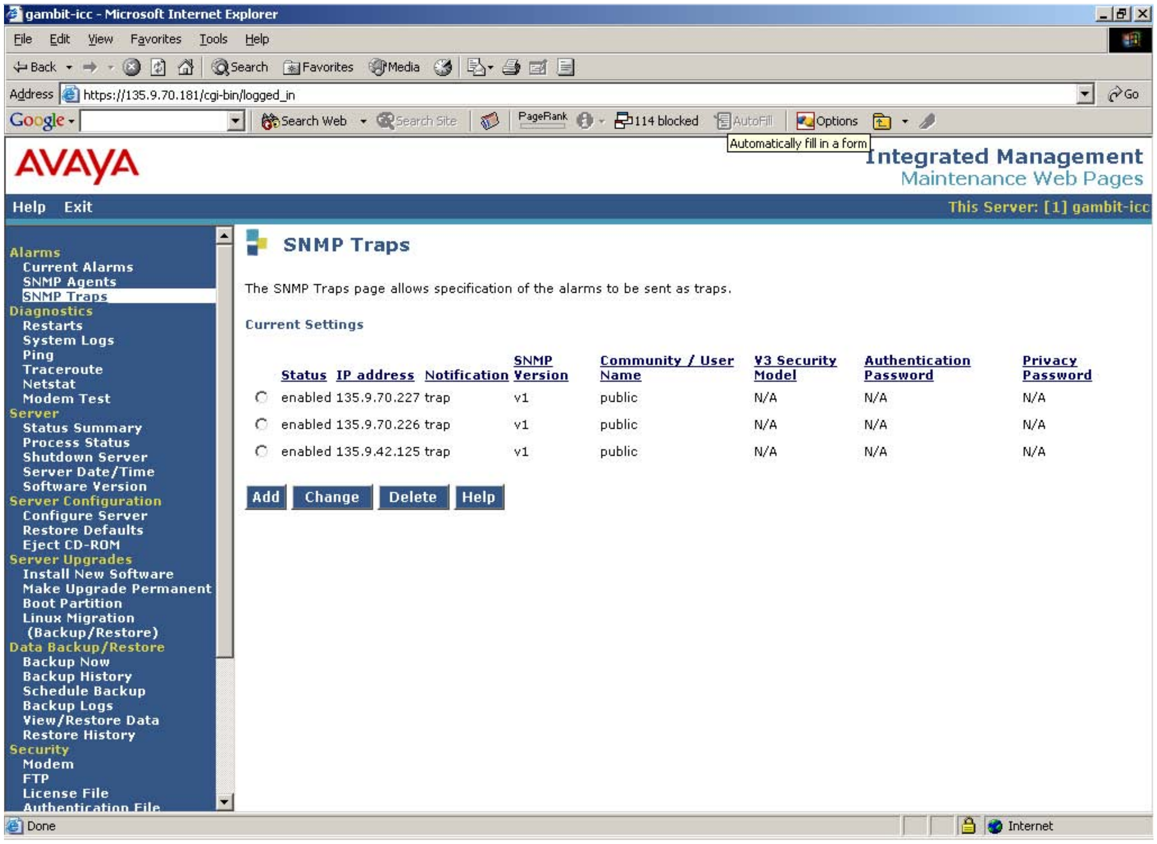
Add Help

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

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

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

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



SNMP Traps

The SNMP Traps page allows specification of the alarms to be sent as traps.

Current Settings

	Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password
○	enabled	135.9.70.227	trap	v1	public	N/A	N/A	N/A
○	enabled	135.9.70.226	trap	v1	public	N/A	N/A	N/A
○	enabled	135.9.42.125	trap	v1	public	N/A	N/A	N/A

Add Change Delete Help

Note:

We do not recommend configuring multiple FPM systems as a method of disaster recovery.

If you want to add nodes that you want to manage, go to Procedure 3: Add Nodes on page 45.

Procedure 3: Add Nodes

To add nodes (for example, voices systems and adjuncts) that you want to manage, you must use the Integrated Management Database (IMD). See the *Avaya Integration Management Database Release 3.0 Configuration* or the Integrated Management Database online help for information on how to add nodes.

Chapter 6: Getting Started

In this chapter you will learn about the following windows and processes:

- Creating logins and assigning roles for FPM users
- 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
- Changing your FPM password
- NMS maps
- Map commands
- Online Help system

Creating FPM Logins and Roles

Users must log into FPM before they can use the FPM user interface. You must use Integrated Management Database (IMD) to

- create FPM roles
- add FPM users
- assign FPM roles to the FPM users

You can set each FPM role to have one or more of the following capabilities:

- **Administration** (Admin)

  Allows the user to access the FPM Administration menu item for the scheduling of data collection and reports, system groups, and trunk group lists from the FPM user interface.

- **BusyoutRelease**

  Allows the user to Busy/Release boards, trunks, trunk groups, stations, and ports from the FPM user interface.

- **Acknowledge**

  Allows the user to acknowledge alerts within the FPM user interface.

- **ReadOnly**

  Allows the user to run the FPM user interface with a read-only permission, where nothing can be done to voice systems, reports, or scheduling.

- **CreateReports**

  Allows the user to

  - create new reports that will be stored on the FPM server for future use
  - schedule reports to be run automatically in the background by the FPM server

To create FPM roles and logins, perform the following procedures:

1. Create FPM roles.
2. Add FPM users.
3. Assign FPM roles to the FPM users.

Procedure 1: Create FPM Roles

To create FPM roles, perform the following steps:

1. Log into Integrated Management Database (IMD), and click **FPM Roles** in the navigation panel of the Integrated Management Database Administrator page.

   The FPM Roles page appears.

2. Click **Add**.

   The Add FPM Role page appears.

3. In the Enter Role Name box, enter the name for the FPM role.
4. In the Available Capabilities list box, select the capability you want to assign to this role. If you want to assign multiple capabilities to this role, press and hold down the **Ctrl** key on your keyboard and click on each capability you want to select.
5. Click **Select**.

   The selected capabilities appear in the Capabilities assigned to this role list box.

6. Click **Add**.

   A page appears confirming that the role was added successfully.

7. Click **OK**.
8. Repeat Steps 2 through 7 for each FPM role you want to create.

When finished, go to Procedure 2: Add User on page 49.

Procedure 2: Add User

Use this procedure to add a user account that can access FPM. If the user was added to Integrated Management Database (IMD) previously, go to Procedure 3: Assign FPM Roles to Users on page 49 to assign an FPM role to this user.

To add a user, perform the following steps:

1. Click **Users** in the navigation panel of the Integrated Management Database Administrator page.

   The Users page appears.

2. Click **New User**.

   The Add User page appears.

3. In the Login box, enter the login for the user.
4. In the User Name box, enter the name of the user.
5. In the Email Address box, enter the email address of the user.
6. In the Phone Number box, enter the telephone number of the user.
7. In the Password box, enter the password for the user’s login.
8. In the Re-type Password box, re-enter the password for the user’s login.
9. Select the **FPM** check box.
10. Click **Add**.
11. Repeat Steps 2 through 10 for any other users you want to add.

When finished, go to Procedure 3: Assign FPM Roles to Users on page 49.

Procedure 3: Assign FPM Roles to Users

Use this procedure to assign FPM roles to users. You can assign multiple FPM roles to a user.

Note:

Make sure you have created an FPM role already.

To assign an FPM role to a user:

1. Click **Users** in the navigation panel of the Integrated Management Database Administrator page.

   The Users page appears.

2. Click **Edit** for the user to which you want to assign an FPM role.

   The Edit User page appears.

3. Select the **FPM** check box (if it is not selected already).

   The Assign Roles link appears next to the FPM check box.
4. Click **Assign Roles**.

   The Assign FPM Roles to a User window appears.
5. Select the check box of each role you want to assign to this user.
6. Click **Save**.

   A page appears confirming that the role was updated successfully.
7. Click **OK**.
8. Click **Update**.
9. Repeat Steps 2 through 8 for each user to which you want to assign an FPM role.

When you want to exit IMD, click **Exit** in the navigation panel.

Starting the Administrative User Interface

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

Procedure

From the FPM server, complete the following procedure:

1. At the login prompt, type **root** and press **ENTER.**
2. At the password prompt, type the root password and press **ENTER.**
3. Open a terminal window.

   The system displays the Linux prompt.
4. Type: **cd /opt/avaya/mfpm/bin/** and press **ENTER**.
5. 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 Communication Manager Feature Servers registered in Fault and Performance Manager. Optionally, add the voice system name at the end of the command for the Communication Manager Feature Server Exception Report for a specific voice system.

Starting the Fault and Performance Manager Client from a Web Browser

When you start the Fault and Performance Manager client from a web browser, you can only view; you can not make changes. You can start the client from a browser only if the browser meets the requirements specified in the Integrated Management 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 Integrated Management Launch Products page.
3. Click the **System Management** tab on the Integrated Management web page.
4. Click **Avaya Fault and Performance Manager**.

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

   The FPM Login dialog box appears.
6. In the Login Name box, enter your login. (All FPM logins and passwords are administered through the Integrated Management Database (IMD).)
7. In the Password box, enter your password.
8. Click **Login**.

   The Fault and Performance Manager window appears.

Starting the Online Help

The online help system describes how to use Fault and Performance Manager. To start the online help with Fault and Performance Manager open, choose **Help>Help Topics or Help>Current Panel**.

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**.

Changing Your FPM Password

Use this procedure to change your password for Fault and Performance Manager. To change your Fault and Performance Manager password, complete the following steps:

1. Using Microsoft Internet Explorer 6.0 or later, go to the IP address or hostname of the Linux server to view the Avaya Integrated Management Launch Products page.
2. On the System Management tab, click **Avaya Integrated Management Database**.

   The Logon window appears.
3. Click **Change Password**.

   The Change Password page appears.
4. In the User ID box, enter your Fault and Performance Manager login.
5. In the Current Password box, enter the current password for your login.
6. In the New Password box, enter the new password you want to use for your login.
7. In the Re-Type New Password box, re-enter the new password you want to use for your login.
8. Click **Change Password**.
9. Click **Cancel** to return to the Logon page.

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 or on Solaris 9.0. After installing the client, you must run mfpmconfig again to configure the HP OpenView server config service TCP port number.

Understanding the NMS Maps

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

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

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

NMS maps

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

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

- NMS Root map
- Avaya Fault and Performance Manager submap
- Avaya USA and state submaps
- Avaya 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) named “default” is the initial user interface to the various Avaya submaps mentioned in the previous section.

NMSI places “explodeable” icons representing the various Avaya submaps on the root map. The Avaya submap icons lead to submaps that contain Proxy Agents and Managed Nodes that have been administered by the user in FPM.

The icon names that display on the root map are:

- Avaya MAP identifies a Generic submap.
- Avaya USA MAP identifies the USA map and associated state submaps.
- Avaya custom submaps will be automatically be defined based on information provided by the user in Proxy Agent or IMD.

Proxy Agent icon colors

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

Table 9: Proxy Agent Icon colors

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

Fault and Performance Manager icon colors

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

- Communication Manager Feature Server
- Multipoint Conferencing Unit (MCU)
- Adjuncts and voice messaging systems

Fault and Performance Manager treats the MCUs as Communication Manager Feature Servers.

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

Table 10: Communication Manager Server icon colors

Object	HP OpenView Color
Communication Manager Feature Server icon	**Dark Blue** = Unknown. Proxy Agent is not responding **Green** = Normal **Cyan** = Warning **Yellow** = Minor **Orange** = Major **Red** = Critical
Line connections to Communication Manager Feature Server icons	**Black** = Up **Red** = Down or Other **Yellow** = Init (initiating) **Cyan** = Off **Salmon** = 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 5.1 (with or without the remote maintenance board)
- Intuity Interchange release 5.1 through 5.4
- Call Management System (CMS) R3V8.3 through R3V11
- CONVERSANT release 7.0 through 9.0
- IA770 INTUITY AUDIX Release 1.0
- S8100 Media Server INTUITY AUDIX
- IA770 INTUITY AUDIX® Option for S8300 ICC Release 1.0 through 2.0
- INTUITY™ AUDIX® on S8100 Media Server
- INTUITY™ AUDIX® LX Release 1.0 through 17.X
- Modular Messaging Release 1.0 and later
- Converged Communications Server (CCS) Release 1.0 and later.
- Interactive Response (IR) Releases 1.0 through 1.2

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

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

Table 11: Other system icon colors

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

Executing Auto-Discovery

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

Auto-Discovery is a feature of your NMS that automatically gathers information about the managed nodes (voice elements) in your telecommunications system, and presents that information graphically using icons and maps.

To execute Auto-Discovery:

From the HP OpenView server, click **Avaya>System View>Rediscover Entire Map**.

Note:

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

Executing Commands from NMS Maps

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

Users can execute the commands in two ways:

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

Some of the Avaya commands and applications are not available on a Solaris server.

The sections below explain the commands and the execution options.

Description of Commands

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

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

MultiSite Administration, Avaya Site Administration, Voice Announcement Manager, Avaya Terminal Configuration, VMON, Proxy Status, Proxy Cache Status, Proxy Incoming AlarmLog, Fault Performance Manager, FPM Report Manager, FPM Exception Report, Telnet to Managed Node, Telnet to Proxy Agent, FPM Sever Status, FPM Server Collection Status, Integrated Management Web Page, and Communication Manager Web Page applications and commands can also be launched from the HPOV default map, Avaya menu.

Table 12: NMS Map commands

Command	Description
Fault and Performance Manager	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 Communication Manager Feature Server on the NMS map, then the command opens the main window with focus on the selected Communication Manager Feature Server.
FPM Report Manager	This command displays the Report Manager window of the Fault and Performance Manager.
	1 of 4

Table 12: NMS Map commands (continued)

Command	Description
FPM Exception Report	This command displays the results of a Fault and Performance Manager Exception report. You can only execute this command for a specific Communication Manager Feature Server on the map. The report shows exceptions only for the selected Communication Manager Feature Server.
Rediscover Entire Map	The Rediscover Entire Map process is primarily driven by the Fault and Performance Manager database and collection process. The database is used because not all Avaya products that Fault and Performance Manager deals with are IP based. Therefore, the Rediscover Entire Map process will place icons on one of the submaps and show connectivity between that device and others without regard to whether HP OpenView can discover that device. This command may run automatically on start-up of any HPOV console window. During the Rediscover Entire Map process, the text message “synchronizing” is shown at the bottom left of the HP OpenView GUI. (This is also true for other System View commands.) At the end of the Rediscover Entire Map process, this text message disappears to denote that the command has completed. The time needed to perform a Rediscover Entire Map depends primarily on the size of your network. For the Rediscover Entire Map command to run, the following conditions must be met: ● The FPM server must be operational. ● HP OpenView must have a Read-Write map open. ● A connection must be established between HP Open View and the Fault and Performance Manager server process, NmsiServer. If any R/O maps are displayed when a Rediscover Entire Map is requested from the R/W map, the R/O maps will not be immediately updated. The user must do a Map> Refresh from each R/O map to bring it into sync with the R/W map. Doing the Map>Refresh will close any open R/O submaps and take the user to the top level of that R/O map. The only exception to this rule is with regard to status updates which are done immediately across all maps and do not require the manual refresh.
	2 of 4

Table 12: NMS Map commands (continued)

Command	Description
Re-register with Server	The Re-register with Server establishes a connection between the Fault and Performance Manager server and HP OpenView. A Re-register with Server is done automatically when the HP OpenView GUI is started. The NMSI code always attempts to keep its Avaya maps of Managed Nodes synchronized with the data received from FPM. The NMSI code automatically adds Managed Nodes to its maps when it receives status for newly added nodes from FPM. You can run the Re-register with Server command even if a session already exists; this does not cause problems. In fact, running the Re-register with Server command is the simplest way to verify that a connection exists between HP OpenView and the Fault and Performance Manager server. If a connection cannot be established, an error message pops up on the screen.
Cleanup DB	The Cleanup DB command removes objects created by the Refresh Entire Map command, as long as the object has no associated symbol.
Telnet to Proxy Agent	This command displays the telnet window to Proxy Agent. From the telnet window, users can log in to Proxy Agent and initiate an emulation session to cut-through to the managed node.
Telnet to Managed Node	This command is for IP-connected nodes. Users can telnet directly to the node rather than going through Proxy Agent.
Update System View Status	This command retrieves and updates the current status of the Managed Nodes in the NMS. This command may run automatically on start-up of any HPOV console window.
Update Managed Node Status	For each Voice System and/or Adjunct that is selected on the NMS map, this command retrieves and updates the current status of the Voice System/Adjunct. You can select one or more voice systems/adjuncts with this command.
Proxy Status	This command retrieves and updates the current status of proxy agents.
Proxy Cache Status	This command retrieves and updates the current status of the cache for proxy agents.
	3 of 4

Table 12: NMS Map commands (continued)

Command	Description
Proxy Incoming Alarm	This command retrieves and updates the current status of incoming alarms for proxy agents.
FPM Server Status	This command retrieves and updates the current status of the FPM server.
FPM Server Collection Status	This command retrieves and updates the current status of FPM collection activities.
Integrated Management Web Page	This command displays the Integrated Management home page.
Communication Manager Web Page	This command displays the Communication Manager home page.
	4 of 4

Exiting the Fault and Performance Manager Client from the Linux Server

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

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

   The system exits the product and displays the Root map.

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

   The system displays the Linux login prompt.

Glossary and Abbreviations

A

ATAC See Avaya Technology and Consulting (ATAC) on page 13.

C

Communication Manager The call processing software that runs on Communication Manager Feature Servers. Formerly known as DEFINITY software.

Communication Manager Feature Server Any of the products that run Communication Manager. Formerly known as DEFINITY system, DEFINITY ECS, switch, PBX, or voice system.

CSI See Communications, Solutions, and Integration (CSI) Group of Software Services on page 13.

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 Configuration and Proxy Agent.

N

Network Management Server This is the Windows or Solaris box that you can install Integrated 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.

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 21.

SNMP Simple Network Management Protocol.

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

T

TSO See Avaya Technical Service Organization (TSO) on page 14.

Index