



**Avaya Integrated Management  
Release 3.1  
Fault and Performance Manager  
Configuration**

555-233-138  
Issue 8  
February 2006

© 2006 Avaya Inc.  
All Rights Reserved.

#### **Notice**

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

**For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.**

**To locate this document on the website, simply go to <http://www.avaya.com/support> and search for the document number in the search box.**

#### **Documentation disclaimer**

Avaya Inc. 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.

#### **Link disclaimer**

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

#### **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>

#### **Copyright**

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

#### **Avaya support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

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

# 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
Product Documentation . . . . .	8
How to Access Books on the Web . . . . .	9
<b>Chapter 1: Resources and Notices.</b> . . . . .	<b>11</b>
Avaya Technology and Consulting (ATAC). . . . .	11
Communications, Solutions, and Integration (CSI) Group of Software Services . . . . .	11
Avaya Technical Service Organization (TSO) . . . . .	12
Avaya Network Management Software Systems Support Group (NMSSS) . . . . .	12
Customized Management Solutions for Avaya Integrated Management. . . . .	13
Avaya Contact Information . . . . .	14
Third-Party Resources . . . . .	15
System Security Notices . . . . .	15
Network Security. . . . .	15
Toll Fraud Security . . . . .	16
Avaya Disclaimer . . . . .	16
Toll Fraud Intervention . . . . .	16
<b>Chapter 2: Overview.</b> . . . . .	<b>17</b>
Product Description . . . . .	17
What's New in this Release . . . . .	19
Supported Systems . . . . .	20
System Requirements . . . . .	21
Hardware . . . . .	21
Hardware Certification. . . . .	21
Software . . . . .	21
Configuration Overview . . . . .	22

<b>Chapter 3: Configuring Fault and Performance Manager. . . . .</b>	<b>23</b>
Configuring Fault and Performance Manager to Integrate with HP OpenView . . . . .	23
Configuring Fault and Performance Manager for Stand-Alone Operation. . . . .	26
<b>Chapter 4: Customizing Fault and Performance Manager . . . . .</b>	<b>29</b>
Introduction . . . . .	29
Setting up Communication Manager Sub Agent . . . . .	29
System Commands . . . . .	30
Start and Stop Commands . . . . .	30
System Health Commands . . . . .	31
Backing up the FPM Database . . . . .	31
Required materials. . . . .	31
Procedure . . . . .	31
Restoring the FPM Database . . . . .	32
Required materials. . . . .	32
Procedure . . . . .	32
Administering Alarm Notification Services . . . . .	32
Script directories. . . . .	32
Alarm notification options. . . . .	33
Description of Alarm Notification Options. . . . .	33
Fault and Performance Manager options . . . . .	33
TeleAlert options. . . . .	34
Peregrine option . . . . .	34
DEFINITY_ARS Script . . . . .	35
AUDIX_ARS Script. . . . .	36
CMS_ARS Script. . . . .	37
CONVERSANT_ARS Script . . . . .	38
<b>Chapter 5: Configuring SNMP Traps . . . . .</b>	<b>39</b>
Recommended Software Requirements . . . . .	39
Configuration Procedures. . . . .	39
Procedure 1: Launch the Maintenance Web Interface . . . . .	40
Procedure 2: Stop the Master Agent . . . . .	42
Procedure 3: Configure SNMP Agent . . . . .	43
Procedure 4: Start the Master Agent . . . . .	45
Procedure 5: Add Nodes . . . . .	46
Testing the SNMP Agent . . . . .	46

<b>Chapter 6: Getting Started</b> . . . . .	<b>53</b>
<b>Creating FPM Logins and Roles</b> . . . . .	<b>53</b>
<b>Procedure 1: Create FPM Roles</b> . . . . .	<b>54</b>
<b>Procedure 2: Add User</b> . . . . .	<b>55</b>
<b>Procedure 3: Assign FPM Roles to Users</b> . . . . .	<b>56</b>
<b>Starting the Administrative User Interface</b> . . . . .	<b>57</b>
<b>Procedure</b> . . . . .	<b>57</b>
<b>Starting the Fault and Performance Manager</b>	
<b>Client from a Web Browser</b> . . . . .	<b>58</b>
<b>Procedure</b> . . . . .	<b>58</b>
<b>Configuring Alarm Filters</b> . . . . .	<b>59</b>
<b>Starting the Online Help</b> . . . . .	<b>62</b>
<b>Exiting the Fault and Performance Manager</b>	
<b>Client from a Web Browser</b> . . . . .	<b>63</b>
<b>Changing Your FPM Password</b> . . . . .	<b>63</b>
<b>Fault and Performance Manager Integration with NMS</b> . . . . .	<b>64</b>
<b>Understanding the NMS Maps</b> . . . . .	<b>64</b>
<b>NMS maps</b> . . . . .	<b>64</b>
<b>Root Map</b> . . . . .	<b>64</b>
<b>Proxy Agent icon colors</b> . . . . .	<b>65</b>
<b>Fault and Performance Manager icon colors</b> . . . . .	<b>65</b>
<b>Other system icon colors</b> . . . . .	<b>66</b>
<b>Executing Auto-Discovery</b> . . . . .	<b>67</b>
<b>Executing Commands from NMS Maps</b> . . . . .	<b>68</b>
<b>Description of Commands</b> . . . . .	<b>68</b>
<b>Exiting the Fault and Performance Manager</b>	
<b>Client from the Linux Server</b> . . . . .	<b>71</b>
 <b>Glossary and Abbreviations</b> . . . . .	 <b>73</b>
 <b>Index</b> . . . . .	 <b>75</b>

## **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](mailto:document@avaya.com)

---

## Product Documentation

The latest version of Avaya Integrated Management product documentation, including this book, is available from the Avaya Support Web Site. To view or download these books from the Web, you must have access to the Internet, an Internet browser, and Adobe Acrobat Reader, version 5.0 or later. Adobe Acrobat Reader is provided on the Avaya Integrated Management CDs and is also available from <http://www.adobe.com>. See [How to Access Books on the Web](#) for instructions on how to view or download these books.

---

## How to Access Books on the Web

To view or download books from the Avaya Support Web Site, follow these steps:

1. Access <http://www.avaya.com/support>.
2. Click **Find Documentation and Downloads by Product Name**.
3. Click the letter **I** in the alphabet listing.
4. Locate the Integrated Management product or offer name and click the corresponding link.
5. Click **View All Documents** to display a list of available books for that product or offer.



# 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 14 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 14 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	<a href="http://www.avaya.com/support">http://www.avaya.com/support</a>
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	<a href="http://aem-support.dr.avaya.com">http://aem-support.dr.avaya.com</a>
Avaya Technology and Consulting (ATAC)	+1 888 297-4700, prompt 2,6 <a href="http://forum.avaya.com">http://forum.avaya.com</a> (requires a password)
Communications, Solutions, and Integration (CSI) Group of Software Services	<a href="http://associate2.avaya.com/sales_market/products/data-implementation-services/">http://associate2.avaya.com/sales_market/products/data-implementation-services/</a>
Integrated Management Services Support Plan	<a href="http://associate2.avaya.com/solution/support_plans/#Enterprise">http://associate2.avaya.com/solution/support_plans/#Enterprise</a>

---

## Third-Party Resources

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

**Table 3: Vendor web sites**

Vendor	Web Sites
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>

---

## 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 14.

## 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 OSSl, 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.

## Overview

- **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.

---

## What's New in this Release

Fault and Performance Manager Release 3.1 introduces the following enhancements:

- Support for the following media servers:
  - S8400 server
  - S8720 server
- Support for the following media modules:
  - G250-DCP media gateway
  - G250-DS1 media gateway
  - MM716 analog 24-port (line only) media module
  - HDMM 40-port Power over Ethernet media module
- Support for duplication of the TN2602AP board.
- The ability to collect local survivable processor (LSP) data and enterprise survivable server (ESS) data using the new "list survivable-server" command in Avaya Communication Manager Release 3.1.
- The ability for Avaya Fault and Performance Manager to access media gateways and other devices via a global default SNMP configuration.
- Support for the Avaya Voice Over IP (VoIP) Monitoring Manager server. FPM also provides the ability to launch Avaya VoIP Monitoring Manager web interface to get information about the selected IP phone or VoIP Monitoring Manager server.
- Support for the Message Networking adjunct. FPM also provides the ability to launch the Message Networking web interface for the selected Message Networking adjunct.
- Alarm enhancements:
  - Support for the new MIB traps definitions for alarmResolved, alarmMajor, alarmMinor, and alarmWarning.
  - The ability to collect and display three new alarm fields (g3alarmsIPAddress, g3alarmsCategory, and g3alarmsErrorCodes) in the Exceptions screen.
- Support for the Managed Security Services feature in Avaya Communication Manager Release 3.1.
- The Assist Engine, which enables you to automatically run the Avaya Communication Manager commands recommended by the Helpdesk feature when an alarm is received.
- The ability for FPM to alert you when the performance criterion you specify occurs.

## Supported Systems

Fault and Performance Manager Release 3.1 supports both SNMP V1 and V2c get and set requests and SNMP V1 alarm traps for the following systems:

- DEFINITY<sup>®</sup> ECS Releases 9.5 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, 3.0, and 3.1
- Avaya Communication Manager Release 9.5 through 11
- Avaya SIP Enablement Services (SES) Server Release 3.1 and Avaya Converged Communications Server (CCS) Release 1.0 and later
- Interactive Response (IR) Releases 1.0 through 1.3
- Modular Messaging Release 1.0 and later
- Message Networking 1.1 through 3.0

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

Fault and Performance Manager Release 3.1 supports only alarm traps for the following systems:

- DEFINITY AUDIX<sup>®</sup> Releases 3.1 through 4.0
- INTUITY AUDIX<sup>®</sup> Release 5.1 (with or without the remote maintenance board)
- INTUITY<sup>™</sup> AUDIX<sup>®</sup> on S8100 Media Server
- INTUITY<sup>™</sup> AUDIX<sup>®</sup> 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<sup>™</sup> Interchange Release 5.1 through 5.4
- CONVERSANT<sup>®</sup> Release 7.0 through 9.0
- IA770 INTUITY AUDIX<sup>®</sup> Option for S8300 ICC Release 1.0 through 2.0
- Message Networking Release 1.0 through 3.0

---

# 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 14.

## Hardware Certification

Avaya requires that Fault and Performance Manager hardware must be Red Hat Enterprise Linux AS R4.0 or 3.0 certified or Red Hat Enterprise Linux ES 4.0 or 3.0 certified. For the Red Hat URL, see [Third-Party Resources](#) on page 15.

 **CAUTION:**

Customers are solely responsible for upgrading their network platforms to meet the NMS platform requirements for Fault and Performance Manager Release 3.1.

## Software

Fault and Performance Manager Release 3.1 operates on:

- Red Hat Enterprise Linux AS R4.0
- Red Hat Enterprise Linux ES R4.0
- Red Hat Enterprise Linux ES 3.0 (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 23.
  - If Fault and Performance Manager runs “standalone,” complete the procedures in [Configuring Fault and Performance Manager for Stand-Alone Operation](#) on page 26.
2. Complete the procedures in [Administering Alarm Notification Services](#) on page 32.
3. If you will be using SNMP traps, complete the procedures in [Configuring SNMP Traps](#) on page 39.
4. If you will be running Fault and Performance Manager with an NMS, complete [Executing Auto-Discovery](#) on page 67.
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 57.

# 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 26.

If you are installing the HP OpenView integrated version, go to [Configuring Fault and Performance Manager to Integrate with HP OpenView](#) on page 23.

---

## 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 3.1* 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 following procedures to configure Fault and Performance Manager to integrate with HP OpenView.

## Configuring Fault and Performance Manager

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
3.1 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 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.
```

7. Use Avaya Integrated Management Database to integrate Avaya Fault and Performance Manager with HP OpenView. See the section “Add an NMSI/NMS Configuration” in *Avaya Integrated Management Release 3.1 Integrated Management Database Configuration, 14-300039*.

## Configuring Fault and Performance Manager for Stand-Alone Operation

Complete the following procedure 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
3.1 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.
```

## Configuring Fault and Performance Manager for Stand-Alone Operation

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 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. 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 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_[0-30]`. 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 3.1 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 3.1 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:

- Vytex, 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 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

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

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

---

## Recommended Software Requirements

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

- Avaya Integrated Management Release 3.1
- Avaya Communication Manager Release 3.1

---

## 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 40).
2. Stop the Master Agent in Avaya Communication Manager ([Procedure 2: Stop the Master Agent](#) on page 42).
3. Configure the SNMP Agent to use Avaya Fault and Performance Manager filtering ([Procedure 3: Configure SNMP Agent](#) on page 43).
4. Start the Master Agent ([Procedure 4: Start the Master Agent](#) on page 45).
5. Add nodes (for example, voice systems and adjuncts) you want to manage ([Procedure 5: Add Nodes](#) on page 46).

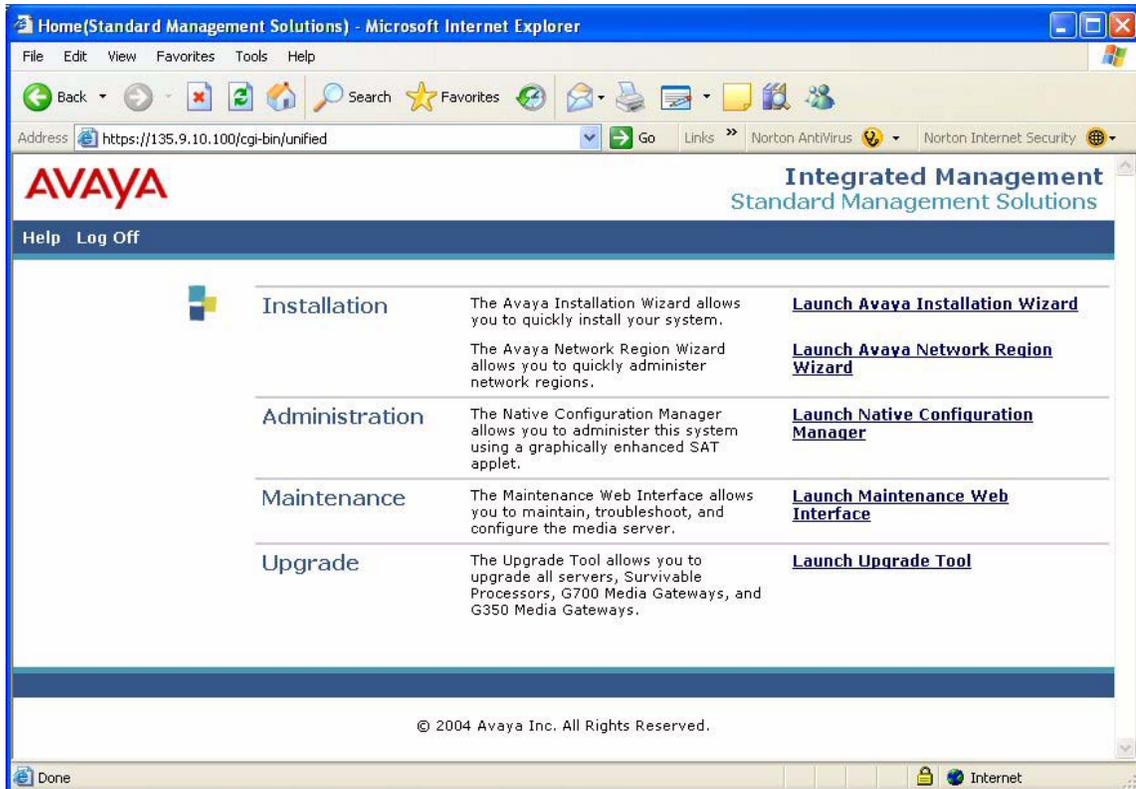
---

## Procedure 1: Launch the Maintenance Web Interface

To launch the Maintenance web interface:

1. Log into the server running Avaya Communication Manager Release 3.1.

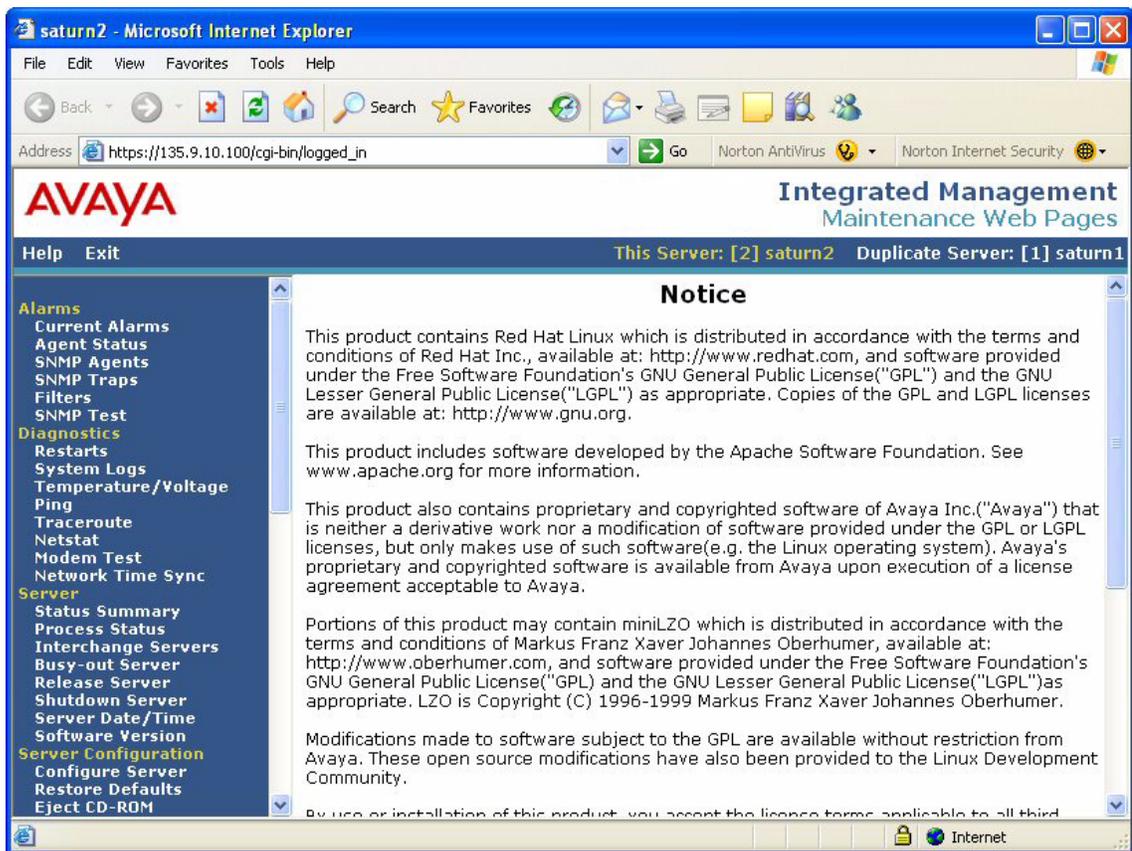
The Integrated Management Standard Management Solutions page appears.



## Procedure 1: Launch the Maintenance Web Interface

### 2. Click **Launch Maintenance Web Interface**.

The Maintenance Web Interface page appears.



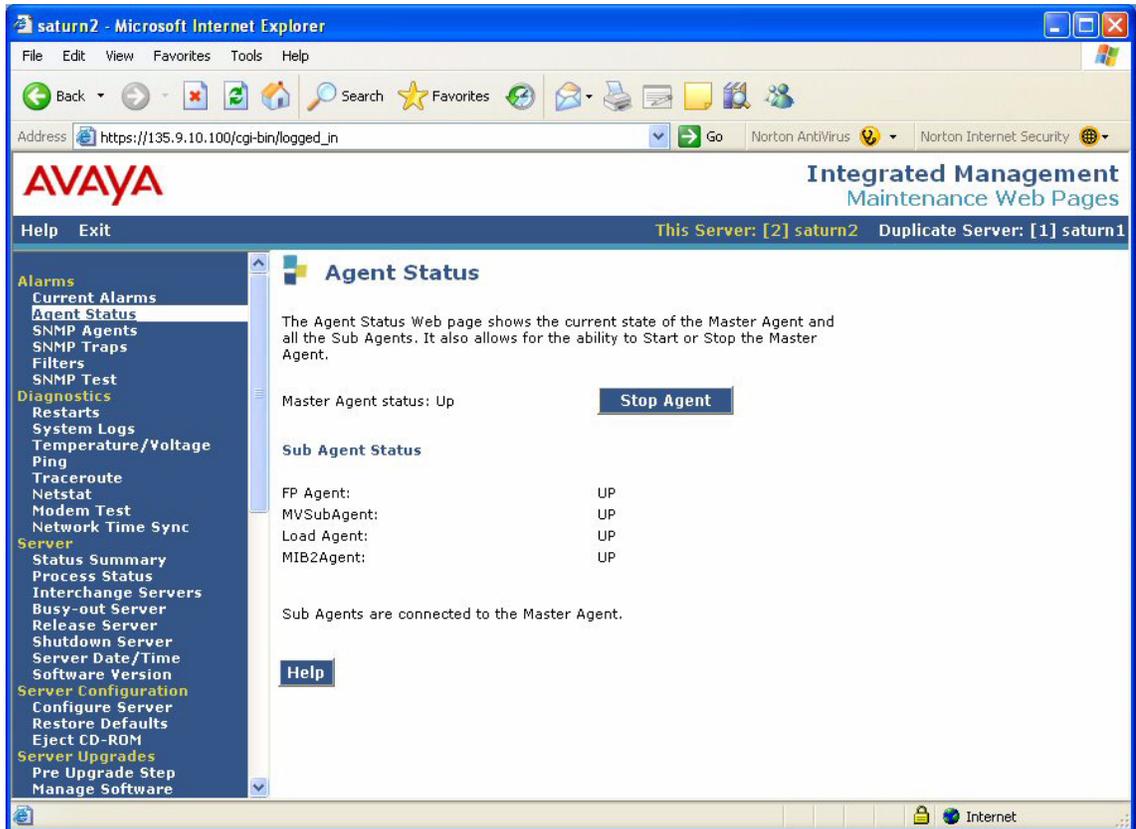
---

## Procedure 2: Stop the Master Agent

To stop the Master Agent:

1. From the Alarms heading located on the navigation frame, click **Agent Status**.

The Agent Status page appears.



2. Click the **Stop Agent** button.

# Procedure 3: Configure SNMP Agent

To configure SNMP agent to use FPM filtering:

- 1. From the Alarms heading located on the navigation frame, click **SNMP Agents**.  
The SNMP Agents page appears.



- 2. Click the **Following IP addresses** option button.
- 3. In the IP address box, enter the IP address of the server running Fault and Performance Manager.

## Configuring SNMP Traps

4. Scroll down and click the **Enable SNMP Version 1** check box.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The browser window is titled 'saturn2 - Microsoft Internet Explorer' and the address bar shows 'https://135.9.10.100/cgi-bin/logged\_in'. The page header includes the Avaya logo and 'Integrated Management Maintenance Web Pages'. The sidebar on the left contains a navigation menu with categories: Alarms, Diagnostics, Server, and Server Configuration. The main content area is titled 'SNMP Users / Communities' and includes an 'IP address5' field. Below this, there are three sections for enabling SNMP versions: 'Enable SNMP Version 1' (checked), 'Enable SNMP Version 2c' (checked), and 'Enable SNMP Version 3' (unchecked). Each checked section has two text input fields for 'Community Name (read-only)' and 'Community Name (read-write)'. The 'Enable SNMP Version 1' section has 'public' in the read-only field and 'g3pa' in the read-write field. The 'Enable SNMP Version 2c' section also has 'public' in the read-only field and 'g3pa' in the read-write field. Below these are sections for 'User (read-only)' and 'User (read-write)', each with fields for 'User Name', 'Authentication Password', and 'Privacy Password'. The 'Authentication Password' and 'Privacy Password' fields have explanatory text: '(for authentication and privacy)' and '(for privacy)' respectively.

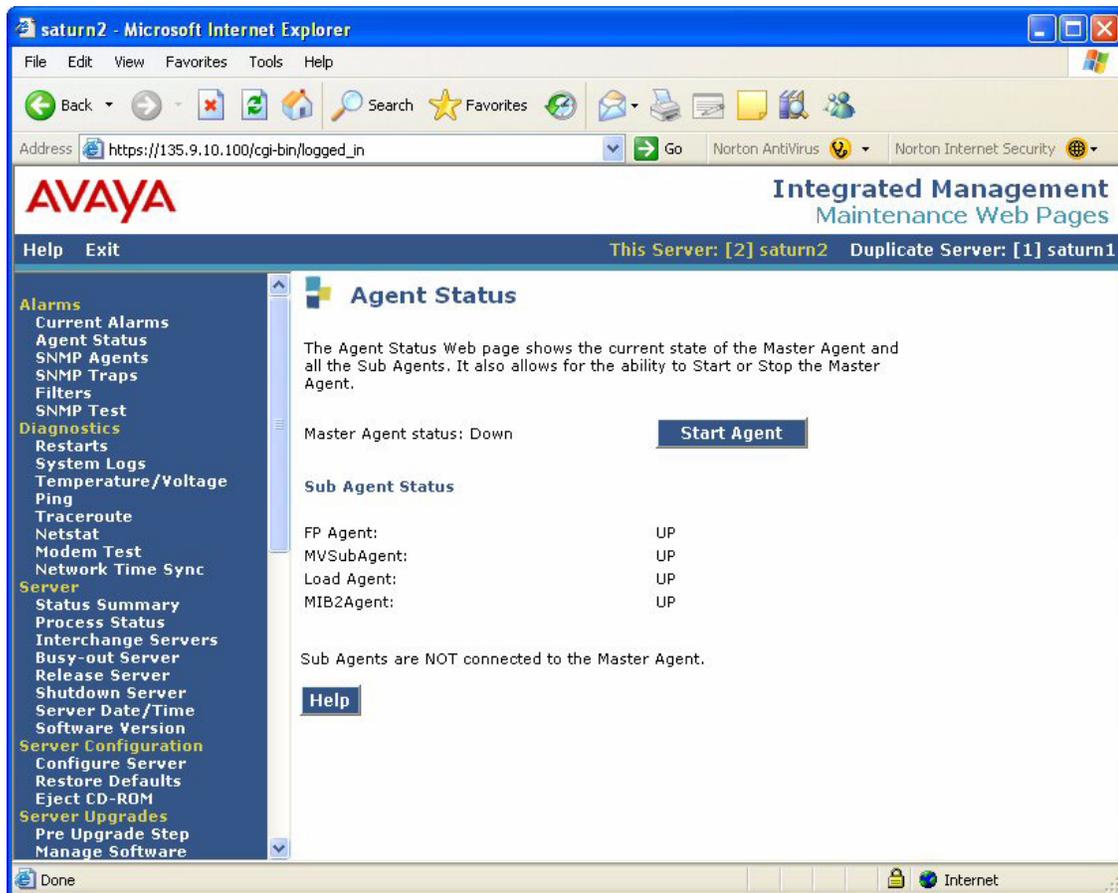
5. Enter the read\_community\_name in the Community Name (read-only) field.
6. Enter the read-write\_community\_name in the Community Name (read-write) field.
7. Click the **Enable SNMP Version 2c** check box.
8. Enter the read\_community\_name in the Community Name (read-only) field.
9. Enter the read-write\_community\_name in the Community Name (read-write) field.
10. Scroll down and click the **Submit** button.

## Procedure 4: Start the Master Agent

To start the Master Agent:

1. From the Alarms heading located on the navigation frame, click **Agent Status**.

The Agent Status page appears.



2. Click the **Start Agent** button.

Before you can use alarm filtering, you must configure alarm filters in Avaya Fault and Performance Manager. See [Configuring Alarm Filters](#) on page 59.

If you want to add nodes that you want to manage, go to [Procedure 5: Add Nodes](#) on page 46.

## Procedure 5: 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 3.1 Configuration* or the Integrated Management Database online help for information on how to add nodes.

---

## Testing the SNMP Agent

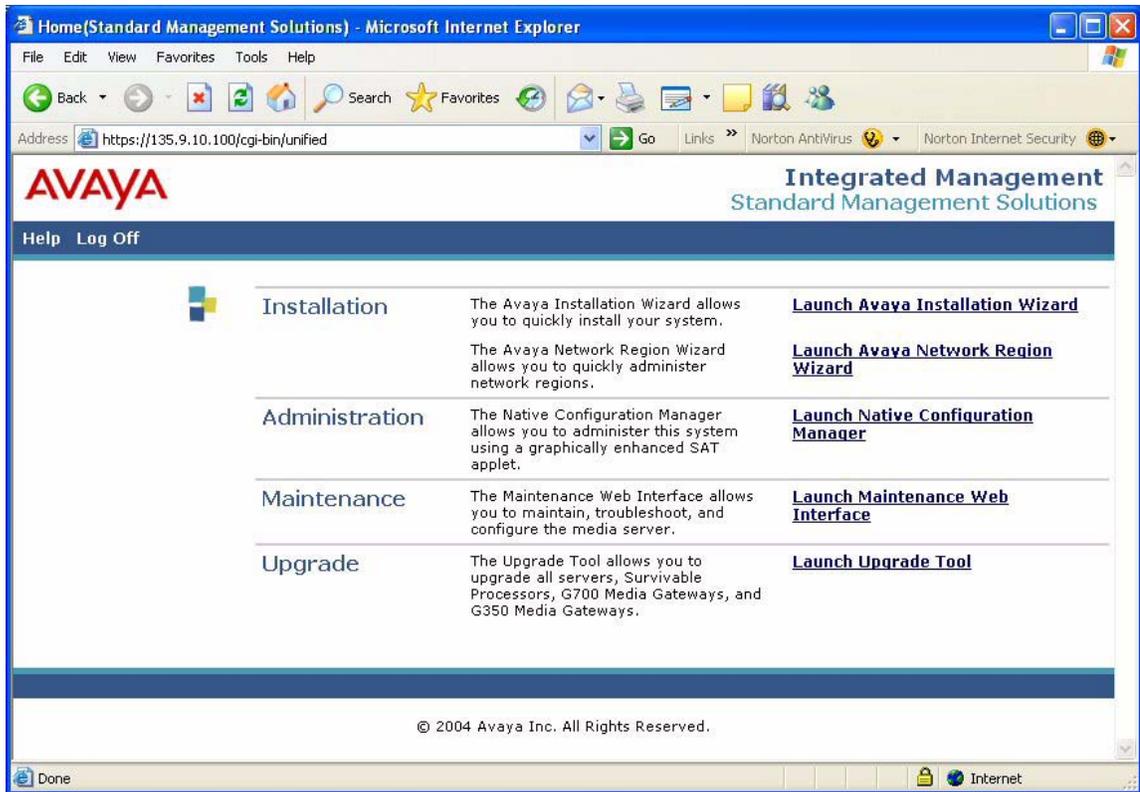
Perform this procedure to determine whether you have configured Avaya Communication Manager Release 3.1 and Avaya Fault and Performance Manager properly for alarm filtering. Before performing this procedure, make sure you have:

- Configured the SNMP Agent in Avaya Communication Manager.
- Configured alarm filtering in Avaya Fault and Performance Manager. See [Configuring Alarm Filters](#) on page 59.

To test the SNMP agent:

1. Log into the server running Avaya Communication Manager Release 3.1.

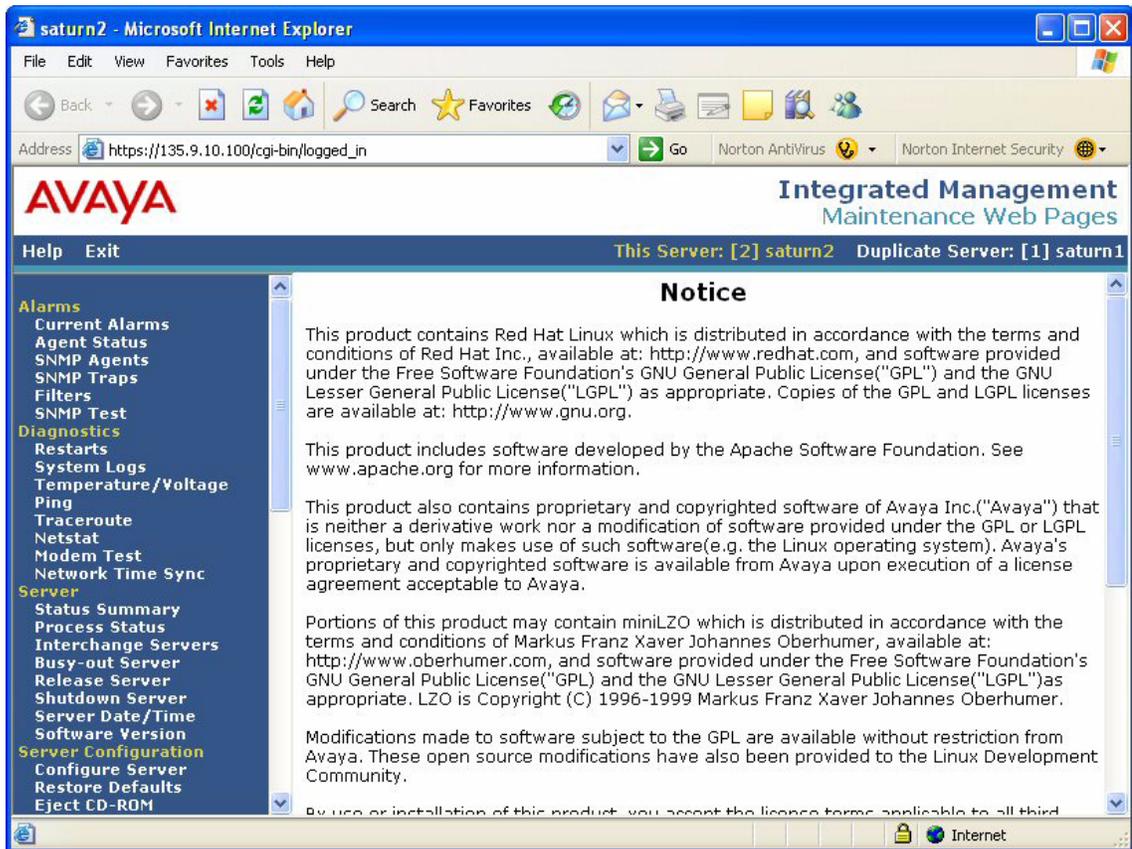
The Integrated Management Standard Management Solutions page appears.



## Configuring SNMP Traps

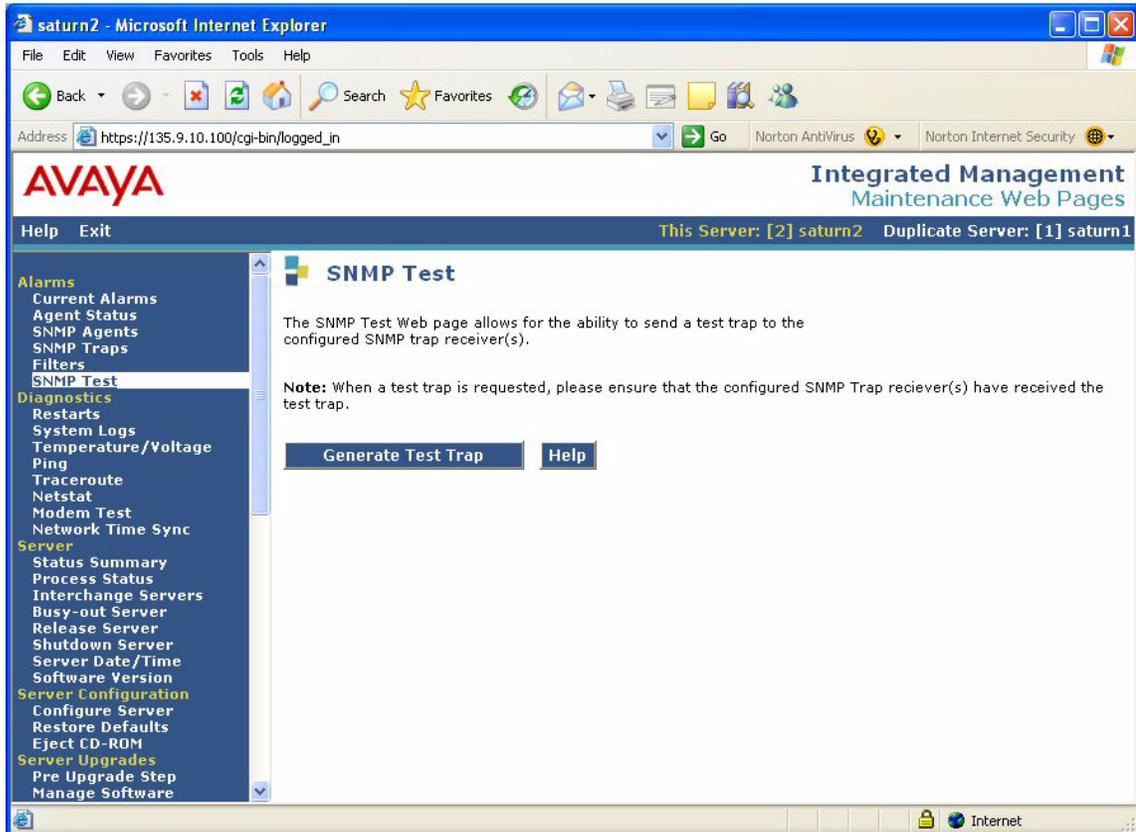
### 2. Click **Launch Maintenance Web Interface**.

The Maintenance Web Interface page appears.



3. From the Alarms heading located on the navigation frame, click **SNMP Test**.

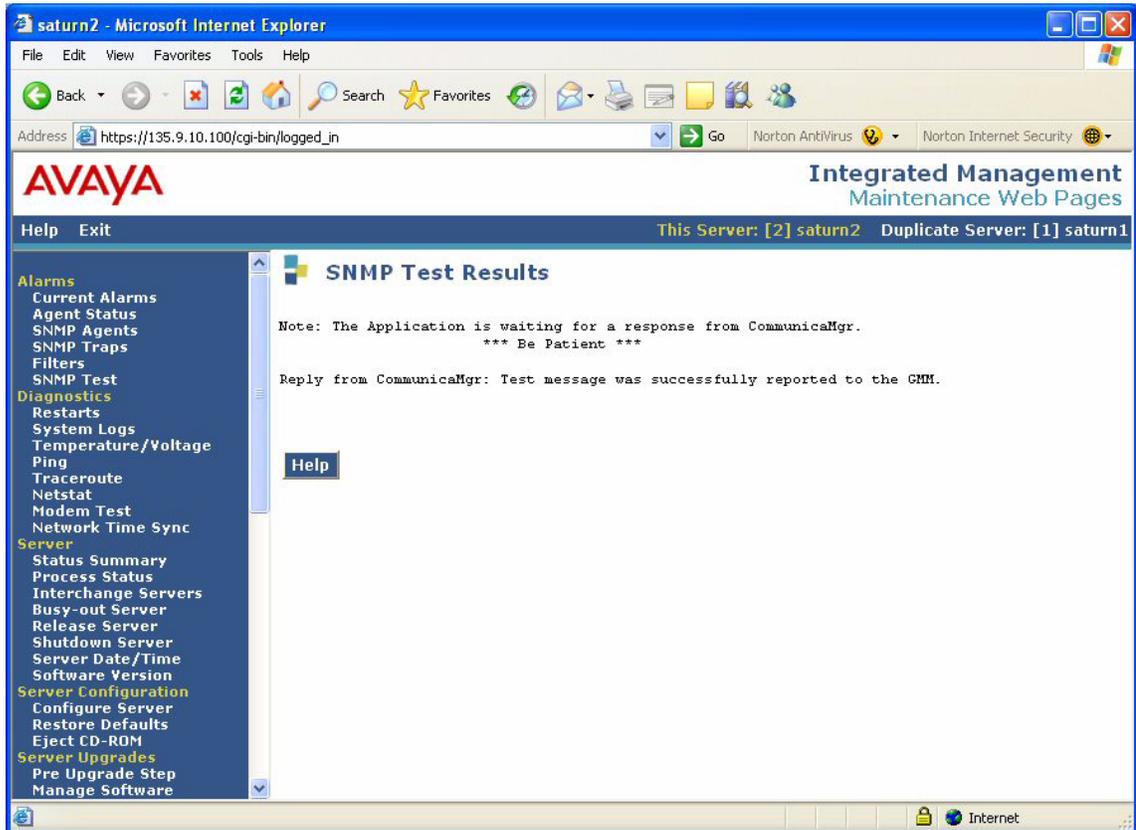
The SNMP Test page appears.



## Configuring SNMP Traps

4. Click the **Generate Test Trap** button.

The SNMP Test Results page appears.



You should see the trap received in Avaya Fault and Performance Manager.

The following is a sample trap in Avaya Fault and Performance Manager.

```

root@lavayaitms:/var/avaya/mfpm/logs
</msg>
<msg client=TrapService tag=Thread-20 time=Tue Jan 17 11:15:49 MST 2006>
In TrapReceiver.callback(), TRAP RECEIVED; agent=/135.9.10.98,
    type=v1, enterprise=.1.3.6.1.4.1.6889.1.8.1, generic=6, specific=4, community=public
VARIABLES:

Object ID: .1.3.6.1.4.1.6889.2.8.2.1.1.1.4
STRING: saturnc
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.18
STRING: 1000018380
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.17
STRING: FPA:00000:0117111539:0000000000:N
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.1
STRING: CUSTOMER ALARM TEST
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.3
STRING:
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.4
STRING:
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.6
STRING: WRN
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.26
STRING: 135.9.10.100
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.27
STRING:
Object ID: .1.3.6.1.4.1.6889.2.8.1.4.6.1.28
STRING:

</msg>
<msg client=TrapService tag=Thread-20 time=Tue Jan 17 11:15:49 MST 2006>
Found TrapProcessor Thread[com.avaya.dnm.trap.G3TrapProcessor,5,main] for oid= .1.3.6.1.4.1.6889.1.8.1.0.4
</msg>
<msg client=TrapService tag=Thread-5 time=Tue Jan 17 11:15:50 MST 2006>
100244751:class com.avaya.dnm.db.schema.exception.DBExceptionList updated
</msg>
<msg client=TrapService tag=Thread-5 time=Tue Jan 17 11:15:50 MST 2006>
selectElement select oid from DBTrapMssEx where _deftyName = 'Saturn' and _type in (13,9) and _severity = 1 and _active = true
and _startDeftyTime = 'Tue Jan 17 11:15:48 MST 2006' and _location = 'DoS Violation board:08C14' and _objectType = '' and _o
bjectId = ''
</msg>
<msg client=TrapService tag=Thread-5 time=Tue Jan 17 11:15:51 MST 2006>
Locking _numWarning31416 _numMinor 36 _numMajor14 _numCritical0 _numInads0
</msg>
<msg client=TrapService tag=Thread-5 time=Tue Jan 17 11:15:51 MST 2006>
13034,1 98%

```

**Configuring SNMP Traps**

# 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.

## Getting Started

- **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

- **MovePN**

Allows the user to move the port networks in an ESS cluster.

- **Helper**

Allows the user to access the Helpdesk feature from the FPM user interface.

- **Assist**

Allows the user to automatically run the Avaya Communication Manager commands recommended by the Helpdesk feature when an alarm is received.

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 55.

---

## 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 56 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. If you want to prevent this user from logging in, select the **Login Disabled** check box.

10. In the Failed Attempts box, enter the maximum number of attempts the user can make to log in to the system.

11. Select the **FPM** check box.

12. Click **Add**.

13. 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 56.

---

## 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.

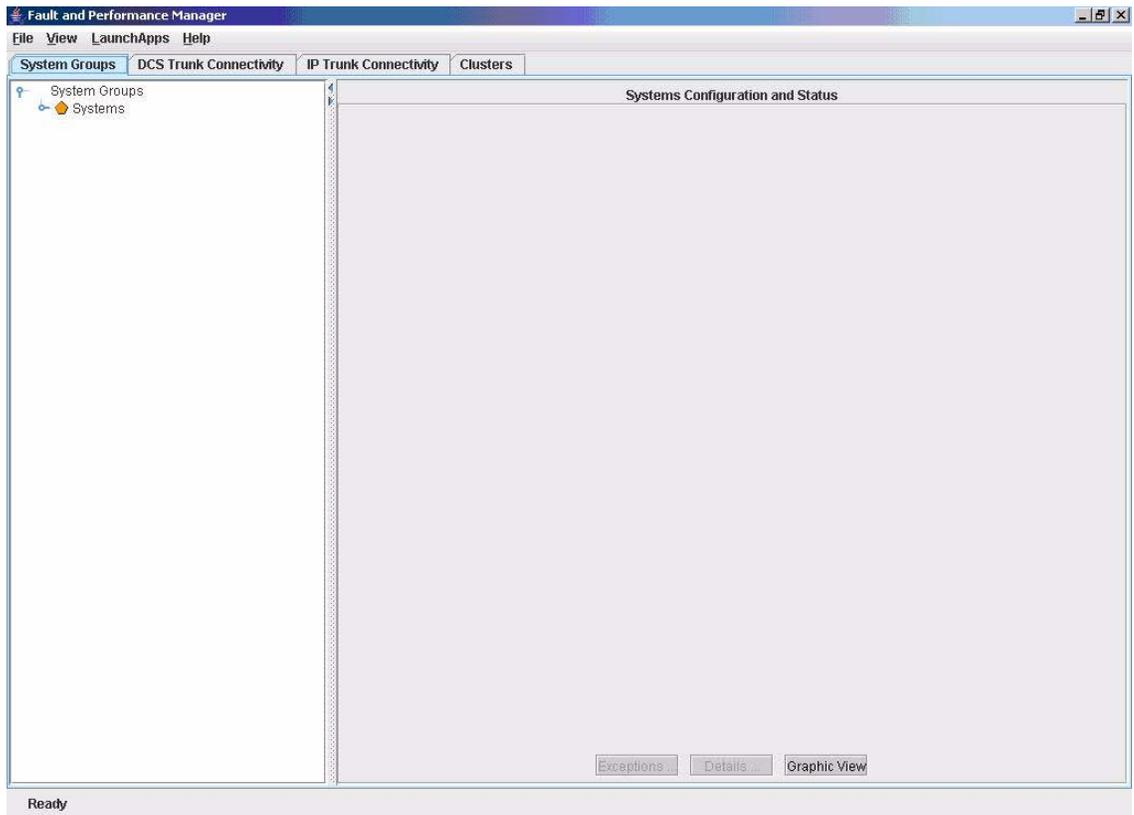
1. Open a supported browser.
2. At the URL address line, type the IP address for the Linux server where Fault and Performance Manager is installed, and press **ENTER**.  
The system displays the Integrated Management Launch Products page.
3. Click the **System Management** tab on the Integrated Management 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.

---

# Configuring Alarm Filters

To configure alarm filters in Avaya Fault and Performance Manager:

1. Access the Avaya Fault and Performance Manager window.



## Getting Started

2. , Click **File>Administration>Default Parameters/Alarms/Errors**.

The Alarms/Errors page appears.

The screenshot displays the 'Fault and Performance Manager' application window. The title bar reads 'Fault and Performance Manager'. The menu bar includes 'File', 'View', 'LaunchApps', 'Help', and 'Tools'. The main window title is 'Default - Alarms/Errors'. On the left, a tree view shows the navigation structure, with 'Alarms/Errors' selected. The main area contains an 'Alarm Filter Panel' with two tabs: 'Filters' and 'Times'. The 'Filters' tab is active, showing a table with the following data:

Filter Type	Severity	Frequency	Category	MO Type	Location
BoardConflicts	Warning	Daily	All	All	All
Definity Alarms	Critical	Daily	All	All	All
Definity Alarms	Major	Daily	All	All	All
Definity Alarms	Minor	Daily	All	All	All
Definity Alarms	Warning	Daily	All	All	All
Errors	None	Daily	All	All	All
Restarts	Major	Daily	All	All	All
Server Alarms	Critical	Daily	All	All	All
Server Alarms	Major	Daily	All	All	All
Server Alarms	Minor	Daily	All	All	All
Server Alarms	Warning	Daily	All	All	All

Below the table are buttons for 'Add', 'Modify', 'Delete', 'Save', 'Reset', and 'Help'. The status bar at the bottom left shows 'Ready'.

3. Select the alarm filter you want to change, and then click the **Modify** button.

The Alarm Filter Configurator page appears.

The screenshot shows a window titled "Alarm Filter Configurator" with a standard Windows-style title bar. The window contains two main sections: "Select Filter Parameters" and "Select Action Parameters".

**Select Filter Parameters:**

Filter Type	Severity	Collection Freq	Category	MO-type	MO-location
Definity Ala...	Warning	Hourly	trunks	ISDN-LNK	01C0101

**Select Action Parameters:**

Alert/Store as	ARS Script	Send Mail to	Trap Level
Warning	None	None	Warning

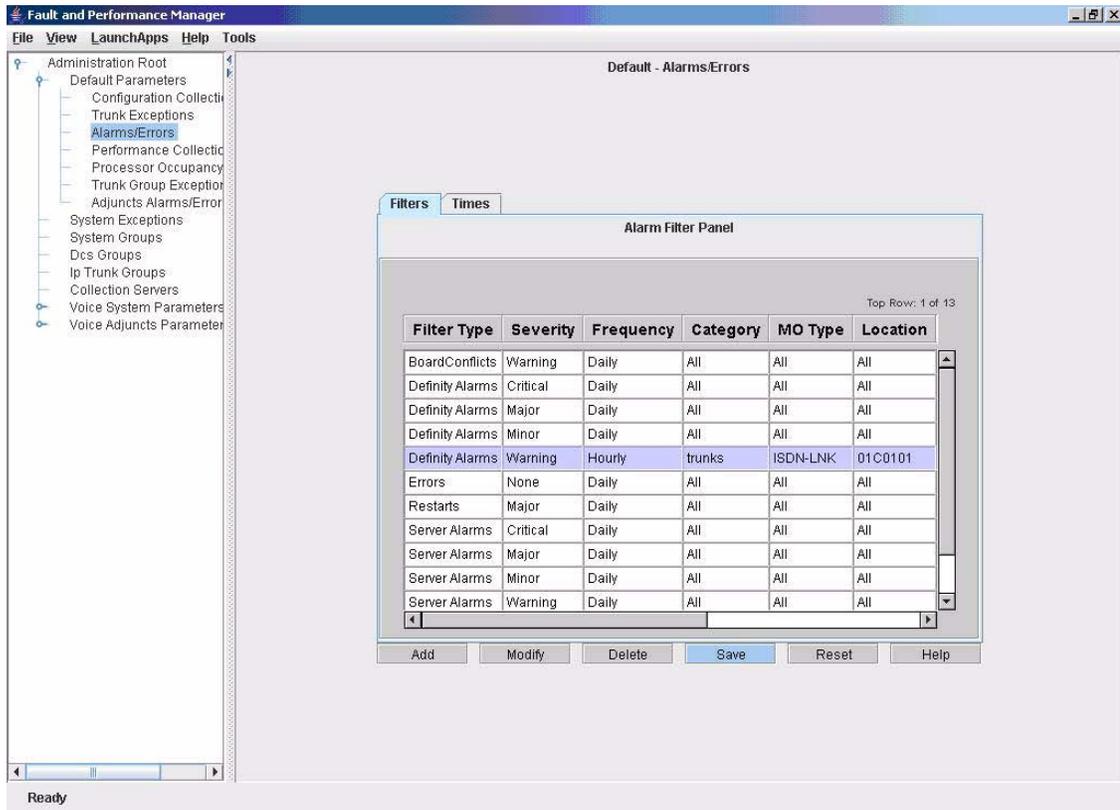
At the bottom of the dialog, there are three buttons: "OK", "Help", and "Cancel".

4. Select the appropriate parameters.

## Getting Started

5. When finished, click the **OK** button.

The Alarms/Errors page appears.



6. Repeat Steps 2 through 4 for each alarm filter you want to change.

7. When finished, click the **Save** button.

The filter parameters are saved in Avaya Fault and Performance Manager and updated in Avaya Communication Manager.

---

## 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 `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).

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	<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:

- 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.

## Getting Started

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	<b>Dark Blue</b> = Unknown. Proxy Agent is not responding <b>Green</b> = Normal <b>Cyan</b> = Warning <b>Yellow</b> = Minor <b>Orange</b> = Major <b>Red</b> = Critical
Line connections to Communication Manager Feature Server 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 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	<b>Dark Blue</b> = Unknown. Proxy Agent is not responding <b>Green</b> = Normal <b>Cyan</b> = Warning <b>Yellow</b> = Minor <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 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	<p>This command displays the results of a Fault and Performance Manager Exception report.</p> <p>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.</p>
Rediscover Entire Map	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>● The FPM server must be operational.</li> <li>● HP OpenView must have a Read-Write map open.</li> <li>● A connection must be established between HP Open View and the Fault and Performance Manager server process, NmsiServer.</li> </ul> <p>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&gt; Refresh from each R/O map to bring it into sync with the R/W map. Doing the Map&gt;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.</p>

**Table 12: NMS Map commands (continued)**

Command	Description
Re-register with Server	<p>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.</p> <p>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.</p>
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 11.

## 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 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 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 20.

**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 12.



# Index

---

## Symbols

>, meaning of . . . . . [7](#)

---

## A

Auto-Discovery  
 execute on public networks . . . . . [67](#)  
 integration function . . . . . [64](#)  
 Avaya Technology and Consulting (ATAC) . . . . . [11](#)

---

## B

backup, database . . . . . [31](#)  
 boldface, meaning of. . . . . [7](#)  
 books  
 giving feedback on . . . . . [8](#)  
 on the web . . . . . [9](#)

---

## C

commands . . . . . [30](#)  
 system health . . . . . [31](#)  
 configuring FP Mgr for stand-alone . . . . . [26](#)  
 contact information  
 third party . . . . . [15](#)  
 contact information for Avaya . . . . . [14](#)

---

## D

database  
 backup. . . . . [31](#)  
 restoring . . . . . [32](#)  
 Discovery  
 introduction. . . . . [69](#)  
 documentation  
 giving feedback on . . . . . [8](#)  
 on the web . . . . . [9](#)

---

## E

editing system files. . . . . [32](#)

---

## F

feedback, giving us your . . . . . [8](#)

---

## H

HP OpenView, integrating FP Mgr with. . . . . [23](#)

---

## I

integrating FP Mgr with HPOV. . . . . [23](#)

---

## M

Microsoft web site . . . . . [15](#)

---

## N

network  
 security . . . . . [15](#)  
 Network Management System (NMS)  
 integration process . . . . . [64](#)

---

## O

OpenView, integrating FP Mgr with . . . . . [23](#)

---

## P

passwords  
 changing . . . . . [15](#), [63](#)

---

## R

Red Hat web site . . . . . [15](#)  
 requirements . . . . . [21](#)  
 resources  
 Avaya Communications, Solutions, and  
 Integration (CSI) Group of Software Services . . . [11](#)  
 Customized Management Solutions for Avaya  
 Integrated Management . . . . . [13](#)  
 restore database . . . . . [32](#)

---

## Index

---

### S

security	
Avaya disclaimer . . . . .	<a href="#">16</a>
for networks . . . . .	<a href="#">15</a>
network . . . . .	<a href="#">15</a>
notices . . . . .	<a href="#">15</a>
toll fraud . . . . .	<a href="#">16</a>
toll fraud intervention . . . . .	<a href="#">16</a>
stand-alone configuration . . . . .	<a href="#">26</a>
system commands . . . . .	<a href="#">30</a>
system files, editing . . . . .	<a href="#">32</a>
system health . . . . .	<a href="#">31</a>
system requirements . . . . .	<a href="#">21</a>

---

### T

Technical Service Organization . . . . .	<a href="#">12</a>
Technical Services Organization . . . . .	<a href="#">12</a>
toll fraud. . . . .	<a href="#">16</a>
Avaya disclaimer . . . . .	<a href="#">16</a>
intervention. . . . .	<a href="#">16</a>
TSO . . . . .	<a href="#">12</a>
typographical conventions . . . . .	<a href="#">7</a>

---

### W

web sites	
third-party . . . . .	<a href="#">15</a>