Avaya Integrated Management Release 5.0 Fault and Performance Manager Configuration

555-233-138
Issue 11
January 2008

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

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.

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 Reader. Adobe Reader 7.0 is provided on the Avaya Integrated Management CD 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 TECHNICAL INFORMATION 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/G450/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 10 for contact information.

Avaya Global Services Delivery (GSD)

Avaya Global Services Delivery (GSD) provides support to the Avaya Integrated Management client teams, field technicians, and customers. The GSD 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 GSD does not support hardware or software that customers purchase from third-party vendors.

Avaya Global Technical Services

Avaya Global Technical Services answers customer calls about products in Avaya Integrated Management. They will either answer your questions directly or connect you with an associate who can answer questions about the products.

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 10 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
Avaya Global Technical Services	+1 800 242-2121 x15921
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 10.

Chapter 2: Overview

Avaya Fault and Performance Manager (Fault and Performance Manager or FPM) 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 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, 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 directly from an IP-enabled voice system using OSSI (a proprietary management protocol) 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.

What's New in this Release

Fault and Performance Manager Release 5.0 introduces the following enhancements:

- Support for Avaya Communication Manager - SIP Enablement Services (SES) co-residency. This will be indicated in the Server Type field of the System Configuration screen.
- Support for servers running Avaya Communication Manager Release 5.0.
- Support for the S8300C server.
- Support for the Avaya Expanded Meet-Me Conferencing (EMMC) server.
- Support for the G450 media gateway.
- Support for the following routers with the IG 550 Integrated Gateway:
  - J2320
  - J2350
  - J4350
  - J6350
- Increased attendant consoles. The Performance: Attendant Groups report can display up to 414 attendant consoles based on up to 100 attendant consoles for a complex switching system when represented as a "Mega Switch," and up to 314 attendant consoles for a geographically dispersed network of cabinets/media gateways/remote offices.
- A Transaction Log. A Transaction Log report has been added to the Exception Report group. This report logs the userID, transaction, and the results of the transaction.
- Simplified filter types in the Alarm Filter Panel.
- Enhanced server alarm filtering. Alarm filtering for a specific equipment type can specify an error code. You can also specify alarm filtering for restart alarms by level.
- Support for the following maintenance object (MO) types in the Help Desk function:
  - VAL-BD (Voice Announcement over LAN circuit pack)
  - DID-TRK (DID trunk)

Supported Systems

Fault and Performance Manager Release 5.0 supports configuration, alarms, and performance data 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, G450, G600, and G700 Media Gateways
- Avaya Communication Manager (Linux) Release 2.1, 3.0, 3.1, 4.0, and 5.0
- Avaya Communication Manager Release 9.5 through 11

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

Fault and Performance Manager Release 5.0 supports only alarm traps for the following systems:

- 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
- 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
- Message Networking Release 1.0 through 3.0
- Secure Services Gateway (SSG)
- Avaya Expanded Meet-Me Conferencing (EMMC) server

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 10.

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 11.

CAUTION:

Customers are solely responsible for upgrading their network platforms to meet the platform requirements for Fault and Performance Manager Release 5.0.

Software

Fault and Performance Manager Release 5.0 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)

Configuration Overview

The configuration process will follow the basic steps listed below:

1. During the software installation, perform one of the following steps:
   - If you want to configure a primary Fault and Performance Manager server, complete the procedures in Configuring a Primary Fault and Performance Manager Server on page 20.
   - If you want to configure a secondary Fault and Performance Manager server, complete the procedures in Configuring a Secondary Fault and Performance Manager Server on page 22.
2. If you will be using SNMP traps, complete the procedures in Configuring SNMP Traps on page 29.
3. If you want to integrate FPM with an NMS, go to Integrating Fault and Performance Manager with an NMS on page 58

Chapter 3: Configuring Fault and Performance Manager

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

If you want to configure a primary FPM server, go to Configuring a Primary Fault and Performance Manager Server on page 20.

If you want to configure a secondary FPM server, go to Configuring a Secondary Fault and Performance Manager Server on page 22.

Configuring a Primary Fault and Performance Manager Server

Complete the following procedure to configure a primary Fault and Performance Manager server.

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
   5.0 software [yes]?
   ```

3. Type **yes** and press **ENTER**.

   The system displays the prompt:

   ```
   Enter FPM server IP or 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:

   Primary FPM server is "xxx.xxx.xxx.xxx"

   ---------------------------------------------

   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:

```
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- [ ]?
```

7. Enter the FQDN of this server, and press **ENTER**.

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

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

Configuring a Secondary Fault and Performance Manager Server

Complete the following procedure to configure a secondary Fault and Performance Manager server.

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
   5.0 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 **no** and press **ENTER**.

   The system displays the message:

   ```
   Avaya Fault and Performance Manager Secondary Data Collection
   Server. Enter FPM Secondary Collector Service name for this server
   [ ]?
   ```

6. Enter the name for the secondary FPM server, and press **ENTER**.

   The system displays the prompt:

   ```
   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- [ ]?
   ```

7. Enter the FQDN for the secondary FPM server, and press **ENTER**.

   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.
- 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 Guide for Avaya Communication Manager, 03-300509*.

System Commands

Start and Stop Commands

Fault and Performance Manager processes normally start automatically at Linux boot time. 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 From a web browser: http://fpmserver/cgi-bin/mfpm/Status.sh	Displays Fault and Performance Manager system process status.
/opt/avaya/mfpm/bin/mfpm gui	Opens a graphical monitor of process status.
mfpmconfig show From a web browser: http://fpmserver/cgi-bin/mfpm/Config.sh	Displays the configuration of the Fault and Performance Manager server.
CollStatus status From a web browser: http://fpmserver/cgi-bin/mfpm/CollStatus.sh?cmd=status	Displays the current collection queues of the Fault and Performance Manager server.
CollStatus schedule From a web browser: http://fpmserver/cgi-bin/mfpm/CollStatus.sh?cmd=schedule	Displays the current scheduled collection items on the Fault and Performance Manager server.

Backing up the FPM Database

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

Please refer to the Linux backup procedure in the *Avaya Integrated Management Release 5.0 System Management Installation and Upgrade*.

Restoring the FPM Database

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

Please refer to the Linux restore procedure in the *Avaya Integrated Management Release 5.0 System Management Installation and Upgrade*.

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 5.0
- Avaya Communication Manager Release 5.0

Configuration Procedures

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

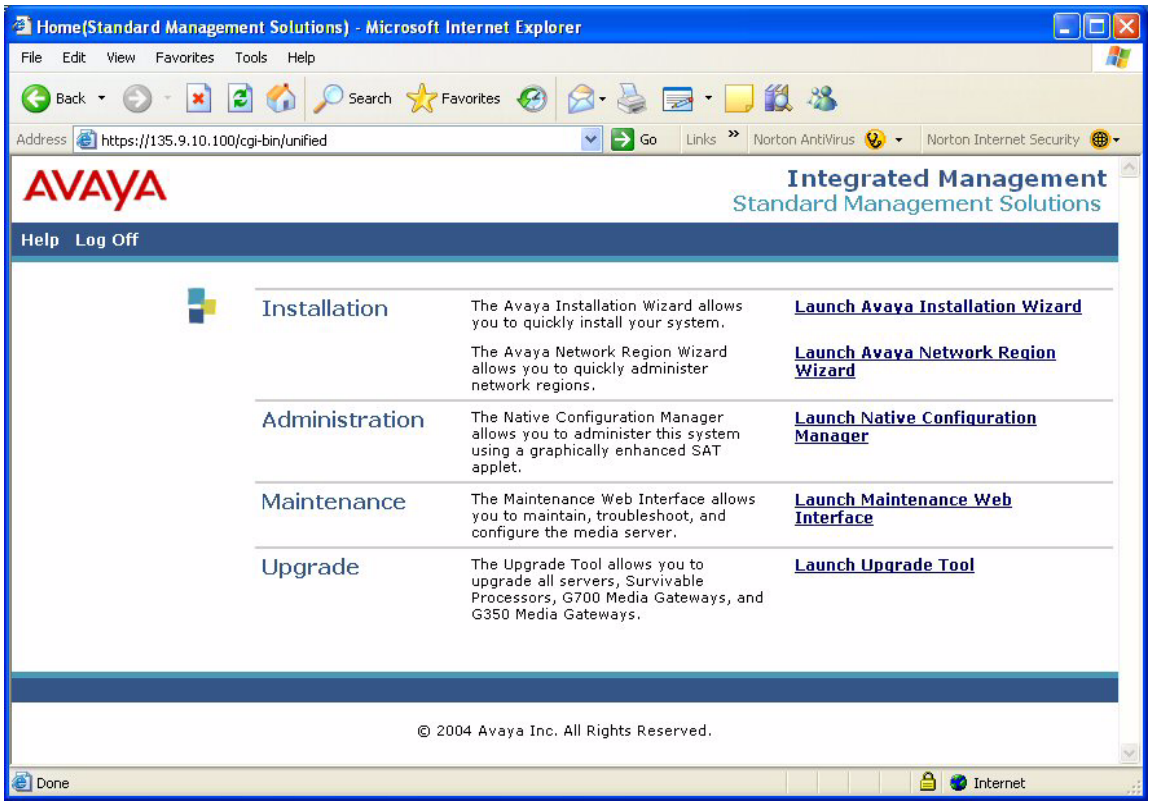
1. Launch the Maintenance web interface (Procedure 1: Launch the Maintenance Web Interface on page 30).
2. Stop the Master Agent in Avaya Communication Manager (Procedure 2: Stop the Master Agent on page 32).
3. Configure the SNMP Agent to use Avaya Fault and Performance Manager filtering (Procedure 3: Configure SNMP Agent on page 33).
4. Start the Master Agent (Procedure 4: Start the Master Agent on page 35).
5. Add nodes (for example, voice systems and adjuncts) you want to manage (Procedure 5: Add Nodes on page 36).

Procedure 1: Launch the Maintenance Web Interface

To launch the Maintenance web interface:

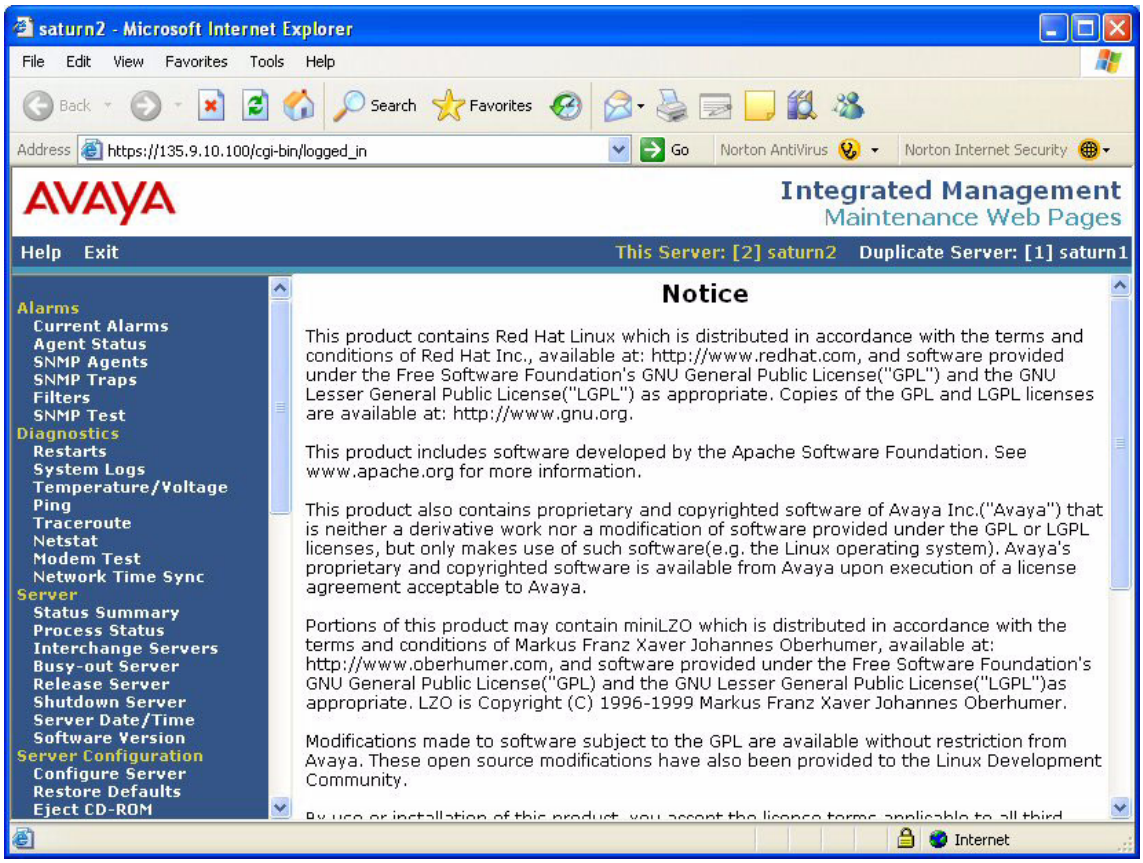
1. Log into the server running Avaya Communication Manager Release 5.0.

   The Integrated Management Standard Management Solutions page appears.



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

   The Maintenance Web Interface page appears.

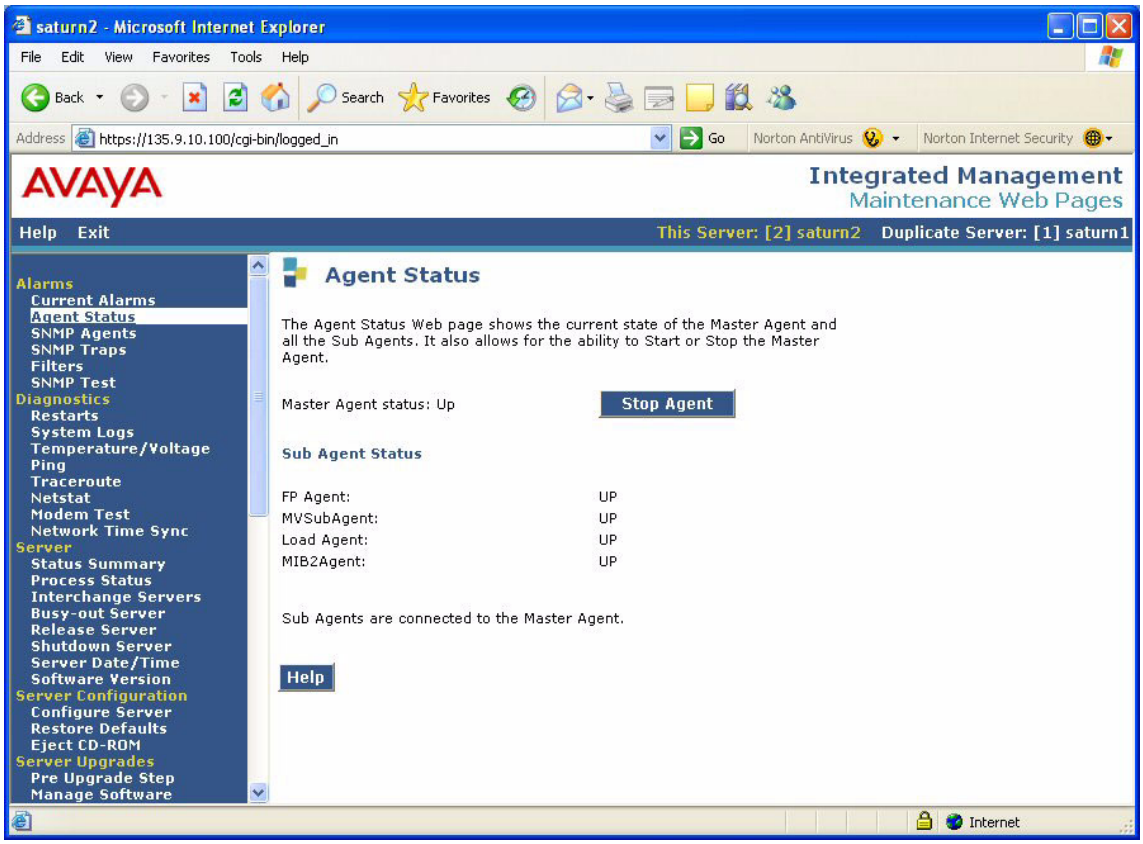


Procedure 2: Stop the Master Agent

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

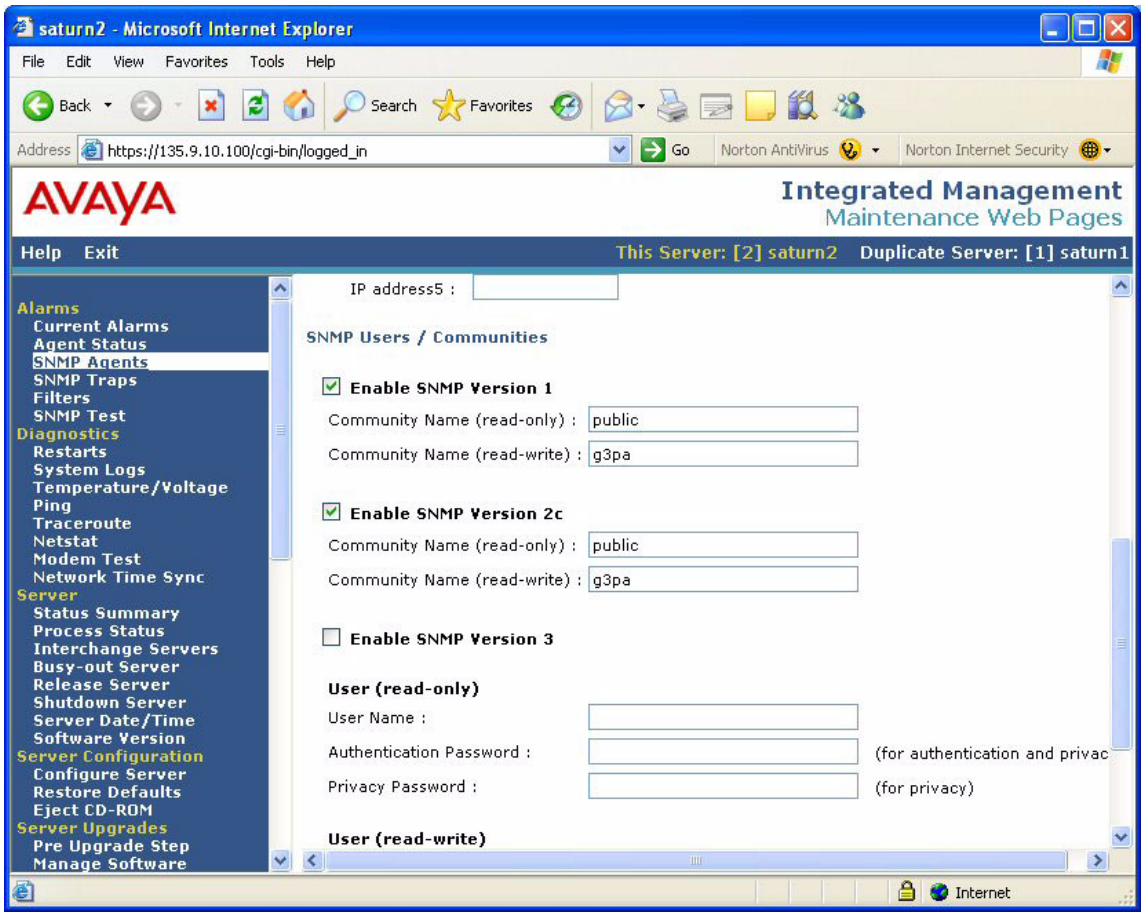
To configure SNMP agent to use FPM filtering:

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.

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



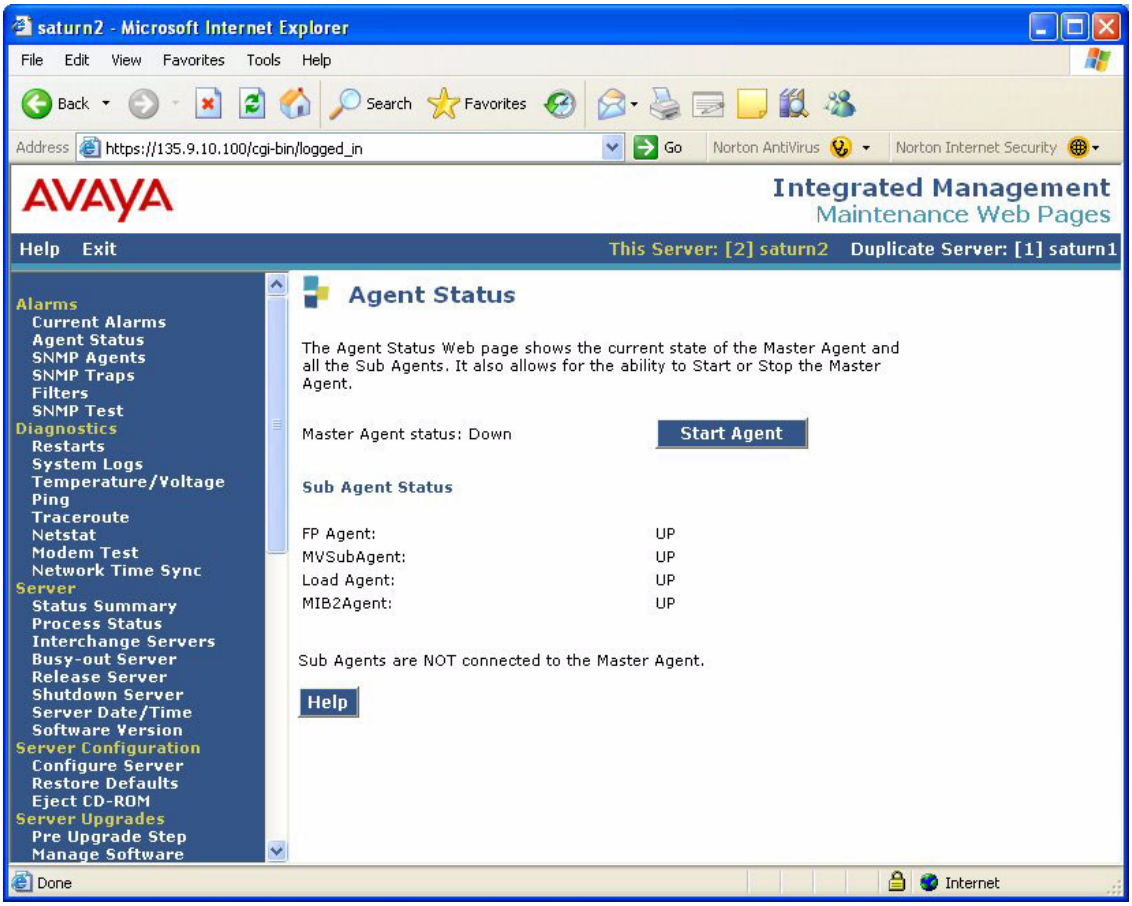
5. Enter the read_community_name in the Community Name (read-only) field. This string must match the information you specified in the SNMP Read Community box in the IMD SNMP Configuration page.
6. Enter the read-write_community_name in the Community Name (read-write) field. This string must match the information you specified in the SNMP Write Community box in the IMD SNMP Configuration page.
7. Click the **Enable SNMP Version 2c** check box.
8. Enter the read_community_name in the Community Name (read-only) field. This string must match the information you specified in the SNMP Read Community box in the IMD SNMP Configuration page.
9. Enter the read-write_community_name in the Community Name (read-write) field. This string must match the information you specified in the SNMP Write Community box in the IMD SNMP Configuration page.
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 50.

If you want to add nodes that you want to manage, go to Procedure 5: Add Nodes on page 36.

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 5.0 Configuration* or the Integrated Management Database online help for information on how to add nodes.

Testing the SNMP Agent

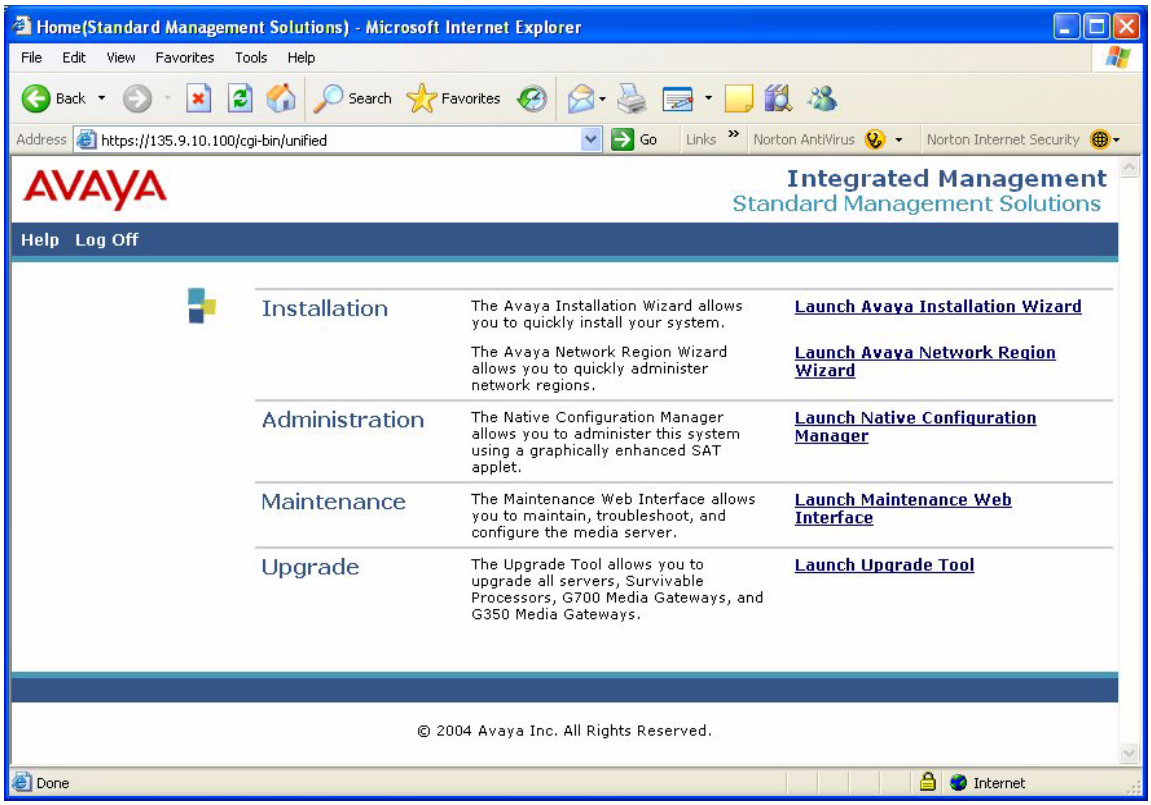
Perform this procedure to determine whether you have configured Avaya Communication Manager Release 5.0 or later and Avaya Fault and Performance Manager properly for alarm filtering. Before performing this procedure, make sure you have:

- Configured the SNMP Agent in Avaya Communication Manager.
- Configured alarm filtering in Avaya Fault and Performance Manager. See Configuring Alarm Filters on page 50.

To test the SNMP agent:

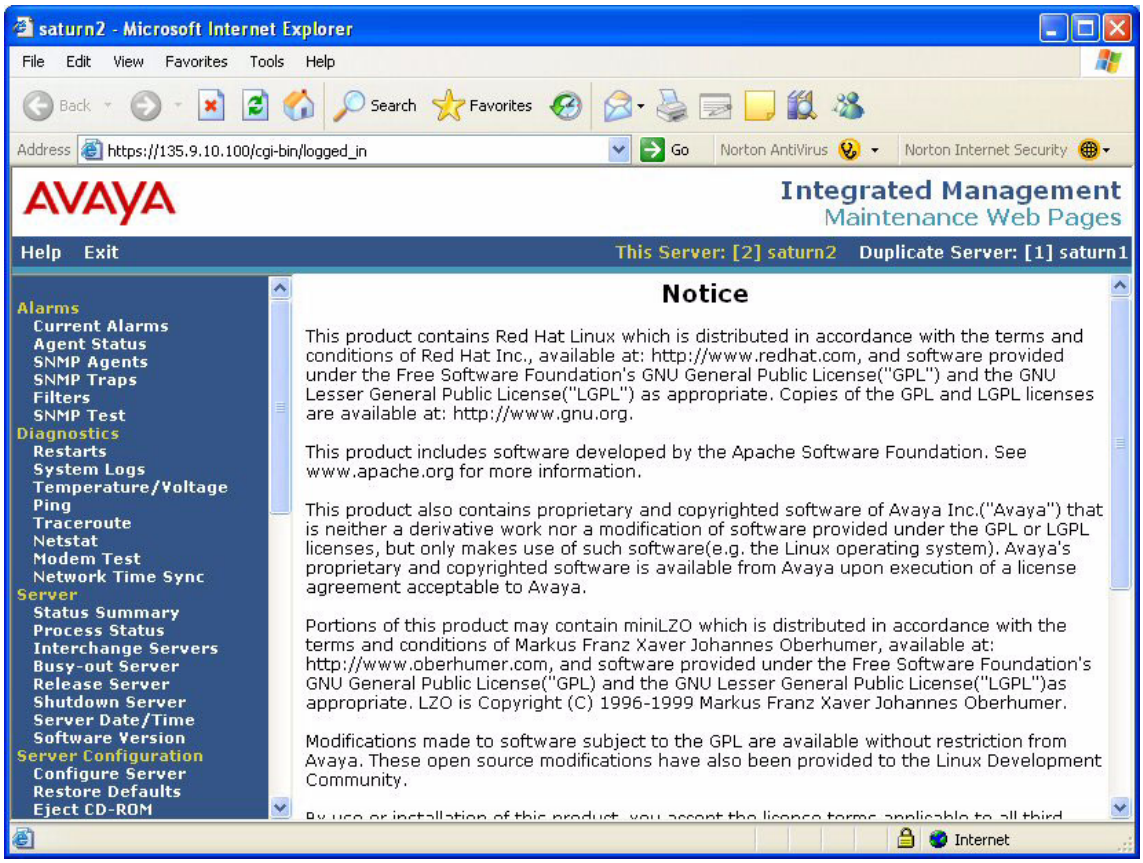
1. Log into the server running Avaya Communication Manager Release 5.0.

   The Integrated Management Standard Management Solutions page appears.



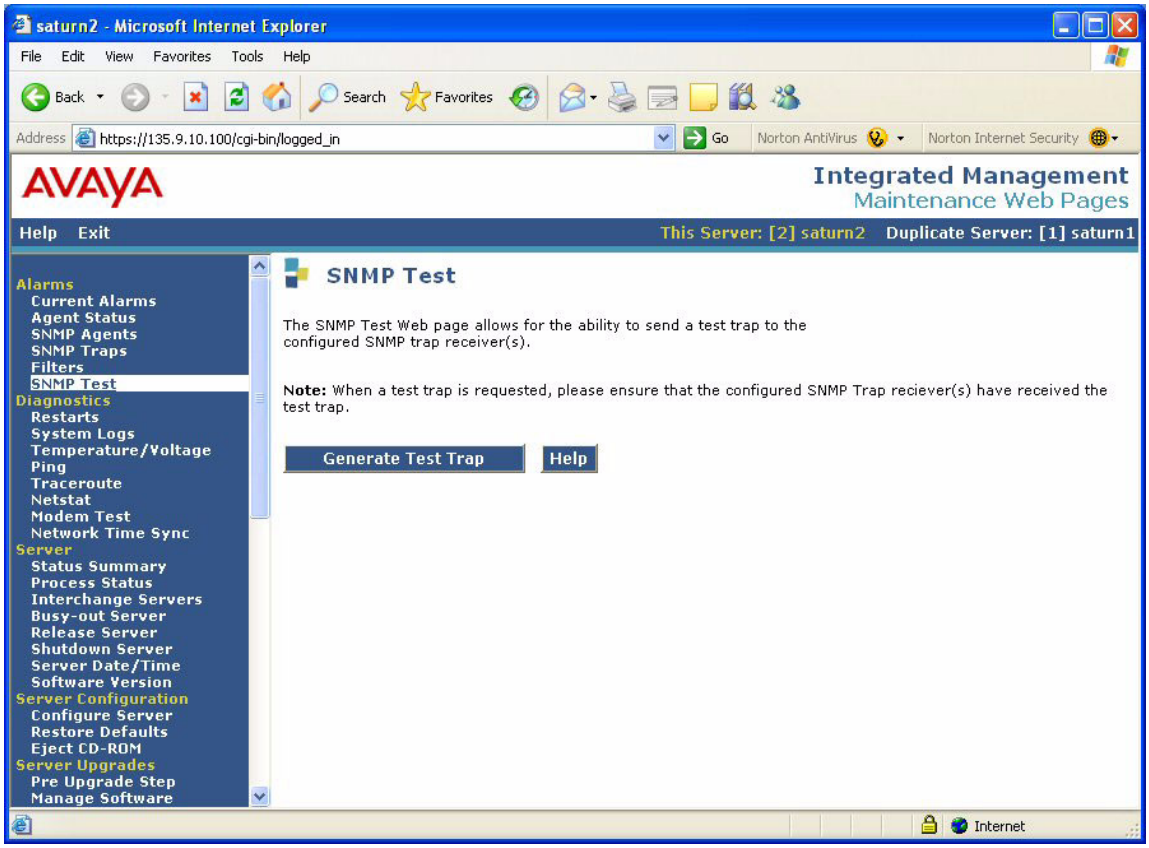
2. Click **Launch Maintenance Web Interface**.

   The Maintenance Web Interface page appears.



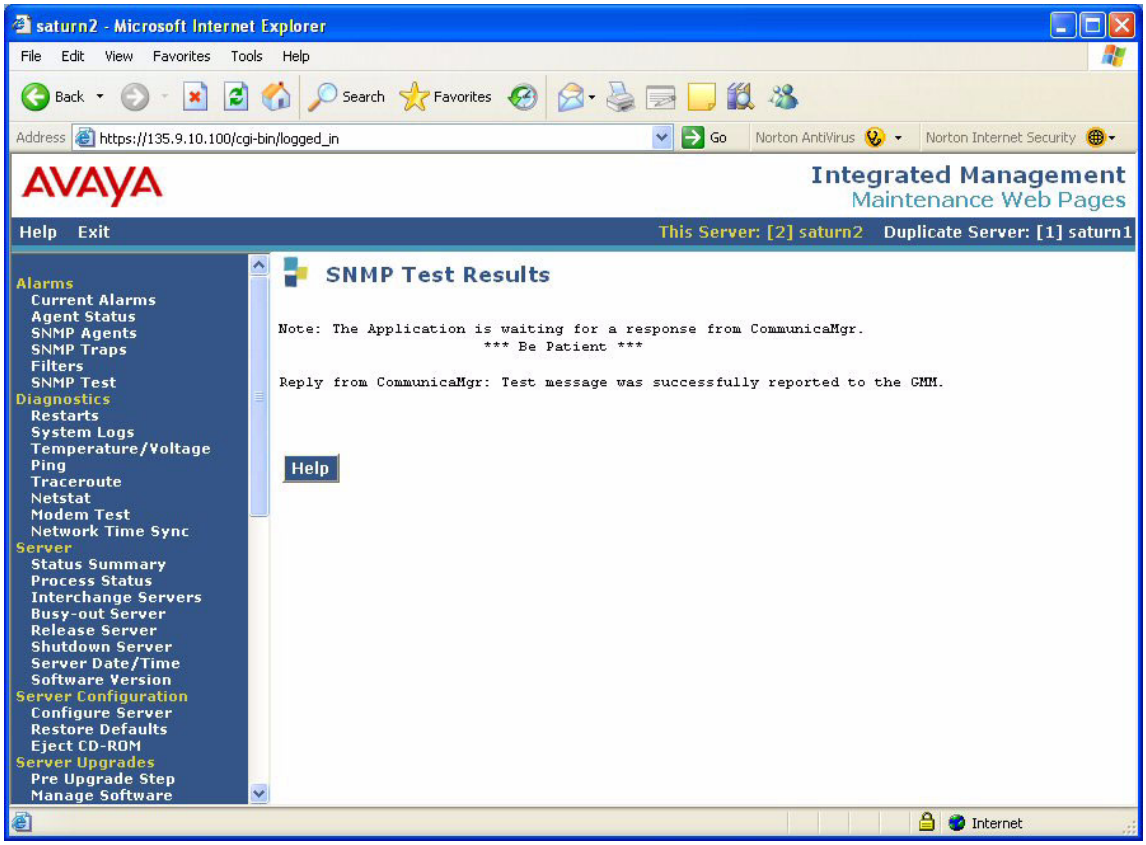
3. From the Alarms heading located on the navigation frame, click **SNMP Test**.

   The SNMP Test page appears.



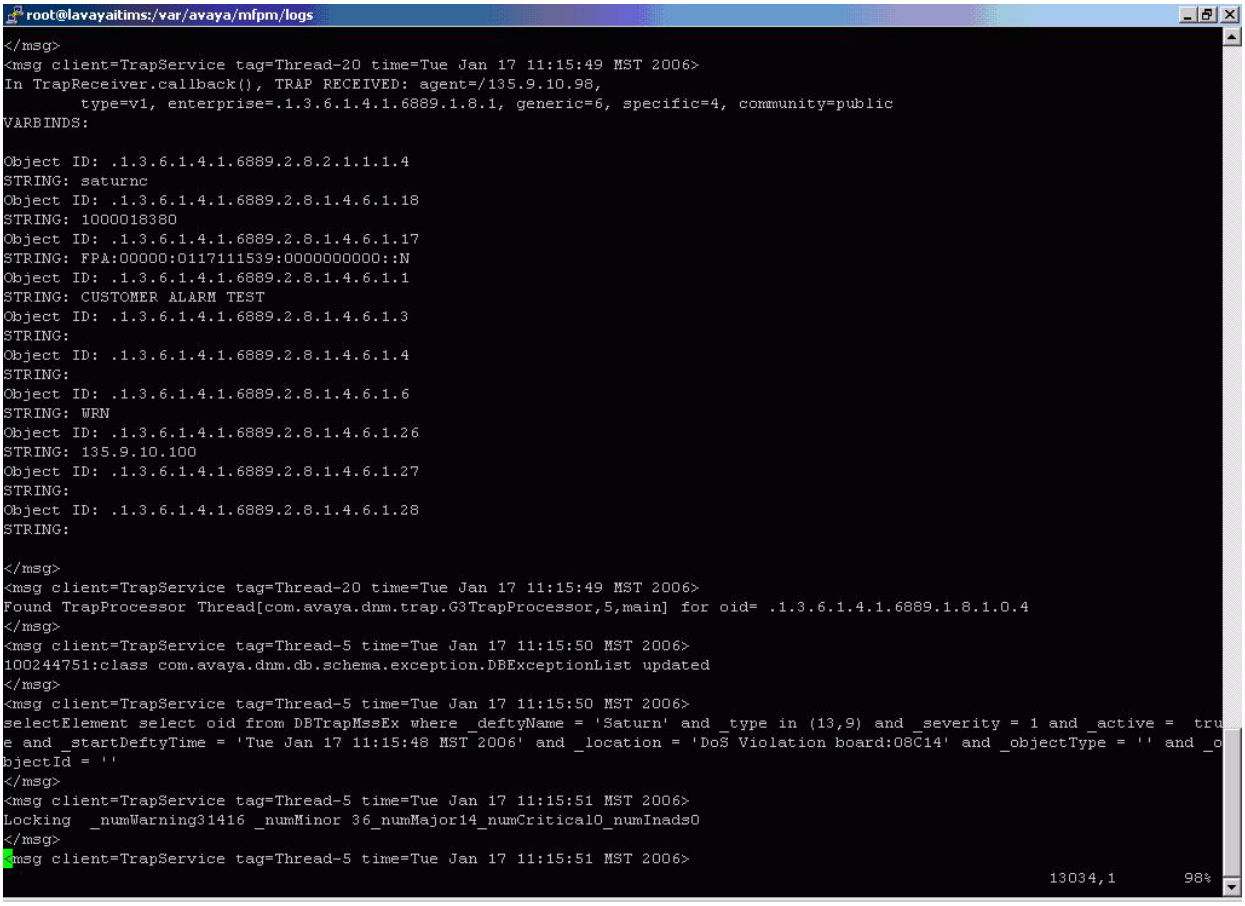
4. Click the **Generate Test Trap** button.

   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.



Chapter 6: Getting Started

This chapter describes how to:

- create logins and assign roles for FPM users
- start the Fault and Performance Manager client from a web browser
- configure alarm filters in FPM
- access the FPM online help
- exit the Fault and Performance Manager client from a web browser
- change your FPM password
- integrate FPM with an NMS

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

- **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.

IMD automatically installs and configures the following two default FPM roles:

- **FPMbrowse**

  The FPMbrowse role has the ReadOnly capability.

- **FPMadmin**

  The FPMadmin role the CreateReports, Admin, BusyoutRelease, Acknowledge, MovePN, Helper, and Assist capabilities.

You can assign these default roles to FPM users, or you can create and assign custom roles.

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

1. Create FPM roles.
2. Add FPM users, and assign FPM roles to the those 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 **>>**.

   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 a User and Assign an FPM Role on page 45.

Procedure 2: Add a User and Assign an FPM Role

Use this procedure to

- add a user account that can access FPM
- assign an FPM role to this user

To add a group of LDAP users, go to Procedure 3: Add an LDAP Group and Assign an FPM Role on page 46.

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.

    The Roles button appears next to the FPM check box.

12. Click **Roles**.

    The Assign FPM Roles to a User window appears.

13. Select the check box of each role you want to assign to this user. You can assign multiple FPM roles to a user.
14. Click **Save**.

    A page appears confirming that the role was updated successfully.

15. Click **OK**.
16. From the Allowed Elements box, select the element(s) this user will be able to access.

    To select multiple elements, press and hold the CTRL key, and then click on the appropriate elements.

17. Click **Add**.
18. Repeat Steps 2 through 17 for any other FPM users you want to add.

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

Procedure 3: Add an LDAP Group and Assign an FPM Role

Use this procedure to

- add an LDAP group that can access FPM
- assign an FPM role to this group

The settings you specify for an LDAP group will apply to all members of the group.

Perform the following steps:

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

   The LDAP Groups page appears.

2. Click **New Group**.

   The Add LDAP Group page appears.

3. In the Group Number box, enter the number for the LDAP group.
4. In the Group Description box, enter a description of this group.
5. If you want to prevent members of this group from logging in, select the **Group Disabled** check box.
6. Select the **FPM** check box.

   The Roles button appears next to the FPM check box.

7. Click **Roles**.

   The Assign FPM Roles to a User window appears.

8. Select the check box of each role you want to assign to this group. You can assign multiple FPM roles to a group.
9. Click **Save**.

   A page appears confirming that the role was updated successfully.

10. Click **OK**.
11. From the Allowed Elements box, select the element(s) this group will be able to access.

    To select multiple elements, press and hold the CTRL key, and then click on the appropriate elements.

12. Click **Add.**
13. Repeat Steps 2 through 12 for any other LDAP groups you want to add.

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

Starting the Fault and Performance Manager Client

To start the Fault and Performance Manager client:

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.

   The system displays the Integrated Management Launch Products page.

2. Click the **System Management** tab on the Integrated Management web page.
3. Click **Avaya Fault and Performance Manager**.

   The Java Plugin Security Warning appears.

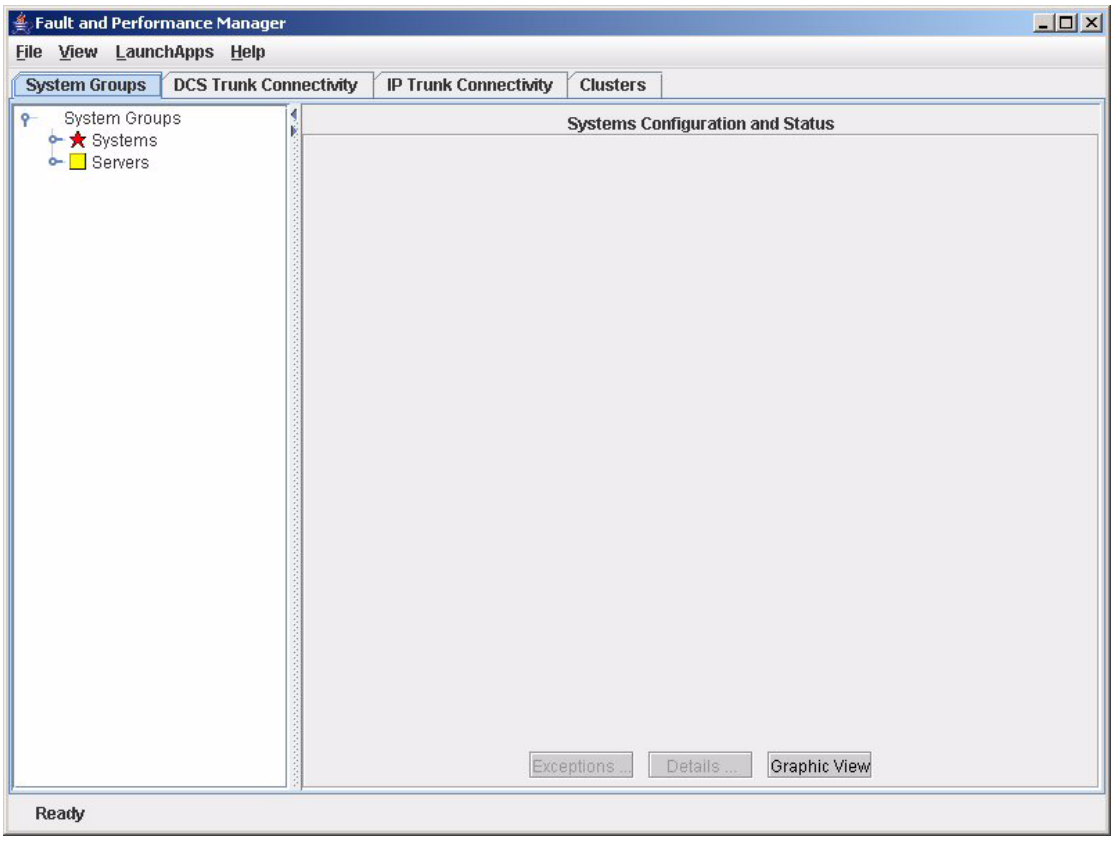
4. Click **Grant this Session**.

   The FPM Login dialog box appears.

5. In the Login Name box, enter your login. (All FPM logins and passwords are administered through the Integrated Management Database (IMD).)
6. In the Password box, enter your password.

7. Click **Login**.

   The Fault and Performance Manager window appears.

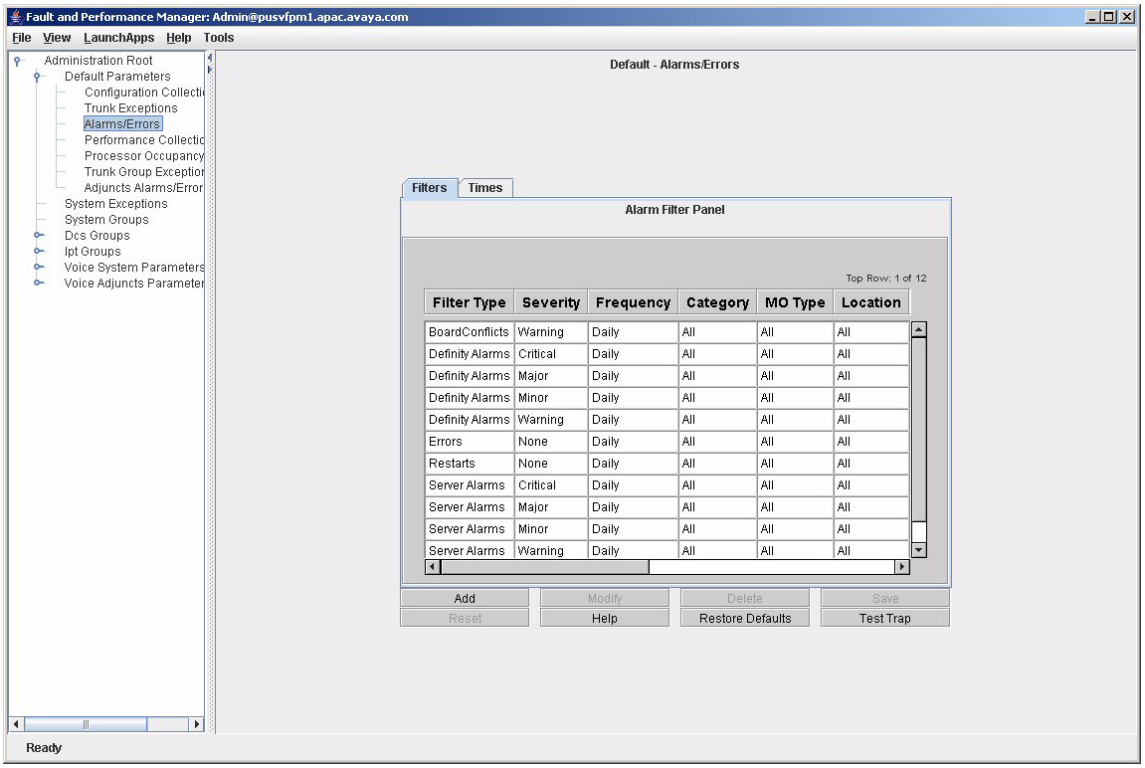


Configuring Alarm Filters

To configure alarm filters in Avaya Fault and Performance Manager:

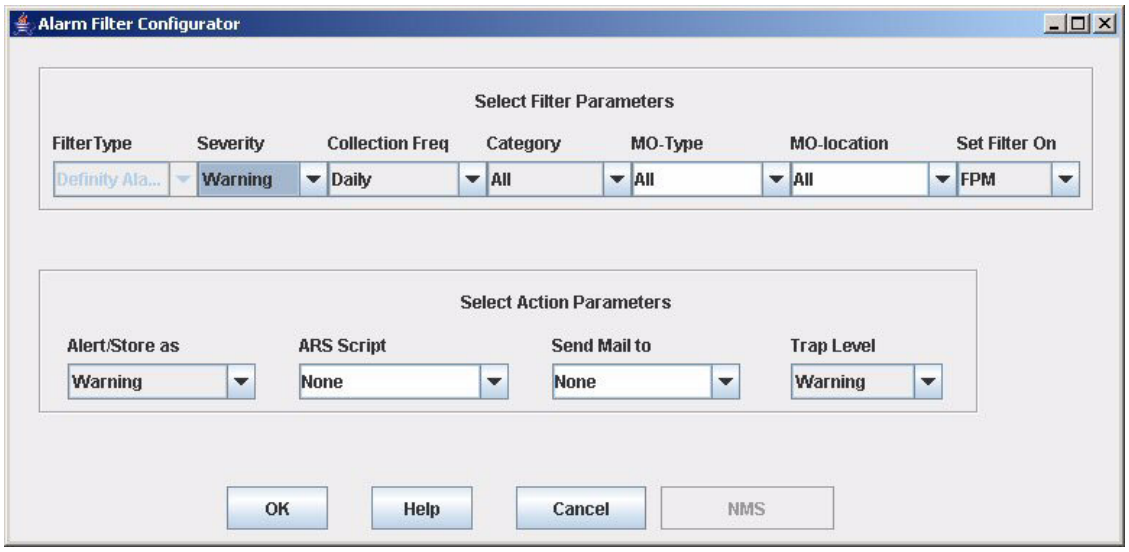
1. Access the Avaya Fault and Performance Manager window.
2. Click **File>Administration**.
3. When the administration panel appears, select **Default Parameters>Alarms/Errors**.

   The Alarms/Errors page appears.



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

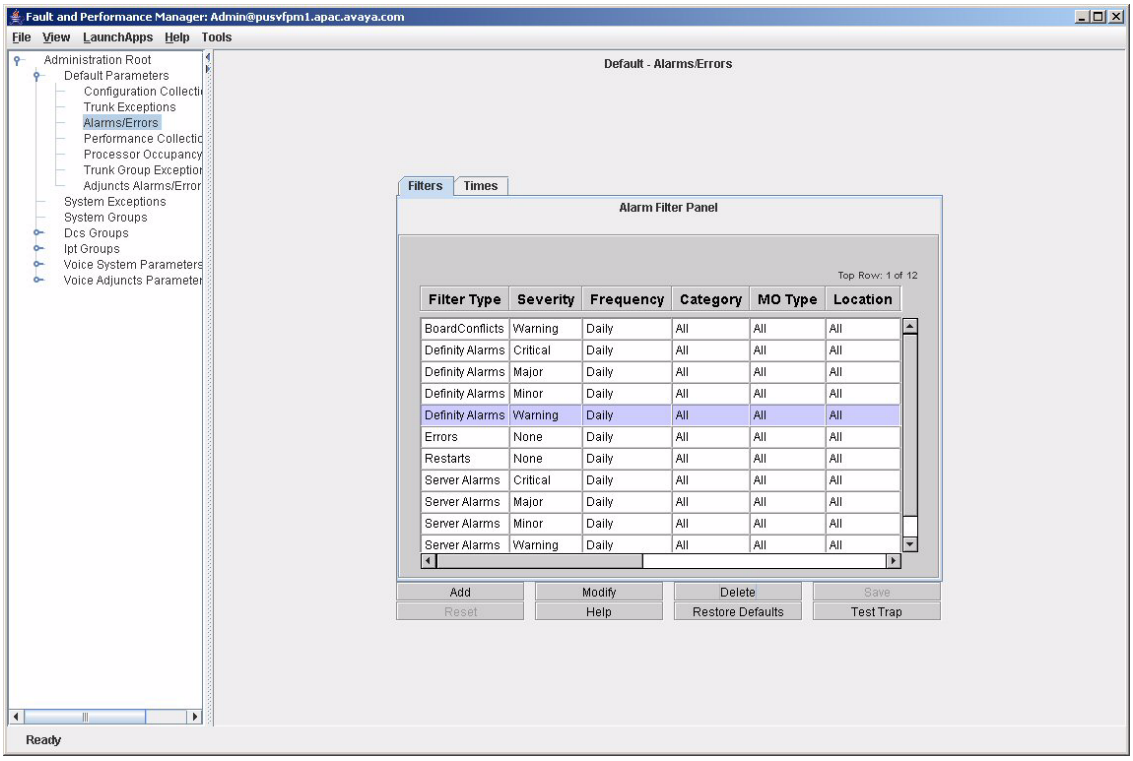
   The Alarm Filter Configurator page appears.



5. Select the appropriate parameters.

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

   The Alarms/Errors page appears.



7. Repeat Steps 2 through 6 for each alarm filter you want to change.
8. When finished, click the **Save** button.

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

   If an error occurs when Avaya Fault and Performance Manager attempts to send the alarm filter to Avaya Communication Manager, an error message will appear. Most errors that occur at this point are related to the SNMPv2c settings in IMD and Avaya Fault and Performance Manager not matching the SNMPv2c settings in Avaya Communication Manager. (See Procedure 3: Configure SNMP Agent on page 33.)

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

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

To exit the Fault and Performance Manager client, 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.

Integrating Fault and Performance Manager with an NMS

Fault and Performance Manager can send traps to any SNMP-based trap receiver. You must use Avaya Integrated Management Database to integrate Avaya Fault and Performance Manager with an NMS. See “Add an NMS Configuration” in *Avaya Integrated Management Release 5.0 Integrated Management Database Configuration,* 14-300039.

Glossary and Abbreviations

A

ATAC — See Avaya Technology and Consulting (ATAC) on page 7.

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 7.

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.

N

Network Management Server — This is the Windows server on which you can install Integrated Management applications.

Network Management System — A system that lets you monitor the health and status of devices on your data network.

S

SNMP — Simple Network Management Protocol.

System Management Server — This is the Linux server on which you install Fault and Performance Manager.

Index

Symbols

A

B

C

D

M

N

P

R

S

T

W