



Avaya Integrated Management
Release 3.1
Proxy Agent
Configuration

555-233-139
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

Preface	7
Purpose.	7
Prerequisites	7
Intended Audience.	7
Conventions Used in This Book	7
Tell Us What You Think!	8
Product Documentation	8
How to Access Books on the Web	9
Chapter 1: Resources and Notices.	11
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	16
Network Security.	16
Toll Fraud Security	16
Avaya Disclaimer	16
Toll Fraud Intervention	16
Chapter 2: Overview.	17
Product Description	17
Proxy Agent	17
Management Information Base (MIB).	17
Alarm-to-Trap Conversion	18
Enterprise Traps	18
Alarm Forwarding	18
Administration	19
User-Defined Script	19
Alarm Filtering	19
Reports	19
SNMP Authentication	19
Proxy Agent Security	20
Supported Systems	20

Contents

System Requirements	21
Hardware	21
Hardware Certification.	21
Software	21
Modems Supported	21
Configuration Overview	22
Chapter 3: Configuring Proxy Agent.	23
Customer Pre-Installation Tasks	23
Materials and Information	23
Configuring Proxy Agent	24
Understanding SNMP Access.	24
SNMP Traps	24
Running the Proxy Agent Configuration Script	24
Uninstalling Proxy Agent	27
Chapter 4: Accessing Proxy Agent.	29
Logging into Proxy Agent.	29
Starting Proxy Agent	30
Stopping Proxy Agent	30
Understanding the Main Menu	31
Understanding the Proxy Admin Screen.	32
Displaying the Proxy Admin Screen	32
Command Descriptions	32
Understanding the Proxy Agent Status Screen	34
Displaying the Proxy Agent Status Screen	34
Proxy Agent Status Screen Description	34
Field Descriptions	36
Chapter 5: Administering Proxy Agent via Integrated Management Database	39
Assigning Proxy Agent to an Element	39
Administering Network Managers	41
Chapter 6: Administering Alarm Services	45
Alarm Forwarding	45
Troubleshooting Alarm Problems	45
Understanding the Alarm Devices Screen	46
Field Descriptions	46

Specifying Alarm Devices	48
Building Custom Alarm Scripts	49
Script Directories	49
DEFINITY_ARS Script	49
Alarm Notification Options	49
AUDIX_ARS Script	50
CMS_ARS Script	51
CONVERSANT_ARS Script	52
Chapter 7: Administering Filter Sets	53
Definition	53
Default Filter-Set	53
Filter Set Commands	54
Pattern Matching	54
Boolean Operator	54
Alarm Severity	55
Day of Week	55
Time of Day	55
Examples of Filter Sets	56
Filter Set 1	56
Explanation	57
Filter Set 2	58
Explanation	58
Understanding the Filter Set Screen	59
Screen Layout	59
Field Descriptions	60
Specifying Filter Sets	64
Adding a Filter Set	64
Changing a Filter Set	66
Displaying the Filter Set Screen	68
Removing a Filter Set	68
Procedure	68
Chapter 8: Setting Preferences	71
Change User-Interface Screens	71
Display Software Version Screen	71
Field Descriptions	71
Change User-Interface Screen	72
Page 1 Field Descriptions	72
Setting the User-Interface Options	73

Contents

Chapter 9: Maintenance and Troubleshooting	75
Adding New Communication Devices	76
Changing Settings for SNMP Access	76
Viewing Alarm and Error Logs	76
Using Alarm Testing Tools	77
Trap Test Scripts.	77
Procedure	78
Chapter 10: Help Screens and Commands	81
Functions Window.	81
Commands and Hotkeys	82
Glossary and Abbreviations	85
Index	87

Preface

Purpose

This book explains how to configure Avaya Proxy Agent.

Prerequisites

Configuring Proxy Agent 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 configuration.

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

Intended Audience

This book is intended for workstation or network administrators.

Conventions Used in This Book

In this book, the following typographical conventions are used:

- Bold type for emphasis and for any information that you should type; for example: **save translation**.
- Courier font for any information that the computer screen displays; for example: `login`.
- 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.

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.
Proxy Agent Documentation Team
Room 3C-313
307 Middletown Lincroft Rd.
Lincroft, NJ 07738
USA

Fax:

Proxy Agent Documentation Team
+ 1 732 852-2469

E-mail:

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](#) on page 9 for instructions on how to view or download these books.

How to Access Books on the Web

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

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)

ATAC works with client teams to develop detailed solutions for connectivity to Avaya Communication Manager solutions. The ATAC also designs network configurations to support Proxy Agent and Avaya Fault and Performance Manager.

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

- Customers do not 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 products 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	http://www.avaya.com/support
Network Management Software Systems Support (NMSSS)	+1 800 237-0016
Communications, Solutions, and Integration (CSI) Group of Software Services	+1 800 730-9108, prompt 3
Integrated Management Product Team	Send email to: AIMtraining@avaya.com
Toll Fraud Intervention	+1 800 643-2353, prompt 1

Table 2: Avaya Internal Resources

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

Third-Party Resources

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

Table 3: Vendor web sites

Vendor	Web Sites
Hewlett-Packard	Main site: http://www.openview.hp.com
Red Hat Linux	Main site: http://www.redhat.com
Remedy	Main site: http://www.remedy.com Scroll down to: action request system
Vytek	Main site: http://www.vytek.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

Proxy Agent uses the standard security features on the Red Hat Linux operating system.

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 Proxy Agent 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 in [Customer-Accessible Resources](#) on page 14.

Chapter 2: Overview

Avaya Fault and Performance Manager together with Avaya Proxy Agent provides a complete solution to fault and performance management of Avaya voice elements in the stand alone mode as well as in an NMS integrated mode.

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

Product Description

Proxy Agent

Proxy Agent is a protocol conversion resource that operates on a Red Hat Linux platform.

Proxy Agent receives alarm notifications from supported systems via network or modem connections, converts these notifications into SNMP traps, and then transmits these SNMP traps to a network management application (such as Avaya Fault and Performance Manager and HP OpenView NNM). Proxy Agent can also relay the received alarm notifications to the Avaya Technical Service Center.

Management Information Base (MIB)

MIBs allow Proxy Agent to access management data from supported systems using SNMP. The MIB view consists of three groups:

- MIB-II group contains the standard SNMP MIB
- Communication Manager Feature Server MIB defines the management data that Proxy Agent collects and converts from the Operations Support System Interface (OSSI) protocol to SNMP
- CONVERSANT, AUDIX, Intuity, Intuity Interchange, and CMS MIB

Proxy Agent places the data extracted from supported systems into the appropriate MIB group. Then, the management application uses SNMP to access the information.

Note:

Proxy Agent does not support non-trap related portions of the G3MIB (Avaya Communication Manager MIB).

To find the ASN.1 format MIB definition files, use the Red Hat Linux path **/opt/avaya/mpa/appl_fls/agent**.

Alarm-to-Trap Conversion

Proxy Agent receives alarm notifications from each supported system that is administered on Proxy Agent.

To receive alarm notifications, you must administer the *alarm source* fields on the ALARM DEVICES screen in Proxy Agent. You must also administer the supported systems to send their alarm notifications to Proxy Agent's alarm receiver. Proxy Agent also receives alarm dispatches and close notifications from the Initialization and Administration System (INADS).

Enterprise Traps

Proxy Agent encapsulates the information contained in the alarm in an enterprise-specific trap and sends the trap to the set of administered network managers. The format of the created traps match the trap definitions in the MIB files for each of the supported systems. These ASN.1 MIB files are included with Proxy Agent and reside in the **/opt/avaya/mpa/appl_fls/agent** directory.

When sending Communication Manager Feature Server alarm traps, Proxy Agent refreshes health, alarm, error, and restart data. This refresh process allows the data to be current when the Network Management server requests the alarm information via SNMP.

Alarm Forwarding

You can administer the ALARM DEVICES screen on Proxy Agent to forward alarms to INADS. When a supported system generates an alarm, Proxy Agent adds a field that contains a sequence number to the end of the alarm stream. Proxy Agent stores the sequence number in the alarm logs.

Proxy Agent uses the sequence number for tracking purposes. Proxy Agent forwards the alarms and the sequence number to INADS or another Proxy Agent computer and includes the number as part of the alarm traps and alarm script arguments.

The Technical Services Organization (TSO) uses the sequence number to trace alarms and verify that the alarms received by Proxy Agent are successfully delivered to the TSO, INADS, and the Network Management server. You can also use this information for tracking in your third-party ticketing system.

Administration

You must activate the alarm forwarding feature on the ALARM DEVICES screen. You must also administer the supported systems as managed nodes via the Integrated Management Database.

User-Defined Script

Proxy Agent offers scripts that you can modify to (for example) have a third-party software application page you when Proxy Agent receives an alarm of a particular type. These scripts are located in the

/opt/avaya/mpa/agent directory. The scripts have not been set up. You must modify the scripts to meet your needs, as described in [Building Custom Alarm Scripts](#) on page 49.

Alarm Filtering

Proxy Agent provides an alarm filtering feature that lets you block the forwarding of certain alarms to INADS. You can create sets of filtering criteria on the FILTER SET screen and then apply the filter sets to all or individual systems.

When a managed node generates an alarm, Proxy Agent checks the filter set and compares each set of criteria for a match against the alarm. If Proxy Agent finds a match for any criteria, then it does not forward the alarm to INADS. If no match is found, then Proxy Agent forwards the alarm to INADS.

Reports

Proxy Agent reports any problems when trying to forward alarms to INADS. Alarm forwarding includes SNMP traps and the execution of the user-defined alarm scripts.

Proxy Agent creates two types of problem reports:

- Receipt of a negative acknowledgement (NAK) from INADS. This usually means that the product ID for the managed node has not been administered in INADS.
- Receipt of an invalid acknowledgment from INADS. This usually occurs if INADS drops the connection too soon, and Proxy Agent receives only part of the acknowledgement (ACK) needed to complete the “handshake” between the two systems.

SNMP Authentication

Proxy Agent provides minimal SNMP authentication through the community strings and node names that you administer in the Integrated Management Database. This authentication is based on a valid community string in the SNMP messages. SNMP uses the same mechanism to authorize the HP OpenView NMS access to the MIB.

Proxy Agent Security

Proxy Agent uses the standard Red Hat Linux login controls and permissions to authorize logins to Proxy Agent.

Supported Systems

Proxy Agent Release 3.1 supports SNMP V1 alarm traps for the following systems:

- DEFINITY ECS Releases 9.2 through 10.x
- Avaya Communication Manager Release 1.1 through 3.1. Proxy Agent supports Avaya Communication Manager Release 3.0 and later on Oryx-Pecos and Microsoft Windows platforms.
- Survivable Remote Processors (SRPs)
- MultiPoint Conferencing Unit (MCU) Release 7.2
- Avaya G350, G600, G700 Media Gateways
- Avaya S8100 Media Servers with CMC1 Media Gateway
- 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
- Modular Messaging Release 1.0 and later

Proxy Agent treats SRPs and MCUs as Communication Manager Feature Servers.

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 [Avaya Internal Resources](#) on page 14.

Hardware Certification

Avaya requires that Proxy Agent hardware must be Red Hat Enterprise Linux ES 3.0 or 4.0 or Red Hat Enterprise Linux AS 3.0 or 4.0 certified. For the Red Hat URL, see [Vendor web sites](#) on page 15.

 **CAUTION:**

Customers are solely responsible for the purchase, support, and maintenance of third-party hardware and software products that are required for this offer.

Software

Proxy Agent Release 3.1 operates on a Linux platform, running Red Hat Enterprise Linux ES 3.0 or 4.0 or Red Hat Enterprise Linux AS 3.0 or 4.0.

Modems Supported

The following alarm receiver devices are supported:

- AT&T 2224CEO
- AT&T 3710 Dataport
- AT&T 3715 Dataport Express
- U.S. Robotics Sportster 33.6
- U.S. Robotics Sportster 56K
- Paradyne Compusphere 3820

The following alarm sender devices are supported:

- AT&T 3710 Dataport
- AT&T 3715 Dataport Express
- U.S. Robotics Sportster 33.6
- U.S. Robotics Sportster 56K

Configuration Overview

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

1. Customers complete the customer pre-installation tasks that are specified in the Integrated Management Services Support Plan, which is accessible through the customer's client executive.
2. Customers communicate with CSI to verify server readiness, finalize technical details, and confirm implementation schedule.
3. Installers complete installation of Avaya Integrated Management described in *Avaya Integrated Management Release 3.1 System Management Installation and Upgrade*.
4. Installers complete [Configuring Proxy Agent](#) on page 24.
5. Installers complete [Administering Proxy Agent via Integrated Management Database](#) on page 39.
6. Installers complete [Administering Alarm Services](#) on page 45.
7. Installers complete [Specifying Filter Sets](#) on page 64.

Chapter 3: Configuring Proxy Agent

This chapter explains how to configure Proxy Agent. Some of the configuration steps are performed during installation.

Customer Pre-Installation Tasks

Before Proxy Agent can be installed, customers must complete several tasks that are defined in the Avaya Integrated Management Services Support Plan. Your client team can download the plan from the URL specified in [Table 2: Avaya Internal Resources](#) on page 14.

Materials and Information

You will need the following materials and information:

- Printed copy of this book
- Completed AIM001 form
- Root login and password for your Red Hat Linux system
- IP address of the Linux server and the Community name being used on the Fault and Performance Manager server
- Default login ID and password or ASG secret key for Communication Manager Feature Servers
- New password for the g3maadm login

Configuring Proxy Agent

Before you configure Proxy Agent, it is important that you understand the following information about SNMP access.

Understanding SNMP Access

When you configure Proxy Agent, you have the option to enable or disable SNMP access to Communication Manager Feature Server management data. By “SNMP access,” we mean SNMP Traps, which are explained in this section.

The Proxy Agent configuration script, which you will launch to configure Proxy Agent, contains prompts to enable or disable this feature. For Proxy Agent to work properly with Avaya Fault and Performance Manager (Fault and Performance Manager), you must enable SNMP Traps.

After Proxy Agent is installed, the only way to change settings for SNMP access is repeat the configuration process and select the appropriate options for SNMP access at that time.

SNMP Traps

You should enable SNMP Traps if the customer wants to receive traps from a large number of supported systems. If SNMP Traps are enabled, then Proxy Agent lets you administer up to **600** managed nodes for each instance of Proxy Agent. This option reduces the load on each instance of Proxy Agent and requires a less powerful computer to manage a larger number of supported systems.

You also have the option to disable SNMP Traps if Proxy Agent is only used for alarming.

Running the Proxy Agent Configuration Script

After installing Proxy Agent, complete the following steps:

1. Logon to the Linux system as *root*.
2. At the Linux prompt type `/usr/sbin/mpaconfig` 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:

```
The Avaya Proxy Agent has three options that allows you to enable or
disable the level of SNMP access to the managed nodes on your
network.
```

```
Option 1 enables only the SNMP alarm traps. By selecting this
function, you can reduce the load on the Proxy Agent and use a less
```

powerful server to manage a larger number of managed nodes. However, you cannot use the Avaya Fault and Performance Manager to manage your voice system.

Option 2 enables only the alarm processing function of the Proxy Agent and disables all SNMP functions. By selecting this option, the Proxy Agent can only receive, filter, and forward alarms to the Initialization and Administration System (INADS) and other designated locations.

Current setting is [SNMP Alarm Traps Only].

Please select one of the following options:

- 1) SNMP Alarm Traps Only
- 2) Alarm Processing Only (No SNMP Support)

Enter your selection [1] :

3. Select 1 or 2 and press ENTER.

Selecting 1 will enable only SNMP alarm traps. Selecting 2 will disable SNMP access. Then, the system displays the appropriate message, including:

The Avaya Proxy Agent allows you to configure the maximum number of Managed Nodes with SNMP access and the maximum number of simultaneous connections allowed to those Managed Nodes. These options allow the Proxy Agent to be tuned based on system resources available.

The current setting for number of Managed Nodes allowed with SNMP access is 150. Do you wish to change that setting? [n]/y:

The Avaya Proxy Agent allows you to configure the maximum number of Managed Nodes with alarming support. This option allows the Proxy Agent to be tuned based on system resources available.

The current setting for number of Managed Nodes with alarming support is 600. Do you wish to change the setting? [n]/y:

4. To continue without changing the current setting, type n.

Then, the system displays:

The current setting for number of simultaneous connections allowed is 30. Do you wish to change that setting? [n]/y:

5. To continue without changing the current setting, Type n.

The system prompts you to enter a new g3maadm password.

Configuring Proxy Agent

6. Type and retype a new `g3maadm` password, pressing **ENTER** after each entry. The system administers the `g3maadm` login and then displays the message:

```
passwd: all authentication tokens updated successfully.
```

The system displays the first device name from the serial I/O subsystem and the device function prompt for that device:

```
UNIX device name: /dev/ttyxxx:
```

```
Select the function for this device:
```

```
[R] Receive Alarms
```

```
[S] Send Alarms
```

```
Or, select one of the options below:
```

```
[N] Next Device (skip this one)
```

```
[X] Exit Modem Setup and continue the installation
```

```
Enter the device function or another option default=R:
```

7. At the prompt, execute one of the options below:
 - a. If the device name is on the AIM001 form, then type the letter that matches the *function* for this device and press **ENTER**.

Depending on which letter you enter in this step, the system displays a different prompt. The prompt below is an example of the maintenance function.

On entering **R**, the following options are displayed:

```
Alarm Receiver Device Type:
```

```
[1] 3710 AT&T Dataport
```

```
[2] 3715 AT&T Dataport Express
```

```
[3] AT&T 2224CEO
```

```
[4] US Robotics Sportster 33.6 Kbps
```

```
[5] US Robotics Sportster 56K Faxmodem
```

```
Or select the option below:
```

```
[N] Next Device (Skip This One)
```

```
Enter the device type or another option:[default=5]
```

On entering S, the following options are displayed:

Alarm Sender Device Type:

[1] 3710 AT&T Dataport

[2] 3715 AT&T Dataport Express

[3] US Robotics Sportster 33.6 Kbps

[4] US Robotics Sportster 56K Faxmodem

Or select the option below:

[N] Next Device (Skip This One)

Enter the device type or another option:[default=4]

- b. If the device name is not on the AIM001 form, then type **N** and press **ENTER**.

If you choose **N**, the system displays the device name and function prompt for the next device in the I/O subsystem.

8. (As appropriate) Repeat Step [7](#) for each device.

9. To exit the Modem Setup program at a device function prompt, type **X** and press **ENTER**.

The system displays the message:

```
Done setting up Devices.
```

Finally, the system displays the message:

```
Reboot the machine by executing reboot.
```

10. At the Linux prompt, type **reboot** and press **ENTER**.

The system reboots the computer, which takes several minutes. You must reboot the system before you administer Proxy Agent. The system displays the Linux login prompt.

11. Go to Step [5](#) of the [Configuration Overview](#) on page 22.

Uninstalling Proxy Agent

Only root users should uninstall Proxy Agent. Please refer to *Avaya Integrated Management Release 3.1 System Management Installation and Upgrade* for complete instructions.

Chapter 4: Accessing Proxy Agent

This chapter explains how to log in to Proxy Agent from the Red Hat Linux prompt and how to access various Proxy Agent menus and screens. This chapter is primarily for new Proxy Agent users.

Logging into Proxy Agent

Complete the following procedure to log in.

1. At the login prompt, type **g3maadm** and press **ENTER**.

The system displays the password prompt.

2. At the password prompt, type the g3maadm password and press **ENTER**.

3. Open a terminal window.

4. At the Linux prompt, type **proxy** and press **ENTER**.

The system displays the Proxy Agent MAIN MENU.

5. At the command line, enter one of the following commands. These commands are explained in the section, [Understanding the Main Menu](#) on page 31.

- To display the Administration screens, type **proxy-admin** and press **ENTER**.
- To display the Communication screens, type **communication** and press **ENTER**.
- To display the Configuration screens, type **configuration** and press **ENTER**.

The system displays the selected application screen.

Starting Proxy Agent

Complete the following procedure to start a Proxy Agent connection.

1. For this procedure, you must start by typing **proxy-admin** and pressing **ENTER** in Step [5](#) of [Logging into Proxy Agent](#) on page 29.

Doing so displays the PROXY ADMIN screen.

2. In the command line, type **start proxy-agent** and press **ENTER**.

The system displays:

```
THIS COMMAND WILL START THE PROXY AGENT
```

```
Do you wish to continue? Yes No
```

3. Press **ENTER**.

The system starts Proxy Agent. Then, the system displays the PROXY ADMIN screen with the confirmation message:

```
Command completed successfully.
```

4. Display the STATUS screen to verify that Proxy Agent is active. See [Understanding the Proxy Agent Status Screen](#) on page 34.

Stopping Proxy Agent

As explained in the section, [Understanding the Proxy Admin Screen](#) on page 32, you must stop Proxy Agent before you can enter an **add**, **remove**, or **change** command. You do not have to stop Proxy Agent when entering a **display** command.

 **CAUTION:**

When you stop Proxy Agent, the existing connections to the administered nodes are dropped.

Complete the following procedure to stop a Proxy Agent connection.

1. For this procedure, you must start by typing **proxy-admin** and pressing **ENTER** in Step [5](#) of [Logging into Proxy Agent](#) on page 29.

Doing so displays the PROXY ADMIN screen.

2. In the command line, type **stop proxy-agent** and press **ENTER**.

The system displays the prompt:

```
Do you wish to continue? Yes No
```

3. Press **ENTER**.

The system stops Proxy Agent and then displays the PROXY ADMIN screen with the confirmation message:

```
Command completed successfully.
```

4. Display the STATUS screen to verify that Proxy Agent is not active. See [Understanding the Proxy Agent Status Screen](#) on page 34.

Understanding the Main Menu

The Proxy Agent MAIN MENU lists the commands that you use to access Proxy Agent screens. The following table describes the commands on the Proxy Agent MAIN MENU.

Table 4: Proxy Agent MAIN MENU

Command	Description
communication	Accesses the Communication application and displays the COMMUNICATION MANAGER screen. Users can manually connect and disconnect a Proxy Agent to and from managed nodes.
configuration	Accesses the Configuration application. This application contains two commands: <ul style="list-style-type: none"> ● display software-version to view the DISPLAY SOFTWARE VERSION screen ● change user-interface to edit the CHANGE USER_INTERFACE screens (4 pages) Refer to Setting Preferences on page 71.
proxy-admin	Accesses the PROXY ADMIN menu. Refer to Understanding the Proxy Admin Screen on page 32.
exit	Closes the Proxy Agent MAIN MENU.
unix-shell	Accesses the Linux prompt.

Understanding the Proxy Admin Screen

The PROXY ADMIN menu lists the commands that you use to access Proxy Agent administration screens and to start and stop Proxy Agent.

Displaying the Proxy Admin Screen

Complete the procedure below to display the PROXY ADMIN screen.

1. Complete [Logging into Proxy Agent](#) on page 29.
2. In Step [5](#), type **proxy-admin** and press **ENTER**.

Doing so displays the PROXY ADMIN screen.

Command Descriptions

The following table describes the commands on the PROXY ADMIN screen. You must have a *g3maadm* login to execute these commands and administer Proxy Agent.

Table 5: PROXY ADMIN screen

Command	Description
add	Accesses the FILTER SET screen in the “add” mode. You create the alarm filtering criteria for a new filter set with this command. NOTE: You must STOP Proxy Agent before executing the add command. Refer to Chapter 7: Administering Filter Sets .
remove	Accesses the FILTER SET screen in the “remove” mode. Users can delete existing alarm filters with this command. NOTE: You must STOP Proxy Agent before executing the remove command. Proxy Agent executes one of the following options: <ul style="list-style-type: none">● Deletes the filter set if it is not assigned to any managed node● Replaces the filter set with the <i>default</i> filter if the filter is assigned to managed nodes Refer to Chapter 7: Administering Filter Sets .

1 of 2

Table 5: PROXY ADMIN screen (continued)

Command	Description
change	<p>Accesses the administration screens. The change command allows users to edit the selected screen.</p> <p>NOTE: Users must STOP Proxy Agent before executing the change command.</p> <ul style="list-style-type: none"> ● change alarm-devices See Understanding the Alarm Devices Screen on page 46. ● change filter-set See Understanding the Filter Set Screen on page 59.
display	<p>Shows the administration screens and the STATUS screen in the view-only mode. The display command does not allow users to change the screens.</p> <p>NOTE: You do not have to STOP Proxy Agent before executing the <i>display</i> command.</p> <ul style="list-style-type: none"> ● display alarm-devices ● display filter-set ● display status -- See Displaying the Proxy Agent Status Screen on page 34.
start	<p>Initiates an Proxy Agent connection to the managed nodes.</p> <p>See Starting Proxy Agent on page 30.</p>
stop	<p>Drops the Proxy Agent connection to the managed nodes.</p> <p>See Stopping Proxy Agent on page 30.</p>
quit	<p>Closes the PROXY ADMIN screen and displays the Proxy Agent MAIN MENU.</p>
2 of 2	

Understanding the Proxy Agent Status Screen

Display the STATUS screen each time you start or stop Proxy Agent so that you can:

- Verify that the Proxy Agent connection is active (or inactive)
- View the status of the Alarm Forwarding feature
- View the connection statistics for the voice system and MCU managed nodes

Displaying the Proxy Agent Status Screen

Complete the following procedure to display the STATUS screen.

1. In Step 5 of [Logging into Proxy Agent](#) on page 29, type **proxy-admin** and press **ENTER**.
Doing so displays the PROXY ADMIN screen.
2. In the command line, type **display status** and press **ENTER**.
Doing so displays the STATUS screen.
3. Press **Ctrl-X** to exit the screen.
The system closes the STATUS screen and displays the PROXY ADMIN screen.

Proxy Agent Status Screen Description

The STATUS screen is view-only and contains the following information:

- Status of Proxy Agent
- Alarm forwarding state
- Node name and state

Note:

To view the status of Proxy Agent using a URL, type:

http://proxy-name/cgi-bin/mpa/Status.sh

(**proxy-name** should be the fully-qualified domain name or IP address of the Proxy Agent computer)

The STATUS screen does not display any connection statistics for the following managed nodes. Proxy Agent supports only alarm handling for these products.

- DEFINITY AUDIX
- Intuity AUDIX
- Intuity Interchange

- Call Management System (CMS)
- CONVERSANT

Proxy Agent supports modem connectivity to the following products:

- DEFINITY AUDIX
- Intuity AUDIX
- Intuity AUDIX LX
- S8100 Audix
- Modular Messaging
- CMS
- Conversant
- Interchange
- Message Networking
- MCU

Figure 1: STATUS screen

display status		(PROXY ADMIN)		Page 1		
STATUS						
Proxy Agent State: active			Alarm Forwarding: ok			
Node Name	State	Last Connection	Attempts	Requests	Errors	
Con Type	Timeout	Last Used	Connects	Responses	Counters	Reset
ecs1	up	12/01/99 14:37:48	1	85	0	
static		12/01/99 15:08:51	1	85		
g3	idle		0	0	0	
dynamic	60		0	0		12/05/99 11:03:55

Command successfully completed, select Cancel to return to the menu

Field Descriptions

The following table describes each of the columns in the STATUS screen. Several of the columns contain two types of data.

Table 6: STATUS screen

Column	Description
Proxy Agent State	<p>Identifies the current activity status of Proxy Agent:</p> <ul style="list-style-type: none"> ● active -- The Proxy Agent has been started ● not active -- The Proxy Agent has been stopped
Alarm Forwarding	<p>Identifies the current state of the alarm forwarding feature. The alarm forwarding feature is active only if the user has administered the ALARM DEVICES screen. Users can turn-off alarm forwarding for individual managed nodes from the Integrated Management Database.</p> <p>The states include:</p> <ul style="list-style-type: none"> ● ok -- Alarm forwarding is active and functioning ● failed -- Alarm forwarding is active, but is not functioning ● other -- Identifies one of the following conditions: <ul style="list-style-type: none"> - Proxy Agent is not active - Alarm forwarding feature is not turned on
Node Name	<p>Identifies the name of the managed node that is associated with Proxy Agent.</p>
Con Type	<p>Identifies the type of connection. It can be one of the following:</p> <ul style="list-style-type: none"> ● static (continuous connection) ● dynamic (temporary connection on an as-needed basis)
State	<p>Identifies the current status of Proxy Agent's connection to a managed node as off. (The connection will always be turned off.)</p>

Table 6: STATUS screen (continued)

Column	Description
Last Used	The date and time of the last successful data retrieval.
Data Requests	The number of requests for data since the counter was reset to zero.
Data Responses	The number of successful responses to data requests since the counter was reset to zero.
Errors	The number of errors that occurred during data requests since the counter was reset to zero.
Counters Reset	The date and time the counter was reset to zero.

2 of 2

Chapter 5: Administering Proxy Agent via Integrated Management Database

This section describes how to

- assign Proxy Agent to an element (such as a voice system or a messaging system) via the Integrated Management Database
- administer network managers via the Integrated Management Database

Assigning Proxy Agent to an Element

To assign Proxy Agent to an element (such as a voice system or a messaging system), perform the following steps:

1. Log into the Integrated Management Database.
2. Click **Elements** in the navigation panel.
The Elements page appears.
3. Click **Edit** for the element to which you want to assign Proxy Agent.
The Edit Element page appears.
4. If you want to use Proxy Agent with a voice system:
 - a. From the Proxy box, select the Proxy Agent system you want to use.
 - b. In the Login box, enter the SAT login for the voice system.
 - c. In the Password box, enter the password for the SAT login.
 - d. In the Re-enter Password box, re-enter the password for the SAT login.
 - e. In the IP Address box, enter the SAT IP address.
 - f. In the Telnet Port box, enter the SAT port number.
 - g. If the system uses ASG:
 1. In the ASG Key box, enter the ASG key.
 2. In the Re-enter ASG Key box, re-enter the ASG key.
 - h. From the Sub Map Type box, select the sub map.
 - i. If you set the Sub Map Type to **USA** or **Custom**, enter the name of the sub map in the Sub Map Name box.
 - j. If you want to forward alarms, select the **Forward Alarms** check box.

Administering Proxy Agent via Integrated Management Database

k. If you want to assign a filter set, enter the name of the filter set in the Filter Set Name box. A filter set is a collection of filter records. A filter record contains one or more of the following types of filtering criteria:

- Pattern matching - can include pattern files and character strings
- Alarm severity
- Day of the week
- Time of day

The Filter Set feature allows you to create filters that Proxy Agent applies to alarms in order to block the forwarding of certain alarms to the Initialization and Administration system (INADS).

5. If you want to use Proxy Agent with an element that is not a voice system:

- a. From the Proxy box, select the Proxy Agent system you want to use.
- b. In the IP Address box, enter the IP address of the system.
- c. In the Telnet Port box, enter the port number of the system.
- d. From the Sub Map Type box, select the sub map.
- e. If you set the Sub Map Type to **USA** or **Custom**, enter the name of the sub map in the Sub Map Name box.
- f. If you want to forward alarms, select the **Forward Alarms** check box.
- g. If you want to assign a filter set, enter the name of the filter set in the Filter Set Name box. A filter set is a collection of filter records. A filter record contains one or more of the following types of filtering criteria:
 - Pattern matching - can include pattern files and character strings
 - Alarm severity
 - Day of the week
 - Time of day

The Filter Set feature allows you to create filters that Proxy Agent applies to alarms in order to block the forwarding of certain alarms to the Initialization and Administration system (INADS).

6. When finished, click **Update**.

7. Repeat Steps 3 through 6 for any other elements to which you want to assign Proxy Agent.

Administering Network Managers

To administer a network manager, perform the following steps:

1. Log into the Integrated Management Database.
 2. Click **Elements** in the navigation panel.
The Elements page appears.
 3. Click **New Element**.
The Add Element page appears.
 4. In the Element Name box, enter the name of the element.
 5. From the Element Type box, select **Integrated Mgmt**.
 6. In the Group box, enter the group for the system.
 7. In the Product Id box, enter the product ID for the system.
 8. In the Note box, enter any notes you want for the system. This box is a “note pad” in which you can enter up to 255 characters.
 9. From the Location box, select the location for the system.
 10. From the Platform Type box, select **Proxy Agent**.
 11. In the Functional Location box, enter the location.
 12. Select the **Active** check box if you want the new element to be activated when you are finished adding it. (This check box is enabled by default.)
 13. From the Proxy box, select the Proxy Agent system you want to use.
 14. Select the **SNMPv1 Enable** check box if you want to enable SNMPv1.
 15. In the SNMPv1 Write box, enter Proxy Agent’s set community string. The NMS uses this to validate SNMP set requests. Valid options are
 - g3pa (default)
 - Any name that identifies a private network
-  **CAUTION:**
You must administer the name of the set community string to match the set community string on the NMS. The name must match on both systems, otherwise the set request will fail.
16. In the SNMPv1 Read box, enter Proxy Agent’s SNMP get community string. The NMS uses this to validate SNMP get requests. Valid options are
 - public (default)
 - Any name that identifies a private network

 **CAUTION:**

You must administer the name of the get community string (public or private) to match the get community string on the NMS. The name must match on both systems, otherwise the get request will fail.

17. From the Default Map Type box, select the default submap. This is the map that you want to use to view managed nodes and their associated instances of Proxy Agent. You may want to select a default submap if you think that you will want to view most of the managed nodes in the same way. If you select a default, you will not have to specify a submap for each individual node using the MANAGED NODES screen. Any new managed nodes that you add will automatically use the default map, unless you specify otherwise (for that individual managed node) using the MANAGED NODES screen. Any change you specify in the MANAGED NODES screen overrides the default submap selection for that managed node only.

Valid options are

- **Generic** (default)

Select the **generic** submap to view all the managed nodes and Proxy Agent computers on one submap.

- **USA**

Select the **usa** submap to show the location of managed nodes in the U.S. The associated state submap shows managed nodes in that state.

- **Custom**

Select the **Custom** submap to organize managed nodes by categories, such as private networks, regions, functions, or international locations.

Use the associated submap name (Default Map Name) to identify groups or locations within the categories, such as:

- Private Network may consist of the Lab and Testing groups
- Regions may consist of North, East, South, and West groups
- Functions may consist of Telemarketing, Sales, and Customer Service groups
- International locations may consist of Africa, Spain, and Greece groups

18. If you set the default map type to **USA** or **Custom**, enter the name of the submap in the Default Map Name box.

19. In the Network Manager 1 IP box, enter the IP address of the first NMS network manager. Valid options are

- Asterisk (*)

The asterisk allows access to all NMS network managers. The asterisk is not valid if you want to use Receive Traps access.

- IP address of the NMS in dot format (for example, 126.1.205.86)

20. From the drop-down list box associated with the Network Manager 1 IP box, select the type of access the network manager has to Proxy Agent. Valid options are:

- Read/Write

Allows the network manager to read and write data to the MIB.

Note:

Fault and Performance Manager requires read/write access.

- Read Only

Allows the network manager only to read data. The network manager cannot change MIB objects that are set with the SNMP SET command.

- Receive Traps

Allows the network manager to receive SNMP traps from Proxy Agent.

Note:

Fault and Performance Manager requires SNMP trap reception.

21. Repeat Steps 19 and 20 for each network manager.

22. When finished, click **Add**.

Chapter 6: Administering Alarm Services

By “administering alarm services,” we mean specifying the means by which supported systems will send their alarms to the Proxy Agent computer, and the means by which the Proxy Agent computer will receive them.

The ALARM DEVICES screen lets you specify default sending and receiving devices. In the past, “alarm devices” were modems. More recently, “alarm devices” may also include TCP/IP connections.

Proxy Agent receives alarms only from the managed nodes listed below:

- DEFINITY ECS, MCU, and Avaya S8100 Media Server with Avaya G600 Media Gateway systems
- Avaya Communication Manager
- DEFINITY AUDIX
- Intuity AUDIX
- Intuity AUDIX LX
- Intuity Interchange
- S8100 AUDIX
- Call Management System (CMS)
- CONVERSANT system
- Modular Messaging
- Message Networking

By default, Proxy Agent forwards the alarms that it receives from managed nodes to INADS. However, you can edit the alarm destination fields to forward the alarms to a device that is supported by the current release of Proxy Agent.

Alarm Forwarding

The alarm forwarding feature is active only if at least one alarm sender has been specified. You can turn alarm forwarding on and off for individual managed nodes on page **A** of the MANAGED NODES screen.

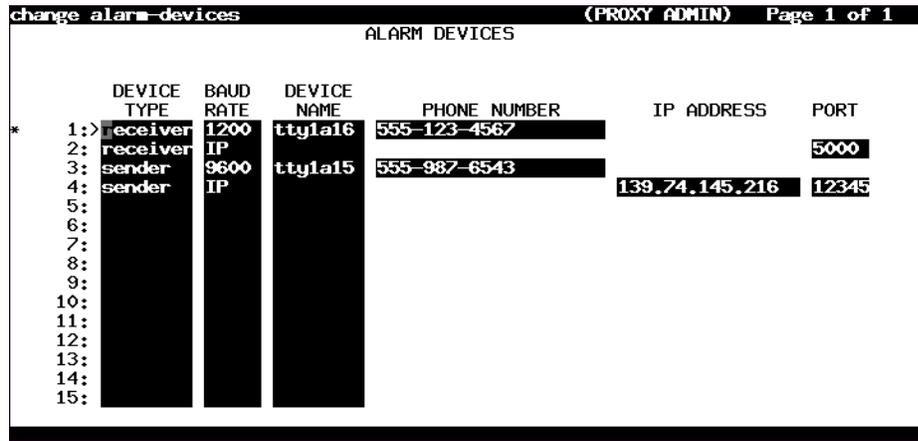
Troubleshooting Alarm Problems

To troubleshoot alarm problems, refer to [Viewing Alarm and Error Logs](#) on page 76.

Understanding the Alarm Devices Screen

Use the ALARM DEVICES screen to enter up to 15 alarm devices that will receive alarms from managed nodes or to forward alarms to INADS.

Figure 2: Alarm Devices screen



Field Descriptions

The table below describes the fields on the ALARM DEVICES screen.

Table 7: Alarm Devices Screen

Field	Description
DEVICE TYPE receiver sender	Identifies the device as a receiver or sender of alarms. Default: Blank Field size: 8 characters
BAUD RATE 1200 2400 9600 19200 IP	Specifies the baud rate for modem connections. Enter IP for TCP/IP connections. Default: Blank Field size: 5 characters

1 of 2

Table 7: Alarm Devices Screen (continued)

Field	Description
DEVICE NAME ttyxxxx	Specifies the tty device used to receive or send alarms. Required for serial alarm devices (baud rate field contains baud rate information). Leave blank if baud rate field is "IP." Default: Blank Field size: 8 characters
PHONE NUMBER	Specifies the phone number used to receive alarms when device type is "receiver" or the phone number to forward the alarm to when device type is "sender." Appears when the baud rate field contains baud rate information, and does not appear if the baud rate field is "IP." If the baud rate field is not IP, and the device type is "sender", the phone number default is the INADS phone number. Default: blank Field size: 20 characters
IP ADDRESS	Contains the IP address used to send alarms over IP. This field is turned on when the device type is "sender" and the baud rate is "IP." Default: blank Field size: 16 characters
PORT	Contains the port number used to receive or send alarms over IP. The field is turned on when the baud rate is "IP." Default: blank Field size: 5 characters
2 of 2	

Specifying Alarm Devices

Complete the procedure below to administer the ALARM DEVICES screen to receive and forward alarms. Refer to the AIM001 form for the information that you need to complete the fields on the screen.

1. Access the PROXY ADMIN menu.
2. Stop Proxy Agent if it is running ([Stopping Proxy Agent](#) on page 30).
3. In the command line on the PROXY ADMIN menu, type **change alarm-device** and press **ENTER**.

The system displays the ALARM DEVICES screen.

4. In the DEVICE TYPE column, specify whether the alarm device is a receiver or a sender.
5. In the BAUD RATE column, Enter **1200, 2400, 9600, 19200**, or enter **IP** for TCP/IP connections.
6. In the DEVICE NAME column, identify the tty device to use for receiving or sending alarms.
If the BAUD RATE field is **IP**, leave this field blank.
7. In the PHONE NUMBER column, enter the phone number used to receive or send alarms.
This field appears only if a numeric baud rate is entered in the BAUD RATE field. Enter **1-800-535-3573** to forward alarms to INADS if the DEVICE TYPE field is **sender**.
8. In the IP ADDRESS column, enter the IP address used to send alarms over IP.
This field appears only if the DEVICE TYPE field is sender and the BAUD RATE field is **IP**.
9. In the PORT field, enter the port number to use to receive and send alarms over IP.
The BAUD RATE field must be **IP**.
10. Press **Ctrl-E** to submit the changes.
The system saves the changes and displays the PROXY ADMIN screen.
11. Go to Step [7](#) of "[Configuration Overview](#) on page 22."
12. Restart Proxy Agent ([Starting Proxy Agent](#) on page 30).

Building Custom Alarm Scripts

Proxy Agent calls a script, located in the `/opt/avaya/mpa/agent` directory, based on the supported system. The arguments that are passed to the script match the arguments that are sent to corresponding scripts on the System Management server. The scripts that are included in Proxy Agent are not set up. You must modify them to meet your needs.

Script Directories

The following sample scripts are located in the `/opt/avaya/mpa/agent` directory:

- `DEFINITY_ARS`
- `AUDIX_ARS`
- `CMS_ARS`
- `CONVERSANT_ARS`

DEFINITY_ARS Script

Alarm Notification Options

System administrators can use the pager or E-mail features or edit the scripts to enable third-party products.

Proxy Agent looks for the **DEFINITY_ARS** script when Proxy Agent receives an alarm from the managed nodes listed below:

- Communication Manager Feature Servers
- MCU
- Avaya S8100 Media Servers with Avaya G600 Media Gateway
- Avaya S8100 Media Server with CMC1 Media Gateway
- Avaya Communication Manager

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

Alarm notification values:

1. System name
2. Error description
3. New status severity

Administering Alarm Services

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

Proxy Agent looks for the **AUDIX_ARS** script when Proxy Agent receives an alarm from the managed nodes listed below:

- DEFINITY AUDIX
- Intuity AUDIX
- Intuity Interchanges

Then Proxy Agent calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then Proxy Agent 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 (DEFINITY for 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

Proxy Agent looks for the **CMS_ARS** script when Proxy Agent receives an alarm trap from the Call Management System (CMS).

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

Administering Alarm Services

6. Old status severity
7. Product type
8. Version
9. ID value
10. Number
11. Name

CONVERSANT_ARS Script

Proxy Agent looks for the **CONVERSANT_ARS** script when Proxy Agent receives an alarm trap from the CONVERSANT system

Then Proxy Agent calls the script and passes the values listed below to the alarm notification program. If a value is not defined, then Proxy Agent 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 7: Administering Filter Sets

Proxy Agent provides an alarm filtering feature that allows you to block the forwarding of certain alarms. You can create sets of filtering criteria on the FILTER SET screen and then apply the filter set to all or individual systems on the MANAGED NODES screen.

The Filter Set feature lets you create filters that Proxy Agent applies to alarms in order to block the forwarding of certain alarms to the Initialization and Administration System (INADS). You can create filtering criteria on the FILTER SET screen and then apply the filter sets to all or individual systems on the MANAGED NODES screen.

When a managed node generates an alarm, Proxy Agent compares each record in the filter set for a match against the alarm. If Proxy Agent finds a match for any filter record, then it does not forward the alarm to INADS. If Proxy Agent does not find a match, then it forwards the alarm to INADS.

Definition

A filter set is a collection of filter records. A filter record contains one or more of the following types of filtering criteria:

- Pattern matching -- can include pattern files and character strings
- Alarm severity
- Day of the Week
- Time of Day

For each filter set, you can create a maximum of **12** filters that contain all or any combination of the four types of filtering criteria. An alarm must match the criteria specified in the filter record before Proxy Agent blocks the alarm.

Default Filter-Set

When you install Proxy Agent, the system supplies a blank default filter set. You can implement one of the options below to set up the system default for alarm filtering:

- Leave the default filter set blank. The system default would be that Proxy Agent forwards alarms without filtering.
- or
- Add filtering criteria to the default filter set. The system default would be the criteria in the default filter set.

Administering Filter Sets

In either event, Proxy Agent applies the default filter set to all alarms unless the user executes one of the options below for individual managed nodes:

- Selects a different filter
- or
- Selects no filter set

You must select one of the alarm filtering options since Proxy Agent does not allow the default filter set to be removed.

Filter Set Commands

You can administer or view the FILTER SET screen from the PROXY ADMIN menu by executing the commands listed below:

- **add filter-set** to create new filter sets
- **change filter-set** to modify existing filter sets
- **remove filter-set** to delete filter sets, except the default filter
- **display filter-set** to view filter sets

Pattern Matching

On the FILTER SET screen, you can enter two types of pattern matching criteria:

- Individual character strings that users enter in the field
- File names that user select from a list

File names refer to pattern files that contain groups of character strings. Only root users should create a pattern file.

All pattern files must reside in the **/opt/avaya/mpa/agent/patterns** directory. The format for the pattern file contains a group character strings that Proxy Agent matches on a per line basis. The file can contain comment lines that start with one of the characters listed below:

- Number symbol (#)
- Tab
- Space

Once the pattern file is created, you can add the file to any filter set on the FILTER SET screen.

Boolean Operator

On the FILTER SET screen, you can specify the boolean operator “**not**” if you want Proxy Agent to block alarms that do not match a specified pattern matching criteria.

If the boolean operator (BOOL OPER) field is blank, then Proxy Agent blocks alarms if they match one or more of the pattern matching criteria in the filter set.

Alarm Severity

On the FILTER SET screen, you can block alarms based on the severity of the alarm. You can select one or more of the alarm severity levels listed below:

Note:

The abbreviated titles are vertically stacked above the ALARM SEVERITY columns.

- Major (MAJ)
- Minor (MIN)
- Warning (WRN)
- Downgraded Warning (DGW)
- Cleared Alarm Notification (CLR)
- System Restart (RST)
- Resolved (RES)

Proxy Agent blocks alarms if they match any of the selected alarm severity criteria and the other filter criteria, if any.

Day of Week

On the FILTER SET screen, you can block alarms based on the day of the week (Monday through Sunday). Proxy Agent blocks alarms if they match any of the selected days of the week and the other filter criteria, if any.

Time of Day

On the FILTER SET screen, you can block alarms that Proxy Agent receives during a specified window of time. You can enter the hours (based on the 24-hour clock) in the *Start* and *End* fields.

Proxy Agent blocks alarms if they match any of the time of day criteria and the other filter criteria, if any.

Examples of Filter Sets

To better understand the workings of the Filter Set feature, this section contains two examples of a some common scenarios.

The examples use two pattern files described below. All pattern files must reside in the **/opt/avaya/mpa/agent/patterns** directory. The lists of objects in the examples below are not intended to be complete. The lists only serve as examples of the types of objects that users can include in a pattern file.

The station pattern file contains a list of Communication Manager maintenance object names:

ANL_LINE
ANL_BD
DIG_LINE
MET_LINE
MET_BD

The trunk pattern file contains a list of Communication Manager trunk maintenance object names:

AUX_TRK
CO_TRK
DID_TRK
TIE_TRK
ISDN_TRK

Filter Set 1

The purpose of Filter Set 1 (fset1) is to block the forwarding of the types of alarms listed below:

- All station alarms
- All trunk alarms received during working hours
- All non-major trunk alarms received during off hours

Figure 3: Example of Filter Set 1 (fset1)

change filter-set		(PROXY ADMIN)		page 1 of 1																					
FILTER SET: fset1																									
PATTERN MATCHING CRITERIA			ALRM SEVERITY																						
FILE/	BOOL	FILE NAME OR	M	M	W	C	R	R	DAY OF WEEK			TIME OF DAY													
STRING	OPER	CHARACTER STRING	A	I	R	G	L	S	J	N	N	W	R	T	S	M	T	W	T	F	S	S	START	END	
1:*	file		station																						
2:	file		trunk													X	X	X	X	X		X	X	08:00	17:00
3:	file		trunk													X	X	X	X	X		X	X		
4:	file		trunk													X	X	X	X	X		X	X	00:00	07:59
5:	file		trunk													X	X	X	X	X		X	X	17:01	23:59
6:																									
7:																									
8:																									
9:																									
10:																									
11:																									
12:																									

Explanation

Filter Set 1 consists of five filters to block the alarm streams that contain one or more of the patterns listed in the **station** pattern file and the **trunk** pattern file.

Each filter is explained below:

- Filter 1 blocks the forwarding of all **station** alarms.
- Filter 2 blocks the forwarding of all **trunk** alarms received during **working** hours. The criteria below defines the working hours for this filter:
 - The *Day of Week* criteria block alarms Monday through Friday
 - The *Time of Day* criteria block alarms between 8:00 and 17:00 hours (8:00 a.m. to 5:00 p.m.)
- Filters 3 through 5, together, block the forwarding of all **non-major trunk** alarms received during **off** hours:
 - Filter 3 blocks non-major trunk alarms on Saturday and Sunday
 - Filter 4 blocks non-major trunk alarms on Monday through Friday *before* working hours (0:00 to 07:59)
 - Filter 5 blocks non-major trunk alarms on Monday through Friday *after* working hours (17:01 through 23:59)

Filter Set 2

The purpose of Filter Set 2 (fset2) is to block the forwarding of the alarm streams listed below:

- All cleared alarm notifications
- All minor alarms that are not listed in the trunk pattern file
- All alarms from the board located in port network 3, carrier C, slot 8
- All restart notifications that do not contain the COLD1 level

Figure 4: Example of Filter Set 2

PATTERN MATCHING CRITERIA			ALARM SEVERITY																
FILE/	BOOL	FILE NAME OR	A	M	M	W	D	C	R	R	DAY OF WEEK							TIME OF DAY	
STRING	OPER	CHARACTER STRING	J	N	N	W	R	T	S	M	T	W	T	F	S	S	START	END	
1:*																			
2:file	not	trunk		X															
3:string		03C08																	
4:string	not	COLD1							X										
5:																			
6:																			
7:																			
8:																			
9:																			
10:																			
11:																			
12:																			

Explanation

Filter Set 2 consists of four filters that contain a pattern file, two character strings, and two boolean operators. These filters target very specific conditions for blocking alarm forwarding.

Each filter is explained below:

- Filter 1 blocks alarm forwarding of all **cleared alarm notifications** (CLR) for the alarm severity criteria.
- Filter 2 blocks alarm forwarding of **non-trunk** alarms with a **minor** (MIN) alarm severity criteria.
- Filter 3 blocks alarm forwarding of all alarms from the **board** located in port network 3, carrier C, slot 8 (03C08)
- Filter 4 blocks alarm forwarding of all **restart notifications** (RST) with a alarm severity level that is **not** COLD1.

Understanding the Filter Set Screen

The figure below shows the fields on the blank FILTER SET screen.

Figure 5: Blank Filter Set screen

The screenshot shows a terminal window titled 'change filter-set' with '(PROXY ADMIN)' and 'page 1 of 1' in the top right. Below the title bar, it says 'FILTER SET:'. The main area is a table with 12 rows and several columns. The columns are: FILE/STRING, BOOL/OPER, FILE NAME OR CHARACTER STRING, ALARM SEVERITY (A, I, R, G, L, S, E), DAY OF WEEK (M, M, W, D, C, R, R), and TIME OF DAY (START, END). The rows are numbered 1 through 12 on the left. The content of the rows is mostly obscured by black boxes, but the column headers are clearly visible.

	FILE/STRING	BOOL/OPER	FILE NAME OR CHARACTER STRING	A	I	R	G	L	S	E	M	M	W	D	C	R	R	START	END
1:*																			
2:																			
3:																			
4:																			
5:																			
6:																			
7:																			
8:																			
9:																			
10:																			
11:																			
12:																			

Screen Layout

The FILTER SET screen contains 12 lines to allow users to enter up to 12 filters in any of the fields in the four criteria columns:

- Pattern Matching Criteria (3 fields)
- Alarm Severity (7 fields)
- Day of Week (7 fields)
- Time of Day (2 fields)

Field Descriptions

The table below contains the field descriptions for the FILTER SET screen.

Table 8: Filter Set Screen

Field	Description
FILTER SET	<p>Contains the name of the filter set.</p> <p>To add a new filter set, the user types the name of the filter set in this field.</p> <p>To change, remove, or display an existing filter set, the user presses Ctrl-y in the field to display the HELP list and selects a filter set name from the list.</p> <p>Field size: 8 characters Default: Blank</p>
<p>Pattern Matching Criteria FILE/STRING</p>	<p>Identifies the type of pattern matching for the filter set. The HELP list (Ctrl-y) contains the valid options:</p> <p>file = a pattern file that contains a group of character strings and resides in the /opt/avaya/mpa/agent/patterns directory</p> <p>string = a character string</p> <p>Only the system administrator should create a pattern file. The format for the pattern file contains character strings that Proxy Agent matches on a per line basis. The file can contain comment lines that start with one of the characters listed below:</p> <ul style="list-style-type: none"> ● Number symbol (#) ● Tab ● Space <p>Field size: 6 characters Default: Blank</p>

Table 8: Filter Set Screen (continued)

Field	Description
<p>Pattern Matching Criteria BOOL OPER</p>	<p>Identifies the boolean operator “not” as a pattern matching criteria.</p> <p>Users can specify the boolean operator “not” if they want Proxy Agent to block alarms that do not match a specified pattern matching criteria.</p> <p>If the boolean operator (BOOL OPER) field is blank, then Proxy Agent blocks alarms if they match one or more of the pattern matching criteria in the filter set.</p> <p>The HELP list (Ctrl-y) only contains the not option.</p> <p>Field size: 4 characters Default: Blank</p>
<p>Pattern Matching Criteria FILE NAME or CHARACTER STRING</p>	<p>Identifies the pattern file name or character string based on the selection in the FILE/STRING field.</p> <p>Users can execute one of the options (a, b, or c) below:</p> <ol style="list-style-type: none"> 1. If <i>file</i> was selected in FILE/STRING field, then users must select a pattern file name from the Help list. The Help list (Ctrl-y) only contains the pattern files names that reside in the /opt/avaya/mpa/agent/patterns directory. 2. If <i>string</i> was selected in the FILE/STRING field, then users must type a character string in the field. 3. If <i>no</i> selection was made in the FILE/STRING field, then users must leave the field blank. <p>Field size: 20 characters Default: Blank</p>

Table 8: Filter Set Screen (continued)

Field	Description
ALRM SEVERITY	<p>Identifies the severity of the alarm filter.</p> <p>Users can select one or more of the days listed below.</p> <p>NOTE: The abbreviated titles are vertically stacked above the ALARM SEVERITY columns.</p> <p>MAJ = Major</p> <p>MIN = Minor</p> <p>WRN = Warning</p> <p>DGW = Downgraded Warning</p> <p>CLR = Cleared Alarm Notification</p> <p>RST = Restart Notification</p> <p>RES = Resolved Alarm</p> <p>Users can execute one of the options (a or b) below:</p> <ol style="list-style-type: none">1. Type “x” in one or more of the fields to select the alarm severity criteria.2. Leave the fields blank. <p>Field size: 1 Default: Blank</p>

Table 8: Filter Set Screen (continued)

Field	Description
DAY OF WEEK	<p>Identifies the day or days in the week to block alarm forwarding.</p> <p>Users can select one or more of the days listed below:</p> <p style="padding-left: 40px;">M = Monday</p> <p style="padding-left: 40px;">T = Tuesday</p> <p style="padding-left: 40px;">W = Wednesday</p> <p style="padding-left: 40px;">T = Thursday</p> <p style="padding-left: 40px;">F = Friday</p> <p style="padding-left: 40px;">S = Saturday</p> <p style="padding-left: 40px;">S = Sunday</p> <p>Users can execute one of the options below:</p> <ul style="list-style-type: none"> ● Type “x” in one or more of the fields to select the day of week criteria. ● Leave the fields blank. <p>Field size: 1 Default: Blank</p>
TIME OF DAY	<p>Identifies the time window to block alarm forwarding.</p> <p>The Time of Day column contains the fields below:</p> <p style="padding-left: 40px;">START field contains the time to begin alarm filtering</p> <p style="padding-left: 40px;">END field contains the time to stop alarm filtering</p> <p>Users must use the 24-hour clock to enter start and end times</p> <p>Users can execute one of the options below:</p> <ol style="list-style-type: none"> 1. Type the hours in both the START and END fields to select the time of day criteria. 2. Leave the fields blank. <p>NOTE: Start time must be earlier than end time. Wraparound time of day is not permitted. The solution is use of two entries (i.e. 5pm - 8am is not valid, instead use: one entry 00:00 - 07:59 and a second entry 17:01 - 23:59).</p>

Specifying Filter Sets

You can access the FILTER SET screen from the PROXY ADMIN menu by executing the commands listed below:

- **add filter-set** to create a new filter set
- **change filter-set** to modify an existing filter set
- **remove filter-set** to delete a filter set
- **display filter-set** to view a filter set

On the FILTER SET screen, the user names each new filter set and enters the filters in the fields for the four types criteria:

- Pattern Matching Criteria (3 fields)
- Alarm Severity (7 fields)
- Day of Week (7 fields)
- Time of Day (2 fields)

Adding a Filter Set

Complete the procedure below to create a new filter set in Proxy Agent.

Note:

To use pattern files as part of the filtering criteria, only the system administrator should create the pattern files.

1. Access the PROXY ADMIN menu.
2. Stop Proxy Agent, if running.
3. In the command line on the PROXY ADMIN menu,
 - a. Type **add filter-set**.
 - b. Press **ENTER**.The system displays a blank FILTER SET screen.
4. In the **FILTER SET** field, type the **name** of the new filter set.
5. In line 1 for the **PATTERN MATCHING CRITERIA** fields, complete the appropriate options below:

FILE/STRING: Execute one of the options (a or b) below:

- a. Press **Ctrl-y** and select **file** or **string** from the list. Press **ENTER**.
- b. Leave the field blank.

BOOL OPER: Execute one of the options (a or b) below:

- c. Leave the field blank.
 - d. Press **Ctrl-Y** and select **not** from the list. Press **ENTER**.
- FILE NAME OR CHARACTER STRING:** Execute one of the options (a, b, or c) below based on your selection in the FILE/STRING field:
- e. If you selected **file**, then press **Ctrl-Y** and select a **pattern file** from the list. Press **ENTER**.
 - f. If you selected **string**, then type a **character string** in the field.
 - g. If you left the field **blank**, then do not enter data in this field.
6. In line 1 for the **ALARM SEVERITY** filter, execute one of the options (a or b) below:
- a. Type **X** in any or all of the fields below:
 - **MAJ** = Major
 - **MIN** = Minor
 - **WRN** = Warning
 - **DGW** = Downgraded Warning
 - **CLR** = Cleared Alarm Notification
 - **RST** = Restart Notification
 - **RES** = Resolved Alarm
 - b. Leave the fields blank.
7. In line 1 for the **DAY OF WEEK** filter, execute one of the options (a or b) below:
- a. Type **x** in any or all of the fields below:
 - **M** = Monday
 - **T** = Tuesday
 - **W** = Wednesday
 - **T** = Thursday
 - **F** = Friday
 - **S** = Saturday
 - **S** = Sunday
 - b. Leave the fields blank.
8. In line 1 for the **TIME OF DAY** filter, execute one of the options (a or b) below:
- a. Use the 24-hour clock to enter time in the both of the fields below:
 - **START:** Type the **time** to begin the filter.
 - **END:** Type the **time** to stop the filter.
 - b. Leave the fields blank.

Administering Filter Sets

- In lines 2 through 12, repeat Step [5](#) through Step [8](#) to add additional filters to the filter set, if appropriate.
- Press **Ctrl-E** to submit the filter set.

The system saves the new filter set and displays the PROXY ADMIN screen.

Changing a Filter Set

Complete the procedure below to change the criteria of an existing filter set.

- Access the PROXY ADMIN menu.
- Stop Proxy Agent if it is running ([Stopping Proxy Agent](#) on page 30).
- In the command line on the PROXY ADMIN menu, type **change filter-set** and press **ENTER**.

The system displays a blank FILTER SET screen.

- In the **FILTER SET** field, Press **Ctrl-Y** and select the **name** of the filter set from the list, and press **ENTER**.

The system displays the filter criteria for the selected filter-set name.

- In line 1 for the **PATTERN MATCHING CRITERIA** fields, complete the appropriate options below:

FILE/STRING: Execute one of the options (a or b) below:

- Press **Ctrl-Y** and select **file** or **string** from the list. Press **ENTER**.
- Leave the field blank.

BOOL OPER: Execute one of the options (a or b) below:

- Leave the field blank.
- Press **Ctrl-Y** and select **not** from the list. Press **ENTER**.

FILE NAME OR CHARACTER STRING: Execute one of the options (a, b, or c) below based on your selection in the FILE/STRING field:

- If you selected **file**, then press **Ctrl-Y** and select a **pattern file** from the list. Press **ENTER**.
- If you selected **string**, then type a **character string** in the field.
- If you left the field **blank**, then do not enter data in this field.

6. In line 1 for the **ALARM SEVERITY** filter, execute one of the options (a or b) below:
 - a. Type **X** in any or all of the fields below:
 - **MAJ** = Major
 - **MIN** = Minor
 - **WRN** = Warning
 - **DGW** = Downgraded Warning
 - **CLR** = Cleared Alarm Notification
 - **RST** = Restart Notification
 - **RES** = Resolved Alarm
 - b. Leave the fields blank.
7. In line 1 for the **DAY OF WEEK** filter, execute one of the options (a or b) below:
 - a. Type **X** in any or all of the fields below:
 - **M** = Monday
 - **T** = Tuesday
 - **W** = Wednesday
 - **T** = Thursday
 - **F** = Friday
 - **S** = Saturday
 - **S** = Sunday
 - b. Leave the fields blank.
8. In line 1 for the **TIME OF DAY** filter, execute one of the options (a or b) below:
 - a. Use the 24-hour clock to enter time in the both of the fields below:
 - **START**: Type the **time** to begin the filter
 - **END**: Type the **time** to stop the filter
 - b. Leave the fields blank.
9. In lines 2 through 12, repeat Step [5](#) through Step [8](#) to add additional filters to the filter set, if appropriate.
10. Press **Ctrl-E** to submit the changes to the filter set.

The system saves the changes and displays the PROXY ADMIN screen.

Displaying the Filter Set Screen

Complete the procedure below to display the FILTER SET screen. The **display** command lets you view the screen only. You cannot make changes to any of the fields.

Note:

You do not have to stop Proxy Agent to execute the **display** command.

1. Access the PROXY ADMIN menu.
2. In the command line on the PROXY ADMIN menu, type **display filter-set** and press **ENTER**.

The system displays a blank FILTER SET screen.

3. In the **FILTER SET** field, press **Ctrl-Y**, select the name of the filter set from the list, and press **ENTER**.

View the criteria for the filter set.

4. Press **Ctrl-X** to exit the screen.

The system closes FILTER SET screen and the displays the PROXY ADMIN screen.

Removing a Filter Set

Proxy Agent lets you delete all filter sets *except* the **default** filter set. If you try to remove a filter set that has been assigned to one or more systems on the MANAGED NODES screen, then Proxy Agent displays a warning message. The message explains that if you remove the filter set, Proxy Agent will replace it with the **default** filter set for the affected the managed nodes.

If you do not want the default filter set to be assigned to individual managed node, then you can clear the default filter set in the *Filter Set Name* field on page A of the MANAGED NODES screen.

Procedure

Complete the procedure below to delete a filter set from Proxy Agent.

1. Access the PROXY ADMIN menu.
2. Stop Proxy Agent if it is running ([Stopping Proxy Agent](#) on page 30).
3. In the command line on the PROXY ADMIN menu, type **remove filter-set** and press **ENTER**.

The system displays a blank FILTER SET screen.

4. In the **FILTER SET** field, press **Ctrl-Y**, select the name of the filter set to be removed, and press **ENTER**.

The system displays the criteria for the selected filter set.

5. To remove the selected filter set, press **Ctrl-E**.

The system displays one of the options below:

- a. If the filter set is not assigned to any managed node, then the system deletes the filter set and displays the PROXY ADMIN screen.

Go to Step [7](#) below.

- b. If the filter set is assigned to one or more managed nodes, then system displays a window with a warning message. The message explains that the selected filter set will be replaced with the **default** filter set for the affected managed nodes. The message also contains a confirmation prompt: *Do you wish to continue?*

Go to Step [6](#) to complete the procedure.

6. At the prompt, select one of the options below:

- a. To remove the filter set, select **Yes**.

The system removes the selected filter set and replaces it with the **default** filter set for the affected managed nodes. Then, the system displays the PROXY ADMIN screen.

- b. To cancel the remove request, select **No**.

The system cancels the remove request and displays the PROXY ADMIN screen.

7. Start Proxy Agent ([Starting Proxy Agent](#) on page 30).

8. Display the STATUS screen, verify that Proxy Agent is active, and exit the screen ([Displaying the Proxy Agent Status Screen](#) on page 34).

Chapter 8: Setting Preferences

Use the Configuration application to set the preferences for the monitor and screen elements and to display the software version.

Change User-Interface Screens

The CHANGE USER-INTERFACE screens contains four pages of configuration and color options.

Page 1 contains the configuration options to:

- Set the color options on the monitor
- Turn on or turn off the audible beep tone

Typically, the configuration options on page 1 are the only options that you may want to change.

Pages 2 through 4 contain the options to customize the colors for the elements listed below:

- Screen elements
- Activity Area elements
- Popup Display Window elements

Display Software Version Screen

The DISPLAY SOFTWARE VERSION screen contains the software release and versions of the Red Hat Linux system, EMANATE, and Proxy Agent that are currently installed.

Field Descriptions

The table below contains descriptions of the field on the DISPLAY SOFTWARE VERSION screen.

Table 9: DISPLAY SOFTWARE VERSION screen

Field	Description
SOFTWARE VERSION (view-only)	
Linux Release	Identifies the release number of Linux operating system that is currently installed. This is a view-only field.
<i>1 of 2</i>	

Table 9: DISPLAY SOFTWARE VERSION screen (continued)

Field	Description
Linux Version	Identifies the version number of the Linux operating system that is currently installed. This is a view-only field.
Proxy Agent Version	Identifies the version number of Proxy Agent software that is currently installed. This is a view-only field.
EMANATE Version	Identifies the version number of the SNMP Research EMANATE agent. This is a view only field.
2 of 2	

Change User-Interface Screen

Page 1 Field Descriptions

The table below contains the field descriptions for configuration options on page 1 of the CHANGE USER-INTERFACE screens.

Table 10: Configuration options

Field	Description
CONFIGURATION OPTIONS (page 1)	
Color Option	<p>Sets the colors for the monitor. Valid options include:</p> <ul style="list-style-type: none"> default -- for color monitors monochrome -- default for black-and-white monitors customize -- change color of screen elements (see pages 2 through 4 below)
Audible Beep Tone?	<p>Sets the beep tone to ON or OFF. Valid options include:</p> <ul style="list-style-type: none"> y (yes) -- Turns ON the beep tone (default) n (n) -- Turns OFF the beep tone

Setting the User-Interface Options

Complete the procedure below to change the system-wide, default parameters for the configuration and color options.

Note:

For color monitors, you must set the TERM variable to **color** or **default** so that Proxy Agent screens will be in color.

1. Access the Proxy Agent MAIN MENU.
2. In the command line, type **configuration** and press **ENTER**.

The system accesses the Configuration application. Then, it displays a blank command line on the Proxy Agent MAIN MENU.
3. In the command line, type **change user-interface** and press **ENTER**.

The system displays the CHANGE USER-INTERFACE screen.
4. In the *Color Option* field on page 1, press **Ctrl-Y**, select one of the options presented, and press **ENTER**.
5. In the *Audible Beep Tone?* field on page 1, press **Ctrl-Y**, select one of the options below, and press **ENTER**.
 - **Y** (yes) to turn-on the beep tone (default)
 - **N** (no) to turn-off the beep tone
6. **Optional.** To customize the colors of the screen elements, complete the steps below:
 - a. Press **Ctrl-Y** to in each field to display the field options.
 - b. Select an option.
 - c. Press **ENTER**.
 - d. Press **Ctrl-D** to access the next page.
7. Execute one of the options below:
 - a. If you made any changes, press **Ctrl-E** to save the changes and exit the CHANGE USER-INTERFACE screen.
 - b. If you do not want to make any changes, press **Ctrl-X** to exit the CHANGE USER-INTERFACE screen.

The system exits the screen and displays the Proxy Agent MAIN MENU.

Setting Preferences

Chapter 9: Maintenance and Troubleshooting

This chapter contains utilities and logs to allow the system administrator to maintain Proxy Agent and troubleshoot problems with alarms, traps, and system errors.

The chapter also contains an example of a Test Trap script to test an event configuration on the Fault and Performance Manager server and the HP OpenView Network Management System (NMS).

Proxy Agent contains several maintenance and troubleshooting options that only the root user should execute. These options include tasks listed below:

- Adding new devices to Proxy Agent after Proxy Agent has been installed
- Changing settings for SNMP access after Proxy Agent has been installed
- Viewing alarm and error logs to troubleshoot the receiving and forwarding of alarms

Note:

To view the alarm log file (alarms received by the Proxy Agent alarm reception system) using a URL; type

`http://proxy-name/cgi-bin/mpa/Alarms.sh?count=XX`

(**proxy-name** should be the node name or IP address of the proxy agent computer and **XX** is the number of lines to show). You can also view the alarm log from the KDE/Gnome Desktop of the Proxy Agent Linux Server by clicking on **Programs>Avaya>Avaya Proxy Agent> Administration>Alarm Log Viewer**.

- Using the alarm testing tools to simulate alarm and trap reception on Proxy Agent and test the event configuration on the Fault and Performance Manager server and the HP OpenView NMS
- View Proxy Agent status and Proxy Agent cache status using the Integrated Management home page

Note:

To view the status of Proxy Agent using a URL; type

`http://proxy-name/cgi-bin/mpa/Status.sh` (**proxy-name** should be the node name or IP address of the proxy agent computer). You can also view the Proxy Agent status from the KDE/Gnome Desktop of the Proxy Agent Linux Server by clicking on **Programs>Avaya>Avaya Proxy Agent> Administration>Proxy Agent Status**.

Note:

To view Managed Node cache data status using a URL; type **`http://proxy-name/cgi-bin/mpa/Status.sh?node=NODE`**

(**proxy-name** should be the node name or IP address of the proxy agent computer and **NODE** should be the name of a specific managed node supported by this proxy agent).

Adding New Communication Devices

The root user can add new communication devices to Proxy Agent by running the `/usr/bin/dpa_portadm` command. To do so, you must access the file and respond to the prompts. The prompts are identical to the prompts in the installation script for the function and the device type. For more information, see:

- [Configuring Proxy Agent](#) on page 24.
- [Uninstalling Proxy Agent](#) on page 27.

Changing Settings for SNMP Access

See [Configuring Proxy Agent](#) on page 24.

Viewing Alarm and Error Logs

Proxy Agent maintains a number of alarm and error logs in the **agent** directory. System administrators can view the logs to troubleshoot problems with receiving and forwarding alarms. To access the logs, edit the directories in the table below.

Table 11: Alarm and error logs

Log	Directory
Event log for alarm receiver device	/opt/avaya/mpa/agent/logs/alarmlog
Error log for alarm receiver device	/opt/avaya/mpa/agent/logs/errorlog
Alarms scheduled to be sent to INADS or other destinations	/opt/avaya/mpa/agent/alarms/alrms_rcvd.log
Alarms successfully sent to INADS or other destinations	/opt/avaya/mpa/agent/alarms/alrms_sent.log

1 of 2

Table 11: Alarm and error logs (continued)

Log	Directory
Audit log	/opt/avaya/mpa/agent/logs/auditlog
Error log for alarm sender device	/opt/avaya/mpa/agent/alarms/alarms.log
2 of 2	

Using Alarm Testing Tools

Proxy Agent contains a set of Trap Test tools. System administrators can use these tools to:

- Simulate the alarm reception on Proxy Agent and
- Test the trap reception and event configuration on the Fault and Performance Manager server and the HP OpenView Network Management System (NMS)

Proxy Agent contains a script for each product type. All scripts reside in the **/opt/avaya/mpa/agent** directory.

Trap Test Scripts

The table below contains the command and function for the trap tests scripts:

Table 12: Trap Test Scripts

Command	Function
TrapTest	Communication Manager Feature Server and MCU traps
CMSTrapTest	Call Management System (CMS) traps
ADXTrapTest	Communication Manager Feature Server AUDIX traps
IADTrapTest	Intuity AUDIX traps
INTTrapTest	Intuity Interchange traps
CVSTrapTest	CONVERSANT traps

Procedure

The procedure below uses the Communication Manager Feature Server TrapTest tool as an example of the format for the alarm testing tools. For other products, the script for the TrapTest tool is slightly different.

Note:

For the tools to work, Proxy Agent must be running and the ALARM DEVICES and MANAGED NODES screens must be properly administered.

1. At the Linux shell, log in to the root (/) directory.
2. Access a test script. The steps below show an example of a TrapTest script:
 - Type **/opt/avaya/mpa/bin/TrapTest**.
 - Press **ENTER**.

The system opens the file and displays the script for the selected trap test, as shown in the example below. The fields may contain the data from the previous test.

```
Avaya Proxy Agent Alarm Trap Test Tool
Current DEFINITY Node Name: NewYork
Current DEFINITY Alarm ID: 1111111111

0) Alarm Clear Trap [alarmClear:0]
2) Major Alarm Trap [alarmMajor:2]
3) Minor Alarm Trap [alarmMinor:3]
5) Major External Alarm Trap [extalarmMajor:5]
6) Minor External Alarm Trap [extalarmMinor:6]
7) TSC Dispatch Alarm Trap [alarmDispatch:7]
8) TSC Close Alarm Trap [alarmClose:8]
9) Restart Notification Trap [alarmRestart:9]

C) Change DEFINITY alarming from
H) Help
Q) Quit

Send which trap?:
```

3. **Select the Change Option.** To change to a different DEFINITY node name, go to the field:
Send which trap?:
 - Type **C** (change).
 - Press **ENTER**.

The system displays the message:

```
Changing DEFINITY that the Alarms will be coming from... You must
set the Node Name and the Alarm ID for the DEFINITY you wish
alarms to be associated with. The Name and ID must match those
```

specified in the managed node form of the Proxy Agent for the switch you wish to send traps for.

Enter new DEFINITY Node Name:

Enter new DEFINITY Alarm ID:

4. **Enter a New Node Name.** As shown in the example below, type a new node name and the alarm ID for a Communication Manager Feature Server. Press **ENTER** after each entry:

Enter new DEFINITY Node Name: **jupiter**

Enter new DEFINITY Alarm ID: **1222222222**

The system displays the new node name and alarm ID in the fields and displays the prompt to select a trap test, as shown below.

Avaya Proxy Agent Alarm Trap Test Tool

Current DEFINITY Node Name: **jupiter**

Current DEFINITY Alarm ID: **1222222222**

- 0) Alarm Clear Trap [alarmClear:0]
- 2) Major Alarm Trap [alarmMajor:2]
- 3) Minor Alarm Trap [alarmMinor:3]
- 5) Major External Alarm Trap [extalarmMajor:5]
- 6) Minor External Alarm Trap [extalarmMinor:6]
- 7) TSC Dispatch Alarm Trap [alarmDispatch:7]
- 8) TSC Close Alarm Trap [alarmClose:8]
- 9) Restart Notification Trap [alarmRestart:9]
- C) Change DEFINITY alarming from
- H) Help
- Q) Quit

Send which trap?:

5. **Select a trap option.** As shown in the example below, type a number (0-9) to select a trap test and press **ENTER**.

Send which trap?: **5**

The system displays the message and the fields shown in the example in the next step.

6. **Execute the trap test.** Users can enter any data in the in the free-form fields. The system does not validate the fields. As shown in the example below, type data in each field and press **ENTER** after each entry:

Enter alarm trap information for External trap

MIB oid names are show in brackets

Switch [g3clientExternalName]: jupiter

Proxy Agent Sequence Number [g3alarmsAlarmNumber]: **0000000012**

Switch Port Location [g3alarmsPort]: **01C1201**

On-Board Alarm Flag [g3alarmsOnBrd]: **Y**

Maintenance and Troubleshooting

```
External Device Alt. Name [g3extdevAltName]: ENVUPS1  
External Device Description [g3extdevDescription]: PROXY AGENT  
UPS  
External Device ID [g3extdevID]: 2001  
External Device Building [g3extdevBuilding]: Building 30  
External Device Address [g3extdevAddress]: 1234 Main St
```

The system displays the message: Alarm Trap Emulation Successful

Then, the system displays the Linux prompt.

7. Access the Fault and Performance Manager server and the HP OpenView NMS to view the results of the test. Repeat this procedure to execute other trap tests.

Chapter 10: Help Screens and Commands

Proxy Agent contains two types of help windows that you can access from any menu or screen. The commands to access the help windows include the following:

- The list command (**Ctrl-L**) displays a **Functions** window that contains the available commands for the current Proxy Agent menu or application screen.
- The help command (**Ctrl-Y**) displays a **help** window for the current Proxy Agent menu or individual field on an application screen. Help windows can be lists of valid options for a specific field or instructions that explain the type of information to input in a field.

Note:

You need only type enough of each command to make it unique. For example: at the proxy main menu, instead of typing “proxy-admin”, you can type just “p”.

The Format Conventions section contains a table that describes the conventions used in this guide.

Functions Window

Users can access the Functions window (**Ctrl-L**) from any menu or application screen in Proxy Agent.

Most commands have hotkeys, which are keyboard short cuts. Hotkeys allow users to execute a command without accessing the Functions window.

Commands and Hotkeys

The table below contains the description for the commands and the hotkeys that are available on Proxy Agent.

Table 13: Commands and Hotkeys

Command	Description
List command Ctrl-L	<p>Displays the Functions window that contains all of the available commands and associated hotkeys for the current screen.</p> <p>To select an option from the Functions window,</p> <ul style="list-style-type: none"> ● Press Ctrl-L to display the Functions window: ● Use the arrow keys or the TAB key to move the cursor to an option on the screen. ● Press ENTER to execute the command.
Help Ctrl-Y	<p>Displays a help window for a field or a menu, as described below:</p> <ul style="list-style-type: none"> ● Field help window contains a list of options for the field. ● Main Menu help window contains explanations of the applications on the menu. ● Submenu help window contains available commands. <p>To access a help list for a specific field,</p> <ul style="list-style-type: none"> ● Move the cursor to the field. ● Press Ctrl-Y to display the help window. ● Move the cursor to an option on the list. ● Press ENTER to execute the option. <p>To exit a help window without selecting an option, press ESC.</p>
Submit Ctrl-E	Saves changes made in the fields on an application screen and exits the screen.
Cancel Ctrl-X	Exits a screen without saving changes.

Table 13: Commands and Hotkeys (continued)

Command	Description
Clear Field Ctrl-K F	Deletes the data in the field where the cursor is located. Users can also delete data in a field by pressing the SPACE BAR .
Page Down Ctrl-D	Displays the next numbered page in a multiple-page application. Example: The MANAGED NODES application contains 10 pages. Press Ctrl-D to page down to the next page (2, 3, 4, etc.).
Page Up Ctrl-U	Displays the previous numbered page in a multiple-page application. Example: In the MANAGED NODES application, press Ctrl-U to page up to the previous page (4, 3, 2, 1).
Page Right Ctrl-N	Displays the next subpage that is to the right of the current page. Example: The MANAGED NODES application is similar to a spreadsheet with columns and rows on 5 subpages (a through e) for each numbered page. Press Ctrl-N to access the next subpage (b, c, d, e) within a spreadsheet application.
Page Left Ctrl-P	Displays the previous subpage that is to the left of the current page. Press Ctrl-P to access the <i>previous</i> subpage (d, c, b, a) within a spreadsheet application.
Page Select (no hotkey)	Displays a window that contains all available page options within a multiple-page application. The options may include any or all of the page commands listed above.
Refresh (no hotkey)	Updates the screen with the current information.
2 of 2	

Glossary and Abbreviations

A

ATAC See [Avaya Technology and Consulting \(ATAC\)](#) on page 11.

C

communication device Any device that enables the Network Management Server (where Proxy Agent is installed) to communicate with “managed nodes.” For example, a modem, or (more recently) TCP/IP connections.

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.

M

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

N

Network Management Server This is the Windows box that you can install Windows-based 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 and/or Proxy Agent on.

T

TSO See [Avaya Technical Service Organization \(TSO\)](#) on page 12.

Index

Symbols

>, meaning of [7](#)

A

Audible Beep Tone field, on Change User-Interface screen [72](#)

Avaya

support web site [9](#)

Avaya Technology and Consulting (ATAC) [11](#)

B

boldface, meaning of [7](#)

books

giving feedback on [8](#)

C

contact information

third party [15](#)

contact information for Avaya [14](#)

D

documentation

giving feedback on [8](#)

F

feedback, giving us your [8](#)

Filter Set

procedure to add new [64](#)

H

Hewlett-Packard web site. [15](#)

I

IMD [39](#)

Integrated Management Database [39](#)

N

network

security [16](#)

P

passwords, changing [16](#)

Proxy Agent

log in security [20](#)

Q

quit command, on Proxy Admin screen [33](#)

R

Red Hat web site [15](#)

Remedy web site [15](#)

resources

Avaya Communications, Solutions, and Integration (CSI) Group of Software Services [11](#)

Customized Management Solutions for Avaya Integrated Management [13](#)

S

security

Avaya disclaimer [16](#)

for networks. [16](#)

network. [16](#)

notices [16](#)

Proxy Agent access [20](#)

SNMP authentication [19](#)

toll fraud [16](#)

toll fraud intervention [16](#)

SNMP

security authentication [19](#)

start command, on Proxy Admin screen [33](#)

stop command, on Proxy Admin screen [33](#)

T

Technical Service Organization [12](#)

Technical Services Organization. [12](#)

Index

toll fraud.	16
Avaya disclaimer	16
intervention.	16
TSO	12
typographical conventions	7

U

Uninstalling	27
Uninstalling Proxy Agent	27

V

Vytek web site	15
--------------------------	--------------------

W

web sites	
third-party	15