Avaya Integrated Management Release 3.0 Proxy Agent Configuration

555-233-139
Issue 7
June 2005

Notice

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

Warranty

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

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

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

How to Get Help

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

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

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

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

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

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

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

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

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

Luokan 1 Laserlaite

Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

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

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

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

Means of Connection

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

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

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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

Installation and Repairs

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

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

Declarations of Conformity

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

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

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

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

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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

Japan

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

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

Preface

Purpose

This book explains how to configure Avaya 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 Enterprise Network Management CDs and is also available from http://www.adobe.com. See How to Access Books on the Web on page 10 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. In the left column, click **System and Network Management**.
3. Scroll to **Integrated Management**, locate the product name, and click the link corresponding to the software release to display a list of available books for that product.

How to Order More Copies of This Book

To order paper copies of this book, call or write us and request the following publication:

Order:

Document Number: 555-233-139
Issue: Issue 7
Date: June 2005

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

If you are calling from somewhere that cannot access US 1-800 numbers, then call:
Voice: + 1 207 866 6701
Fax: + 1 207 626 7269

Write:

Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835
USA

Chapter 1: Resources and Notices

Avaya provides a variety of planning, consulting, and technical services. The sections below briefly describe the resources and services that are available.

Client executives are your primary contact to obtain information and explore options to meet your specific business needs.

Avaya Technology and Consulting (ATAC)

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 16 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 16 for contact information. The Product Team will assist customers with Avaya Integrated Management projects and will provide:

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

Avaya Contact Information

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

Table 1: Customer-Accessible Resources

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

Table 2: Avaya Internal Resources

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

Third-Party Resources

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

Table 3: Vendor web sites

Vendor	Web Sites
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 16.

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 uses TCP/IP ports to collect configuration and management data from supported systems. Proxy Agent converts OSSI (Operations Support System Interface) data generated by Avaya Call Processing software and Avaya Communication Manager into Simple Network Management Protocol (SNMP) data, and it generates SNMP traps when supported systems generate alarms and system errors.

Proxy Agent then transmits the SNMP data to Fault and Performance Manager on the System Management Server. The System Management Server is a Linux system.

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.

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 52.

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 3.0 supports both SNMP V1 and V2c get and set requests and SNMP V1 traps for the following systems:

- DEFINITY ECS Releases 9.2 through 10.x (the system must support IP access for system administration)
- Avaya Communication Manager Release 1.1 through 3.0. Proxy Agent supports Avaya Communication Manager Release 3.0 on Linux, 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, S8300, S8500, S8700, S8710 Media Servers with CMC1 Media Gateway

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

Proxy Agent Release 3.0 supports only SNMP alarms for the following systems:

- DEFINITY AUDIX Releases 3.1 through 4.0
- Intuity AUDIX Release 5.1 (with or without the remote maintenance board)
- Intuity 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

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 16.

Hardware Certification

Avaya requires that Proxy Agent hardware must be Red Hat Enterprise Linux ES 2.1 or 3.0 or Red Hat Enterprise Linux AS 3.0 certified. For the Red Hat URL, see Vendor web sites on page 17.

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 3.0 operates on a Linux platform, running Red Hat Enterprise Linux ES 2.1 or 3.0 or Red Hat Enterprise Linux AS 3.0.

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 3.0 System Management Installation and Upgrade*.
4. Installers complete Configuring Proxy Agent on page 25.
5. Installers complete Administering Proxy Agent via Integrated Management Database on page 43.
6. Installers complete Administering Alarm Services on page 49.
7. Installers complete Specifying Filter Sets on page 68.

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 16.

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 Polling, SNMP Traps, and SNMP Set capabilities, 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 these features. For Proxy Agent to work properly with Avaya Fault and Performance Manager (Fault and Performance Manager), you must enable SNMP polling and SNMP Traps. However, you can also select other options to meet a customer’s specific business requirements.

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 Polling

For Proxy Agent to poll the supported systems and create enterprise-specific traps, you must enable SNMP Polling. The configuration script automatically enables SNMP Traps, since both options are required for SNMP polling.

You can choose to disable SNMP polling if you plan to use Proxy Agent only as an alarm notification device, and not use Fault and Performance Manager.

SNMP Polling

During the installation of Proxy Agent, you have the option to enable or disable SNMP polling:

- If you enable SNMP polling, then Proxy Agent supports only the number of managed nodes specified during installation.
- If users disable SNMP polling, then Proxy Agent can support up to 600 managed nodes.

To change these options after Proxy Agent has been installed, you must change the options at the appropriate prompts in the configuration (mpaconfig) script.

SNMP Traps

If SNMP Polling is disabled, then the configuration script displays the prompt to enable or disable SNMP Traps. You should enable SNMP Traps if the customer wants to receive traps from a large number of supported systems. If SNMP Polling is disabled and 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.

SNMP Set Capability

When you configure Proxy Agent, you can also enable or disable the SNMP Set Capability. This feature allows users on the Network Management server to perform the following tasks from Fault and Performance Manager:

- Busy-out and release boards, ports, trunk groups and trunks
- Set the QoS information from the voice system IP Network Region parameters

⚠ WARNING:
Due to security limitations in SNMP, you should enable the SNMP Set Capability only if Proxy Agent is behind a fire wall.

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 both the SNMP voice system access and the SNMP
   alarm traps.

   By selecting this option, you can use the Avaya Fault and
   Performance Manager to manage your voice systems via SNMP access.

   Option 2 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 3 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 Voice System Access and SNMP Alarm Traps

2) SNMP Alarm Traps Only

3) Alarm Processing Only (No SNMP Support)

Enter your selection [2] :
```

3. Select **1**, **2**, or **3** and press **ENTER.**

   Selecting 1 enables SNMP polling and allows Proxy Agent to interact with the System Management Server. Selecting 2 will enable only SNMP alarm traps. Selecting 3 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:

   You will be required to enter a password for the Login ID.

   Changing password for user g3maadm.

   New Password:
   ```

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

   The system displays the reasons to disable or enable SNMP Set Capability. The SNMP Set Capability allows network managers on the Fault and Performance Manager server and the HP OpenView NMS to execute the tasks below from Avaya Fault and Performance Manager.

   - Busy-out and release alarms
   - Set the system date and time (Not supported on S8300, S8700, and S8710)

Then the system displays the prompt:

```
The Avaya Proxy Agent allows only limited SNMP sets of the Voice
System. Currently, the Voice System date and time can be set via
SNMP. Trunks, Trunk Groups, Boards and Ports can also be busied-out
or released via an SNMP Set.  Since the Proxy Agent does not use a
secure version of SNMP, this should only be enabled if your Proxy
Agent is behind a firewall.  Security implications are that someone
could busy out a trunk group and take it out of service by issuing
an SNMPv1 set request to the Avaya Proxy Agent.  The only method of
security in the current release, is a private community string.  It
is suggested that this only be enabled if you are aware of what the
security versus functionality trade-offs are.  Avaya will not be
held liable for any service outage as a result of the customer or
other party issuing an SNMP set request to busy or release busy a
trunk, trunk-group, board or port, or to modify the Voice System
time.

WARNING: If you are not behind a secure firewall, it is strongly
suggested that this option be disabled!!

The current setting is SNMP Set Capability is DISABLED.

Should SNMP Set Capability be ENABLED? [n]/y :
```

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

   a. If Proxy Agent is not behind a secure fire wall, type **n** to disable SNMP Set capability.

   b. If Proxy Agent is behind a secure fire wall, type **y** to enable SNMP Set capability.

   If you enable SNMP Set capability, the system displays:

   ```
   SNMP Set Access to Voice Systems has been enabled.
   ```

   You will be required to enter a password for the Login ID.

   ```
   Changing password for user g3maadm.

   New password:

   Retype new password:
   ```

7. 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:
   ```

8. 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.

9. (As appropriate) Repeat Step 8 for each device.
10. 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.
```

11. 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.

12. Go to Step 5 of the Configuration Overview on page 24.

Uninstalling Proxy Agent

Only root users should uninstall Proxy Agent. Please refer to *Avaya Integrated Management Release 3.0 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 35.
   - 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 33.

   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 38.

Stopping Proxy Agent

As explained in the section, Understanding the Proxy Admin Screen on page 35, 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 33**.**

   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 38.

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. Refer to Troubleshooting Connections on page 80.
configuration	Accesses the **Configuration** application. This application contains two commands: • **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 75.
proxy-admin	Accesses the PROXY ADMIN menu. Refer to Understanding the Proxy Admin Screen on page 35.
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 33.
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: • Deletes the filter set if it is not assigned to any managed node • Replaces the filter set with the *default* 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	Accesses the administration screens. The **change** command allows users to edit the selected screen. **NOTE:** Users must STOP Proxy Agent before executing the **change** command. • **change alarm-devices** See Understanding the Alarm Devices Screen on page 50. • **change filter-set** See Understanding the Filter Set Screen on page 63.
display	Shows the administration screens and the STATUS screen in the view-only mode. The **display** command does not allow users to change the screens. **NOTE:** You do not have to STOP Proxy Agent before executing the *display* command. • **display alarm-devices** • **display filter-set** • **display status** -- See Displaying the Proxy Agent Status Screen on page 38.
start	Initiates an Proxy Agent connection to the managed nodes. See Starting Proxy Agent on page 33.
stop	Drops the Proxy Agent **connection** to the managed nodes. See Stopping Proxy Agent on page 34.
quit	Closes the PROXY ADMIN screen and displays the Proxy Agent MAIN MENU.

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 33, 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
- Connection statistics (only for the DEFINITY ECS, MCU, and Avaya S8100 Media Servers with Avaya G600 Media Gateway managed nodes)

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)

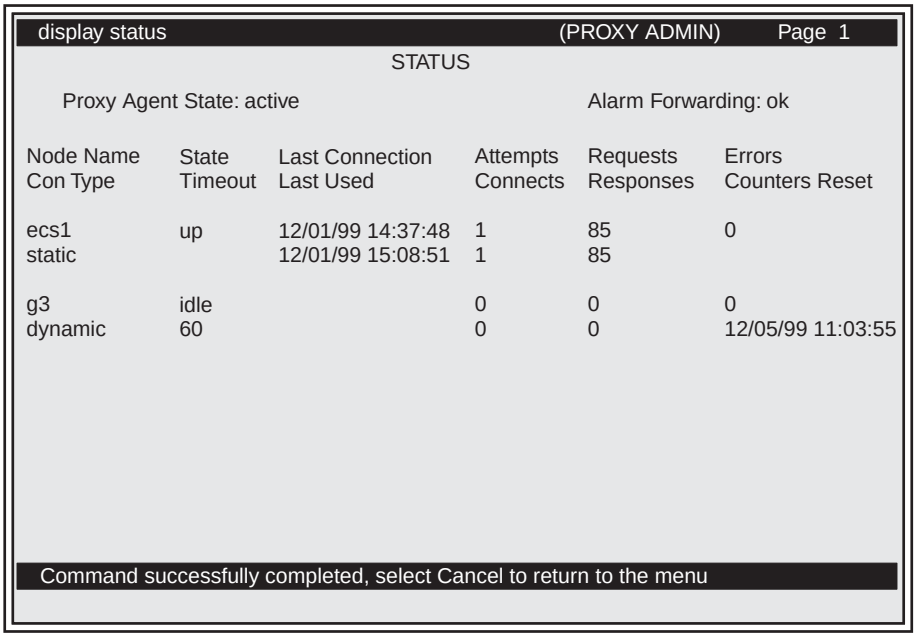
The STATUS screen does not display any connection statistics for the following managed nodes. Proxy Agent supports only alarm handling for these products.

- 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 (aka Cloak)
- S8100, S8300, S8500, S8700, S8710 Audix
- Modular Messaging
- CMS
- Conversant
- Interchange
- Message Networking
- MCU

Figure 1: STATUS screen



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	Identifies the current activity status of Proxy Agent: • **active** -- The Proxy Agent has been started • **not active** -- The Proxy Agent has been stopped
Alarm Forwarding	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. The states include: • **ok** -- Alarm forwarding is active and functioning • **failed** -- Alarm forwarding is active, but is not functioning • **other** -- Identifies one of the following conditions: - Proxy Agent is not active - Alarm forwarding feature is not turned on
Node Name	Identifies the name of the managed node that is associated with Proxy Agent.
Con Type	Identifies the type of connection. It can be one of the following: • **static** (continuous connection) • **dynamic** (temporary connection on an as-needed basis)

1 of 2

Table 6: STATUS screen (continued)

Column	Description
State	Identifies the current status of Proxy Agent's connection to a managed node. The states include: • **init** (initiate) -- A connection attempt is in progress • **up** -- The connection is established • **down** -- The connection attempt has failed • **off** -- The connection has been turned off • **idle** -- A **dynamic** connection is not connected in standby mode • **other** -- The connection has failed and the state is unknown
Timeout	Indicates the number of **minutes** a dynamic connection will remain up without receiving data transmission.
Last Connection	The **date** and **time** of the last successful connection.
Last Used	The **date** and **time** of the last successful data retrieval.
Attempts	The number of connection attempts since the counter was reset to zero.
Connects	The number of successful connections since the counter was reset to zero.
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.

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).

l. From the Start Type box, select the appropriate setting.

m. From the Start State box, select the appropriate setting.

n. In the Dynamic Timeout box, enter the timeout value.

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 S8500 Voice System
- Avaya Communication Manager
- DEFINITY AUDIX
- Intuity AUDIX
- Intuity AUDIX LX
- Intuity Interchange
- S8100, and S8300, 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.

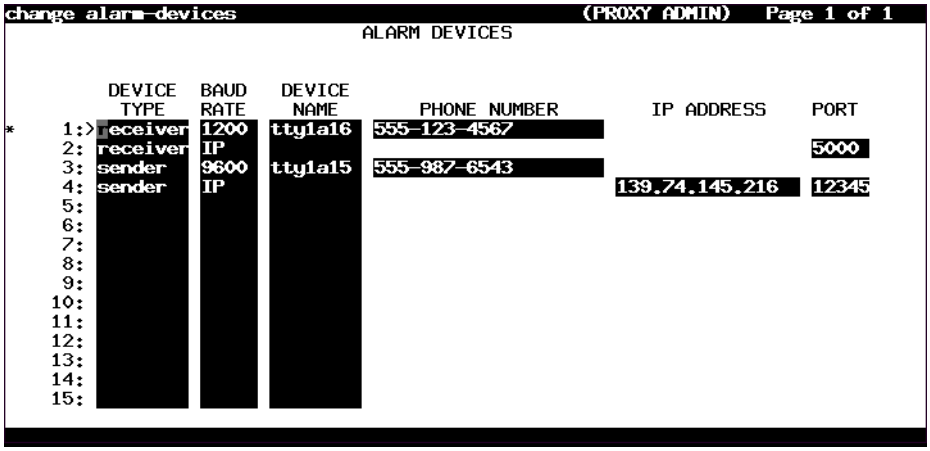
Troubleshooting Alarm Problems

To troubleshoot alarm problems, refer to Viewing Alarm and Error Logs on page 87.

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 34).

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 24."
12. Restart Proxy Agent (Starting Proxy Agent on page 33).

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
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
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.

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 filer 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

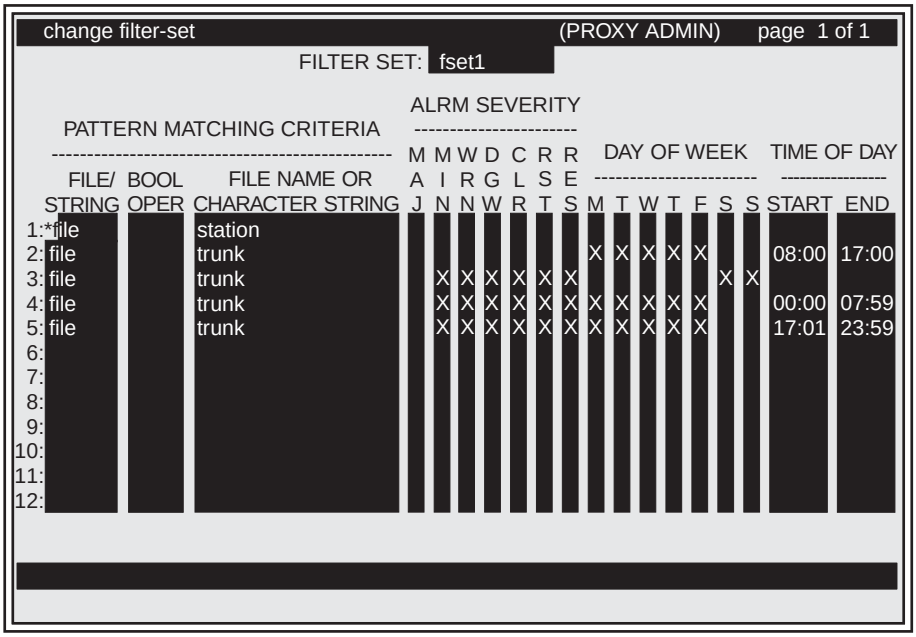
ISDN_TRK

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)



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:

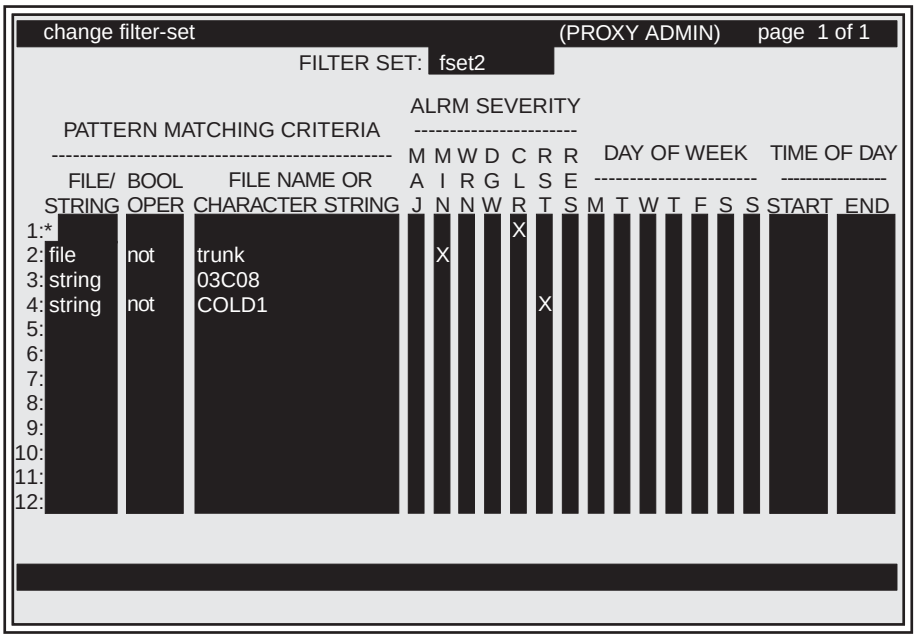
- Filter 1 blocks the forwarding of all **station** alarms.
- Filter 2 blocks the forwarding of all **trunk** alarms received during **working** hours. The criteria below defines the working hours for this filter:
  - The *Day of Week* criteria block alarms Monday through Friday
  - The *Time of Day* 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



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.

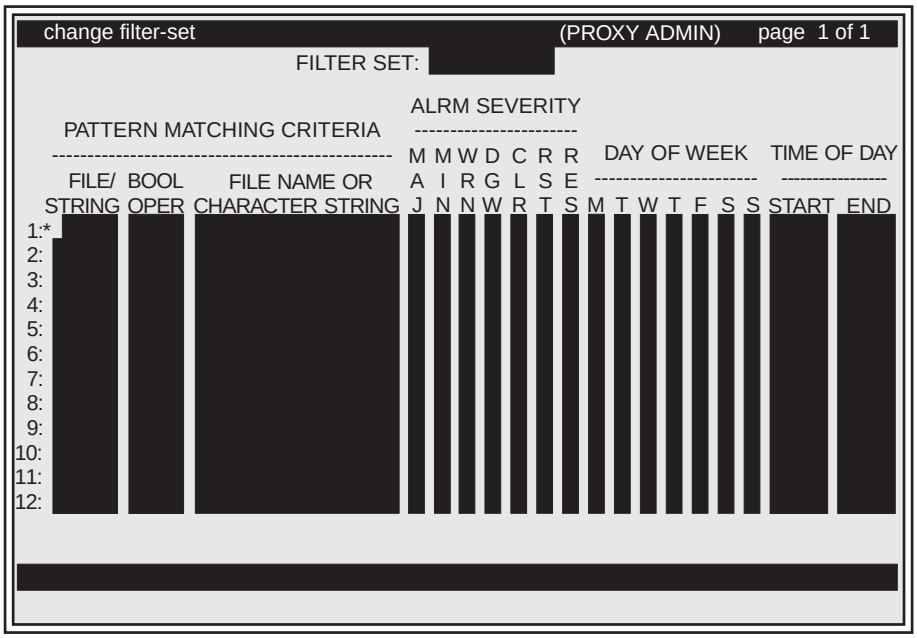
Each filter is explained below:

- 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



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	Contains the name of the filter set. To add a new filter set, the user types the name of the filter set in this field. 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. Field size: 8 characters Default: Blank
Pattern Matching Criteria FILE/STRING	Identifies the type of pattern matching for the filter set. The HELP list (Ctrl-y) contains the valid options: **file** = a pattern file that contains a group of character strings and resides in the **/opt/avaya/mpa/agent/patterns** directory **string** = a character string 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: • Number symbol (#) • Tab • Space Field size: 6 characters Default: Blank
	1 of 4

Table 8: Filter Set Screen (continued)

Field	Description
Pattern Matching Criteria BOOL OPER	Identifies the boolean operator "**not**" as a pattern matching criteria. Users can specify the boolean operator "**not**" if they 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. The HELP list (Ctrl-y) only contains the **not** option**.** Field size: 4 characters Default: Blank
Pattern Matching Criteria FILE NAME or CHARACTER STRING	Identifies the pattern file name or character string based on the selection in the FILE/STRING field. Users can execute one of the options (a, b, or c) below: 1. If *file* 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 *string* was selected in the FILE/STRING field, then users must type a character string in the field. 3. If *no* selection was made in the FILE/STRING field, then users must leave the field blank. Field size: 20 characters Default: Blank

2 of 4

Table 8: Filter Set Screen (continued)

Field	Description
ALRM SEVERITY	Identifies the severity of the alarm filter. Users can select one or more of the days listed below. **NOTE:** The abbreviated titles are vertically stacked above the ALARM SEVERITY columns. **MAJ** = Major **MIN** = Minor **WRN** = Warning **DGW** = Downgraded Warning **CLR** = Cleared Alarm Notification **RST** = Restart Notification **RES** = Resolved Alarm Users can execute one of the options (a or b) below: 1. Type “**x**” in one or more of the fields to select the alarm severity criteria. 2. Leave the fields blank. Field size: 1 Default: Blank
	3 of 4

Table 8: Filter Set Screen (continued)

Field	Description
DAY OF WEEK	Identifies the day or days in the week to block alarm forwarding. Users can select one or more of the days listed below: **M** = Monday **T** = Tuesday **W** = Wednesday **T** = Thursday **F** = Friday **S** = Saturday **S** = Sunday Users can execute one of the options below: • Type "**x**" in one or more of the fields to select the day of week criteria. • Leave the fields blank. Field size: 1 Default: Blank
TIME OF DAY	Identifies the time window to block alarm forwarding. The Time of Day column contains the fields below: **START** field contains the time to begin alarm filtering **END** field contains the time to stop alarm filtering Users must use the 24-hour clock to enter start and end times Users can execute one of the options below: 1. Type the hours in both the START and END fields to select the time of day criteria. 2. Leave the fields blank. **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).
	4 of 4

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,
   - Type **add filter-set**.
   - 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.
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 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.

1. Access the PROXY ADMIN menu.
2. Stop Proxy Agent if it is running (Stopping Proxy Agent on page 34).
3. In the command line on the PROXY ADMIN menu, type **change filter-set** and press **ENTER**.

   The system displays a blank FILTER SET screen.
4. 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.
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.

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 34).
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 33).

8. Display the STATUS screen, verify that Proxy Agent is active, and exit the screen (Displaying the Proxy Agent Status Screen on page 38).

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.

1 of 2

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	Sets the colors for the monitor. Valid options include: **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?	Sets the beep tone to ON or OFF. Valid options include: **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.

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:

- Troubleshooting connections
- 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).

Troubleshooting Connections

The Communication application allows manual connection of Proxy Agent to managed nodes to troubleshoot connection problems. The procedures contain the login prompts to access managed nodes and Communication Manager Feature Servers that are protected by the Access Security Gateway (ASG) software.

The purpose of the **Communication** application is to troubleshoot connections between Proxy Agent and managed nodes.

In all other instances, users access the MANAGED NODES screen to initiate the Proxy Agent connection with individual managed nodes.

There are two types of connection procedures to manually log in to the managed nodes:

- Connecting to Managed Nodes on page 82.
- Connecting to Communication Manager Feature Servers with ASG on page 83.

The login prompts display in separate popup windows on the COMMUNICATION MANAGER screen.

Understanding the Communication Manager Screen

Field Descriptions

The table below contains the descriptions for the fields on the COMMUNICATION MANAGER screen.

Table 11: Communication Manager screen

Connection 1	Contains the first managed node that is currently connected to Proxy Agent. The field is **blank** if a managed node is NOT currently connected. Valid options include: • List of all **managed nodes** administered on Proxy Agent • The **disconnect** command if a managed node is currently connected. The disconnect command does not appear on the list if the field is blank.
Connection 2	Contains the second managed node that is currently connected to Proxy Agent. The field is **blank** if a second managed node is not currently connected. Valid options include: • List of all **managed nodes** administered on Proxy Agent • The **disconnect** command if a managed node is currently connected. The disconnect command does not appear on the list if the field is blank.
STATUS	Identifies the current state of the Proxy Agent connection to a managed node. The valid options for the STATUS states include: **IDLE** -- A dynamic connection is not connected **CONNECTED** -- A managed node is connected This is a view-only field.

Connecting to Managed Nodes

This section contains the procedure to manually login to one or two managed nodes to troubleshoot connections between Proxy Agent and managed nodes.

Required Materials

Users must know the information listed below to complete the procedure:

- Login name for each managed node
- Password to access the each managed node

Procedure

Complete the procedure below to manually login to managed nodes.

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

   The system displays the COMMUNICATION MANAGER screen,
3. In the *Connection 1* field, execute one of the options below:

   a. If the field is blank, then press **Ctrl-Y,** select a managed node from the list, and press **ENTER**.

   b. If the field contains a connection that you want to change, then disconnect the managed node and select a different managed node, as follows:

   - Press **Ctrl-Y**.
   - Select **disconnect** to drop the current connection.
   - Press **ENTER**.
   - Press **Ctrl-Y** again.
   - Select a different **managed node name** for the first connection.
   - Press **ENTER**.

   The system displays the node name in the *Connection 1* field.
4. **Optional**. In the *Connection 2* field, execute one of the options (a or b) in Step 3 above to connect to a second managed node:

   The system displays the node name in the *Connection 2* field.

Note:

If you select a second node name in the Connection 2 field, the system displays the login windows for each of the selected node names. Users must repeat Step 5 through Step 9 below for the second connection.

5. Press **Ctrl-E** to submit the changes.

   The system saves the changes and displays the *login* window for the node name selected in the *Connection 1* field.

6. In the *Login* field, type the managed node login and press **ENTER**.
7. In the *Password* field, type the managed node password and press **ENTER**.

   The system displays the prompt:

   ```
   Save Login/Password for SNMP access (y/n)? n
   ```

8. Execute one of the options below:

   a. To save new login data the first time, press **Y** and press **ENTER**.

   b. To connect to two managed nodes for an administration session, do **NOT** save the login data if the data has been previously saved. Instead, press **ENTER** to select **N** (no).

   The system displays the message:

   ```
   Negotiating protocol communications
   ```

   Then, the system displays the Proxy Agent MAIN MENU that contains the confirmation message: `Connected To managed node`

9. At the completion of the task, complete the procedure to Disconnecting from Managed Nodes on page 86.

Connecting to Communication Manager Feature Servers with ASG

This section contains the procedure to manually connect to Communication Manager Feature Servers that are protected by Access Security Gateway (ASG) and to troubleshoot connections between Proxy Agent and managed nodes.

The ASG login procedure includes the tasks below:

- The user enters a login and optionally saves the ASG secret key at the prompts on the screen. The secret key is a 20-character octal string.
- The system responds with a numeric challenge that contains a 7-digit number.

- To generate a response to the challenge, the user enters the secret key, challenge, and other required data into a hand-held ASG device. The device generates a 7-digit numeric response to the system challenge.
- The user enters the numeric response in the field to gain access to the Communication Manager Feature Server.

Required Materials

Users must know the following information and have the ASG device to complete the ASG login procedure:

- Login name for the Communication Manager Feature Server ASG secret key to access the Communication Manager Feature Server
- Challenge from the Communication Manager Feature Server
- Hand-held ASG device to generate a response to the challenge from the Communication Manager Feature Server

ASG Procedure

Complete the following procedure to manually login to ASG-protected Communication Manager Feature Servers.

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

   The system displays the COMMUNICATION MANAGER screen, in the *Connection 1* field, execute one of the options below:

   a. If the field is **blank**, press **Ctrl-Y,** select a managed node from the list, and press **ENTER**.

   b. If the field contains a connection that you want to change, then disconnect the managed node and select a different managed node:

   - Press **Ctrl-Y**.
   - Select **disconnect** to drop the current connection.
   - Press **ENTER**.
   - Press **Ctrl-Y** again.
   - Select a different **managed node name** for the first connection
   - Press **ENTER**.

   The system displays the selected node name in the *Connection 1* field.
3. **Optional**. In the *Connection 2* field, execute one of the options in Step 2 above to connect to a second managed node:

   The system displays the selected node name in the *Connection 2* field.

Note:

If you selected a second node name in the Connection 2 field, the system displays the ASG login windows for each of the selected node names. You must repeat Step 4 through Step 11 below for the second connection.

4. Press **Ctrl-E** to submit the changes.

   The system saves the changes and displays the *login* window for the node name selected in the *Connection 1* field.

5. In the *Login* field, type the managed node login and press **ENTER**.

   The system displays one of two windows depending on whether or not the login and secret key have been saved.

6. Execute one of the options (a or b) listed below:

   a. To save the login and secret key for new managed nodes, go to Step 7.

   b. To not save the login and secret key for managed nodes, go to Step 8.

7. To save the login data, execute the following steps:

   a. At the prompt, type **Y** (yes) and press **ENTER**.

   The system displays a window with the first prompt:

   `Access Security Gateway (ASG) Secret Key:`

   b. At the prompt, type the **secret key** and press **ENTER**.

   The system displays a second prompt:

   `Save Login & ASG Secret Key for SNMP access (y/n)?`

   c. At the prompt, type **Y** (yes) and press **ENTER**.

   The system displays the window with the numeric challenge: `Challenge: XXX-XXXX`

   d. Go to Step 9 to complete the remaining steps in the procedure.

8. **Do NOT Save the Login**. If the login and ASG secret key have previously been saved, the system displays a window with the prompt: `Would you like to re-save Login/ASG Secret Key for SNMP access (y/n)?`

   To connect to a managed node without saving the ASG and secret key for an emulation session, execute the steps (a and b) below:

   a. At the prompt, type **N** (no) and press **ENTER**.

   The system displays the window with the numeric challenge: `Challenge: XXX-XXXX`

   b. Go to Step 9 to complete the remaining steps in the procedure.

9. **ASG Device**. Access the hand-held ASG device and enter the required data in the device (secret key, challenge, etc.).

   The ASG device displays a 7-digit numeric response.

10. In the *Response* field, type the response number from the ASG device and press **ENTER**.

    The system displays the message: `Negotiating protocol communications`

    Then, the system displays the Proxy Agent MAIN MENU that contains the confirmation message:

    `Connected To managed node`

11. At the completion of the task, complete the procedure to Disconnecting from Managed Nodes on page 86.

Disconnecting from Managed Nodes

Complete the procedure below to manually disconnect the managed nodes.

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

   The system displays the COMMUNICATION MANAGER screen.
3. In the *Connection 1* field, press **Ctrl-Y**, select **disconnect**, and press **ENTER**.
4. **Optional**. In the *Connection 2* field, press **Ctrl-Y**, select **disconnect**, and press **ENTER**.
5. Press **Ctrl-E** to submit the changes.

   The system drops the connections and displays the Proxy Agent MAIN MENU.

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 25.
- Uninstalling Proxy Agent on page 31.

Changing Settings for SNMP Access

See Configuring Proxy Agent on page 25.

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 12: 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
Audit log	/opt/avaya/mpa/agent/logs/auditlog
Error log for alarm sender device	/opt/avaya/mpa/agent/alarms/alarms.log

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 13: 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
   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 14: Commands and Hotkeys

Command	Description
List command **Ctrl-L**	Displays the **Functions** window that contains all of the available commands and associated hotkeys for the current screen. To select an option from the Functions window, • 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**	Displays a help window for a field or a menu, as described below: • 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. To access a help list for a specific field, • 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. To exit a help window without selecting an option, press **ESC**.
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.

1 of 2

Table 14: 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 ***previous*** 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 13.

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 22.

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 14.

Index

Symbols

A

B

C

D

F

H

I

N

P

Q

R

S

T

U

V

W