Avaya MultiVantage™ Proxy Agent

Release 1.3
Installation and Configuration

555-233-139
Issue 4
May 2003

Notice
Every effort was made to ensure that the information in this book 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 followowing website:

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 working on your company's behalf). Be aware that there is 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 s*uspect 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.

How to Get Help
For additional support telephone numbers, go to the Avaya Web site:

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

If you are:

- Within the United States, click *Escalation Lists*, which includes escalation phone numbers within the USA.
- Outside the United States, click *Escalation Lists* then click *Global Escalation List*, which includes phone numbers for the regional 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 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 – an Avaya customer's 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
- 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.

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

Email: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya Web site:

http:www.avaya.com/support/

Table of Contents

Preface

Purpose

This book explains how to install and set up Avaya MultiVantage™ Proxy Agent.

Prerequisites

Installing and configuring MultiVantage Proxy Agent requires familiarity with network administration, knowledge of the Red Hat Linux operating system, and proficiency with Linux administration. This knowledge is not delivered in this book but is essential for a successful installation.

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

Intended Audience

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

Fax: MultiVantage Proxy Agent Documentation Team
+ 1 732 852-2469

E-mail: document@avaya.com

How to Get This Book (and Others) on the Web

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

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

1. Access *http://www.avaya.com/support*.
2. Click **Product Documentation**.
3. Click **System and Network Management**.
4. Locate the heading "Avaya VisAbility Management Suite," and click the link corresponding to the software release.
5. Locate the title of the book, and click the link corresponding to the book.

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 4
Date: May 2003

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

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 MultiVantage™ solutions. The ATAC also designs network configurations to support MultiVantage Proxy Agent and Avaya MultiVantage™ Fault and Performance Manager.

Avaya Remote Network Implementation Services (RNIS)

For this product, RNIS offers customers the following services:

- Verify platform readiness
- Remotely install MultiVantage Proxy Agent
- Configure the network management server for each voice system to be managed by MultiVantage Proxy Agent
- Verify customer acceptance
- Custom on-site services

Avaya Technical Service Organization (TSO)

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

Avaya Contact Information

You may find the following contact information helpful at various times during the process of installing and setting up this product This information was accurate at the time this book went to press. We update this information with each new release of MultiVantage Proxy Agent.

Customers can access only the resources in Table 1 (not Table 2). To view Avaya web sites, Avaya recommends that you use Internet Explorer.

Table 1. Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://support.avaya.com/
Network Management Software Systems Support group	1-800-237-0016.
Remote Network Implementation Services (RNIS)	http://www1.avaya.com/enterprise/who/docs/implementationservices/fullprodinfo.html
Toll Fraud Intervention	1-800-643-2353 prompt 1

Table 2. Avaya Internal Resources

Resource	Contact Information
Avaya Enterprise Management Support	http://aem-support.dr.avaya.com/
Avaya Technology and Consulting (ATAC)	Phone: 1-888-297-4700, prompt 2, 6 Main site (requires a password): http://forum.avaya.com
Remote Network Implementation Services (RNIS)	http://associate2.avaya.com/sales_market/products/data-implementation-services/
VisAbility Management Services Support Plan	http://associate2.avaya.com/solution/support_plans/#Enterprise
VMS001 Form	http://associate2.avaya.com/sales_market/products/data-implementation-services/ Then click “Avaya VisAbility™ Management Suite Configuration Request Form #1.”

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*
Peregrine	Main site: *http://www.peregrine.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

MultiVantage 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 MultiVantage 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 "Avaya Contact Information" on page 12 for the Toll Fraud Intervention phone number.

2 Overview

Avaya MultiVantage™ Fault and Performance Manager together with Avaya MultiVantage™ Proxy Agent provide 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 MultiVantage Proxy Agent work together as an integrated application.

Product Description

MultiVantage Proxy Agent

MultiVantage Proxy Agent is a protocol conversion resource. It resides on a stand-alone personal computer and operates on a Red Hat Linux platform.

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

MultiVantage 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 MultiVantage 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
- MultiVantage solution MIB defines the management data that MultiVantage Proxy Agent collects and converts from the Operations Support System Interface (OSSI) protocol to SNMP
- CONVERSANT, AUDIX, Intuity, Intuity Interchange, and CMS MIB

MultiVantage 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 **/usr/local/avaya/mpa/appl_fls/agent**.

Cache mechanism

The cache mechanism speeds up data access to management information. Due to the nature of the interface to the system data, MultiVantage Proxy Agent does not directly extract the data for each SNMP *GetRequest* or *GetNext Request* message. Therefore, MultiVantage Proxy Agent places the system data in a cache and uses the cached data to respond to requests from the network manager for MIB data.

For example, MultiVantage Proxy Agent will cache data from a system form that contains a table. A series of *GetNextRequests* that are used to parse the table will initiate a single request for that form. MultiVantage Proxy Agent provides the cache data in a set of objects for each cached group. This allows the network manager to make use of the cached data in Fault and Performance Manager.

Cache objects

MultiVantage Proxy Agent creates the cache file when the you establish the first connection to a supported system. MultiVantage Proxy Agent will retrieve any missing cache data when it reconnects to a supported system. You can manually execute the “refresh” command from Fault and Performance Manager.

MultiVantage Proxy Agent adds the following objects to the cache files for each group that uses caching:

- A read-only object that specifies the time since the data in the cache was extracted from the system.
- A read-write object that specifies the time interval for which cached data is considered valid. MultiVantage Proxy Agent uses this value and the age value to determine if the system data needs to be refreshed.
- A read-only object that contains the amount of time that MultiVantage Proxy Agent used to extract the system data.
- A read-write object that indicates the cache contains refreshed data.
- A read-only object that identifies the groups that contain table data and indicates the number entries in the table.

If MultiVantage Proxy Agent encounters voice system command errors during the refresh process, then the cache file will contain null data. However, if an attempt to refresh a cached object fails because of command contention on the voice system, then the existing cache will not be disturbed.

Alarm-to-Trap Conversion

MultiVantage Proxy Agent receives alarm notifications from each supported system that is administered on the MANAGED NODES screen on MultiVantage Proxy Agent.

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

Enterprise traps

MultiVantage 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 MultiVantage Proxy Agent and reside in the **/usr/local/avaya/mpa/appl_fls/agent** directory.

When sending MultiVantage solution alarm traps, MultiVantage 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 MultiVantage Proxy Agent to forward alarms to INADS. When a supported system generates an alarm, MultiVantage Proxy Agent adds a field that contains a sequence number to the end of the alarm stream. MultiVantage Proxy Agent stores the sequence number in the alarm logs.

MultiVantage Proxy Agent uses the sequence number for tracking purposes. MultiVantage Proxy Agent forwards the alarms and the sequence number to INADS or another MultiVantage 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 MultiVantage 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 on the MANAGED NODES screen. The screen also allows you to administer alarm forwarding on a node-by-node basis.

User-defined script

MultiVantage Proxy Agent offers scripts that you can modify to (for example) have a third-party software application page you when MultiVantage Proxy Agent receives an alarm of a particular type. These scripts are located in the /usr/local/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 67.

Alarm filtering

MultiVantage 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 on the MANAGED NODES screen.

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

Reports

MultiVantage 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.

MultiVantage 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 MultiVantage Proxy Agent receives only part of the acknowledgement (ACK) needed to complete the “handshake” between the two systems.

System Security

MultiVantage Proxy Agent supports both MultiVantage Solutions login sessions and the Access Security Gateway (ASG) interface.

Login Security

To safeguard access to supported systems, Avaya strongly recommends that when you create a login on the MultiVantage software, you grant only the minimal permissions that MultiVantage Proxy Agent needs to collect management data. In addition, you should only enable SNMP Set Capability if MultiVantage Proxy Agent is behind a secure fire wall.

Default Login screen

The DEFAULT LOGIN screen lets you enter a system-wide default login and password or ASG key for MultiVantage solutions. The system automatically displays the login and allows the user to modify the password on page E of the MANAGED NODES screen. Refer to "Administering Default Login" on page 55.

This feature reduces the time required to administer large numbers of MultiVantage solutions on MultiVantage Proxy Agent. With this feature, you do not have to manually connect to each MultiVantage solution and save the login data.

ASG login

For MultiVantage solutions that are protected by ASG, MultiVantage Proxy Agent automatically generates a response to a challenge if the login and ASG key have already been administered when you administer new MultiVantage solutions to MultiVantage Proxy Agent.

SNMP Authentication

MultiVantage Proxy Agent provides minimal SNMP authentication through the community strings and node names that you administer on the NETWORK MANAGERS screen and the MANAGED NODES screen. 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.

MultiVantage Proxy Agent Security

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

Supported Systems

MultiVantage Proxy Agent Release 1.3 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 MultiVantage Software Release 1.1 through 1.3. MultiVantage Proxy Agent Release 1.3 supports Avaya MultiVantage Software Release 1.3 on Linux, Oryx-Pecos, and Microsoft Windows platforms.
- Survivable Remote Processors (SRPs)
- MultiPoint Conferencing Unit (MCU) Release 6.0 and later
- Avaya G600 Media Gateway
- Avaya S8100 Media Server with CMC1 Media Gateway

MultiVantage Proxy Agent treats SRPs and MCUs as MultiVantage solutions.

MultiVantage Proxy Agent Release 1.3 supports only SNMP alarms for the following systems:

- DEFINITY AUDIX Releases 3.1 through 4.0
- Intuity AUDIX Release 4.3 or later (with or without the remote maintenance board)
- Intuity Interchange Release 5.1 through 5.3
- Call Management System (CMS) R3V6 through R3V8
- CONVERSANT Release 7.0

System Requirements

Hardware

You should work with your Avaya client team to determine the hardware requirements that meet your business and performance specifications. Your client team has access to the VisAbility Management Suite Services Support Plan, which contains the information they need to help you determine hardware requirements in your situation. Your client team can download the package from the URL listed in Table 2 on page 13.

Hardware Certification

Avaya requires that MultiVantage Proxy Agent hardware must be Red Hat Linux 7.3 certified. For the Red Hat URL, see "Vendor web sites" on page 14.

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

MultiVantage Proxy Agent Release 1.3 operates on a Linux platform, running Red Hat Linux 7.3.

Installation and 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 VisAbility Management Suite Services Support Plan, which is accessible through the customer's client executive.
2. Customers communicate with RNIS to verify server readiness, finalize technical details, and confirm implementation schedule.
3. Installers complete "Installing MultiVantage Proxy Agent" on page 27.
4. Installers complete "Configuring MultiVantage Proxy Agent" on page 29.
5. Installers complete "Administering Network Managers" on page 49.
6. Installers complete "Administering Default Location" on page 59.
7. Installers complete "Administering Alarm Services" on page 63.
8. Installers complete "Specifying Filter Sets" on page 86.
9. Installers complete "Specifying the Default Login" on page 57.
10. Installers complete "Specifying Managed Nodes" on page 108.

3 Installing and Configuring MultiVantage Proxy Agent

This chapter explains how to install and configure MultiVantage Proxy Agent.

Customer Pre-Installation Tasks

Before MultiVantage Proxy Agent can be installed, customers must complete several tasks that are defined in the VisAbility Management Suite Services Support Plan. Your client team can download the plan from the URL specified in Table 2 on page 13.

Installing MultiVantage Proxy Agent

Required Materials

Before you begin, assemble the following:

- Printed copy of this book
- Avaya VisAbility Management Suite CD-ROM set
- Completed VMS001 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 MultiVantage Fault and Performance Manager server
- Default login ID and password or ASG secret key for MultiVantage solutions
- New password for the g3maadm login
- Instructions for installing Red Hat 7.3, which is available from the Avaya Service Centre web site, and also in the "VisAbility Implementation Guidelines" document, which is available from your client executive team.

Procedure

Avaya strongly recommends that you select default installation options whenever appropriate. The default options maintain consistency when upgrading to new releases.

*** Note:** The installation script overwrites previous settings during the installation process.

1. Ask all users to log off the system.
2. Close all open windows and applications.
3. At the login prompt, type **root** and press **ENTER**.
4. At the password prompt, type the root password and press **ENTER.**
5. Insert the "Avaya VisAbility Management Suite: Linux Server Installation" CD.
6. Open a terminal window.
7. Type **cd /mnt/cdrom** and press **ENTER.**
8. At the Linux prompt, type **./vms_setup.bin** and press **ENTER**.
9. Follow the wizard prompts to complete the installation.

Configuring MultiVantage Proxy Agent

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

Understanding SNMP Access

When you configure MultiVantage Proxy Agent, you have the option to enable or disable SNMP access to MultiVantage solution management data. By "SNMP access," we mean SNMP Polling, SNMP Traps, and SNMP Set capabilities, which are explained in this section.

The MultiVantage Proxy Agent configuration script, which you will launch to configure MultiVantage Proxy Agent, contains prompts to enable or disable these features. For MultiVantage Proxy Agent to work properly with Avaya MultiVantage™ 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 MultiVantage 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 MultiVantage 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 MultiVantage Proxy Agent only as an alarm notification device, and not use Fault and Performance Manager.

SNMP polling

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

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

To change these options after MultiVantage 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 MultiVantage Proxy Agent lets you administer up to **600** managed nodes for each instance of MultiVantage Proxy Agent. This option reduces the load on each instance of MultiVantage 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 MultiVantage Proxy Agent is only used for alarming.

SNMP Set Capability

When you configure MultiVantage 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 system date and time (This task is not supported on S8300 and S8700 platforms)

 **SECURITY ALERT:**

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

Running the MultiVantage Proxy Agent Configuration Script

After installing MultiVantage Proxy Agent, complete the following steps:

1. 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:

   ```
   Current setting is SNMP Voice System Access and
   SNMP Alarm Traps ENABLED.

   Please select from one of the following options:

   1) SNMP Voice System Access and SNMP Alarm Traps
   Enabled
   ```

```
2) SNMP Alarm Traps Only

3) Alarm Processing Only (NO SNMP Support)

Enter your selection [1]:
```

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

Selecting 1 enables SNMP polling and allows MultiVantage 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 MultiVantage Proxy Agent has the ability to allow
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:
```

3. 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:
```

4. 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 MultiVantage™ Fault and Performance Manager.

— Busy-out and release alarms

— Set the system date and time (Not supported on S8300 and S8700)

Then the system displays the prompt:

```
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]:
```

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

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

   b. If MultiVantage 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 System's has been
   enabled.

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

   Changing password for user g3maadm.

   New password:
   ```

6. Type and retype a new `g3maadm` password, pressing **ENTER** after each entry.

   The system administers the `g3maadm` login and then displays the message:

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

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

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

   Select the function for this device:

   [R] Receive Alarms

   [S] Send Alarms

   Or, select one of the options below:

   [N] Next Device (skip this one)

   [X] Exit Modem Setup and continue the
   installation

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

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

   a. If the device name is on the VMS001 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 VMS001 form, then type **N** and press **ENTER**.

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

8. (As appropriate) Repeat **Step 7** for each device.

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

   The system displays the message:

   ```
   Done setting up Devices.
   ```

   Finally, the system displays the message:

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

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

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

11. Go to **Step 5** (on page 25) of the **Installation and Configuration Overview**.

Uninstalling MultiVantage Proxy Agent

Only root users should uninstall MultiVantage Proxy Agent. This section explains only how to remove MultiVantage Proxy Agent. For information on removing Linux, refer to the Linux system documentation.

1. Ask all users to log off the system.
2. Stop MultiVantage Proxy Agent (see page 38).
3. Close all open windows and applications.
4. Log off the system.
5. At the login prompt, type **root** and Press **ENTER**.
6. At the password prompt, type the root password and press **ENTER**.
7. Open a terminal window.
8. Type **cd /usr/local/avaya/uninstall** and press **ENTER.**
9. Type **. /uninstaller.bin** and press **ENTER.**

   The installation wizard appears.
10. Select the feature to be removed (the system defaults to all the features already installed)
11. Click **Next** and follow the prompts.

4 Accessing MultiVantage Proxy Agent

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

Logging in to MultiVantage 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 MultiVantage 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 39.

   — 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 MultiVantage Proxy Agent

Complete the following procedure to start a MultiVantage Proxy Agent connection.

1. For this procedure, you must start by typing **proxy-admin** and pressing **ENTER** in **Step 5** on page 37.

   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 MultiVantage 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 MultiVantage Proxy Agent is active. See "Understanding the MultiVantage Proxy Agent Status Screen" on page 43.

Stopping MultiVantage Proxy Agent

As explained in the section, "Understanding the Proxy Admin Screen" on page 40, you must stop MultiVantage Proxy Agent before you can enter an **add, remove,** or **change** command. You do not have to stop MultiVantage Proxy Agent when entering a **display** command.

CAUTION:

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

Complete the following procedure to stop a MultiVantage Proxy Agent connection.

1. For this procedure, you must start by typing type **proxy-admin** and pressing **ENTER** in **Step 5** on page 37**.**

   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 MultiVantage Proxy Agent and then displays the PROXY ADMIN screen with the confirmation message:

   ```
   Command completed successfully.
   ```

4. Display the STATUS screen to verify that MultiVantage Proxy Agent is not active. See "Understanding the MultiVantage Proxy Agent Status Screen" on page 43.

Understanding the Main Menu

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

Table 4. MultiVantage Proxy Agent MAIN MENU

Command	Description
communication	Accesses the **Communication** application and displays the COMMUNICATION MANAGER screen. Users can manually connect and disconnect a MultiVantage Proxy Agent to and from managed nodes. Refer to "Troubleshooting Connections" on page 120.
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 115.
proxy-admin	Accesses the PROXY ADMIN menu. Refer to "Understanding the Proxy Admin Screen" on page 40.
exit	Closes the MultiVantage 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 MultiVantage Proxy Agent administration screens and to start and stop MultiVantage Proxy Agent.

Displaying the Proxy Admin Screen

Complete the procedure below to display the PROXY ADMIN screen.

1. Complete "Logging in to MultiVantage Proxy Agent" on page 37.
2. In **Step 5** on page 37, 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 MultiVantage 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 MultiVantage Proxy Agent before executing the **add** command. Refer to "Administering Filter Sets" on page 73.
	(Sheet 1 of 3)

Table 5. PROXY ADMIN screen

Command	Description
remove	Accesses the FILTER SET screen in the "remove" mode. Users can delete existing alarm filters with this command. *** Note:** You must STOP MultiVantage Proxy Agent before executing the **remove** command. MultiVantage 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 "Administering Filter Sets" on page 73.
change	Accesses the administration screens. The **change** command allows users to edit the selected screen. *** Note:** Users must STOP MultiVantage Proxy Agent before executing the **change** command. • **change network-managers** See "Understanding the Network Managers Screen" on page 49. • **change default-location** See "Understanding the Default Location Screen" on page 60. • **change alarm-devices** See "Understanding the Alarm Devices Screen" on page 64. • **change filter-set** See "Understanding the Filter Set Screen" on page 79. • **change managed-nodes** See "Understanding the Managed Nodes Screen" on page 95. • **change default login** See "Specifying the Default Login" on page 57.
	(Sheet 2 of 3)

Table 5. PROXY ADMIN screen

Command	Description
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 MultiVantage Proxy Agent before executing the *display* command. • **display alarm-devices** • **display filter-set** • **display default-location** • **display default-login** • **display managed-nodes** • **display status** -- See "Displaying the MultiVantage Proxy Agent Status Screen" on page 43.
start	Initiates an MultiVantage Proxy Agent connection to the managed nodes. See "Starting MultiVantage Proxy Agent" on page 38.
stop	Drops the MultiVantage Proxy Agent **connection** to the managed nodes. See "Stopping MultiVantage Proxy Agent" on page 38.
quit	Closes the PROXY ADMIN screen and displays the MultiVantage Proxy Agent MAIN MENU.
	(Sheet 3 of 3)

Understanding the MultiVantage Proxy Agent Status Screen

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

- Verify that the MultiVantage 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 MultiVantage Proxy Agent Status Screen

Complete the following procedure to display the STATUS screen.

1. In **Step 5** on page 37, 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.

MultiVantage Proxy Agent Status Screen Description

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

- Status of MultiVantage Proxy Agent
- Alarm forwarding state
- Node name and state
- Connection statistics (only for the DEFINITY ECS, MCU, and Avaya MultiVantage™ S8100 Media Server with Avaya™ G600 Media Gateway managed nodes)

*** Note:** To view the status of MultiVantage 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 MultiVantage Proxy Agent computer)

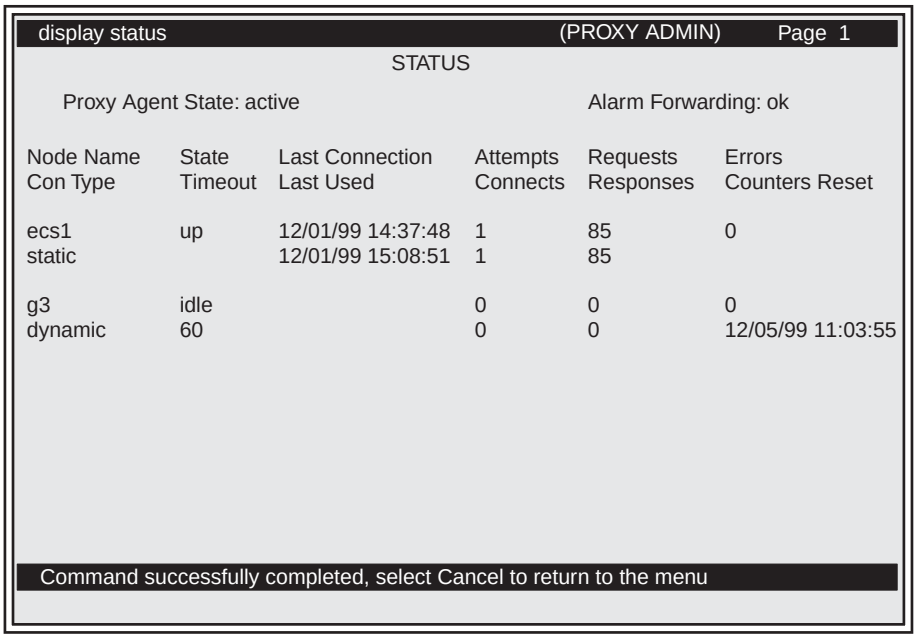
The STATUS screen does not display any connection statistics for the following managed nodes. MultiVantage Proxy Agent supports only alarm handling for these products.

- 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
- Intuity Interchange
- S8100 AUDIX
- Call Management System (CMS)
- MCU

Figure 1. STATUS screen



sdnmdst LJK 092299

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 MultiVantage Proxy Agent: • **active** -- The Proxy Agent has been started • **not active** -- The Proxy Agent has been stopped
	(Sheet 1 of 3)

Table 6. STATUS screen

Column	Description
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 MANAGED NODES screen. 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: — MultiVantage 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 MultiVantage 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)
State	Identifies the current status of MultiVantage 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
	(Sheet 2 of 3)

Table 6. STATUS screen

Column	Description
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.
	(Sheet 3 of 3)

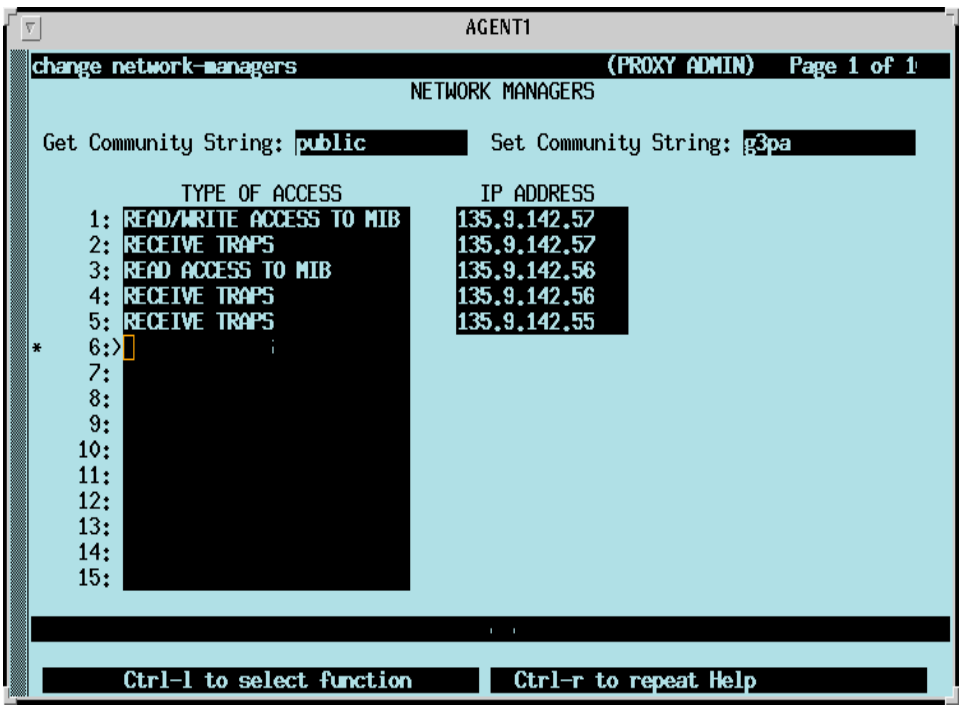
5 Administering Network Managers

When you “administer network managers,” you are telling MultiVantage Proxy Agent the IP addresses of the “network managers” that can communicate with MultiVantage Proxy Agent or receive information from it. By “network managers” we mean any network device that accesses MultiVantage Proxy Agent using SNMP; for example, the System Management Server or the computer that hosts HP OpenView Network Management System (NMS).

Understanding the Network Managers Screen

This screen lets you set up the communication link between MultiVantage Proxy Agent, the System Management Server, and the HP OpenView NMS.

Figure 2. Network Managers screen



See also

— "Management Information Base (MIB)" on page 18

— "Cache mechanism" on page 18

— "SNMP Authentication" on page 22

Field Descriptions

The table below describes the fields in the NETWORK MANAGERS screen.

Table 7. Network Managers Screen

Field	Description
Get Community String	Identifies MultiVantage Proxy Agent's SNMP Get Community String. The NMS uses this to validate SNMP get requests. Valid options for this field 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.** Required field. Field size: 15 characters
Set Community String	Identifies MultiVantage Proxy Agent's Set Community String. The NMS uses this to validate SNMP set requests. Valid options for this field 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.** Required field. Field size: 15 characters
	(Sheet 1 of 2)

Table 7. Network Managers Screen

Field	Description
TYPE OF ACCESS	Identifies the type of access a network manager has to MultiVantage Proxy Agent. • **Read/Write access to MIB** -- allows the NMS to read and write data to the MIB. *** Note:** Fault and Performance Manager requires read/write access. • **Read access to MIB** -- allows the NMS only to read data in the MIB. The NMS cannot change MIB objects that are set with the SNMP SET command. • **Receive Traps** -- allows the NMS to receive SNMP traps from MultiVantage Proxy Agent. *** Note:** Fault and Performance Manager requires SNMP trap reception. Default: **READ/WRITE ACCESS TO MIB** in line 1
IP ADDRESS	Identifies the IP address of the NMS. Valid options for this field are: • Asterisk (*****) -- default in line 1. The asterisk allows access to all NMS network managers. The asterisk is **not** valid for RECEIVE TRAPS access. or • IP address of the NMS in dot format. Example: 126.1.205.86 **SECURITY ALERT:** **You should enter the IP address for each network manager to limit access to the MIB.** Required field. Field size: 15 characters
	(Sheet 2 of 2)

Specifying Network Manager Locations and MIB Access

This procedure provides the System Management Server and the NMS with access to SNMP data collected from the managed nodes. The System Management Server and the NMS use this data to populate the tables and graphical displays in the appropriate Avaya MultiVantage™ Fault and Performance Manager (Fault and Performance Manager) screens.

In this process, you add both the Network Management Server and the NMS as "network managers," and you assign the type of access that each has to the MultiVantage Proxy Agent Management Information Base (MIB).

You can administer three types of access for each network manager:

- Read/Write Access to MIB
- Read only Access to MIB
- Receive Traps

You assign each type of access on a separate line in the NETWORK MANAGERS screen.

Procedure

Complete the procedure below to add new network managers or to change data for existing network managers.

1. At the MAIN MENU, Type **proxy-admin** and press **ENTER.**

   The system displays the PROXY ADMIN menu.

2. If MultiVantage Proxy Agent is running, type **stop proxy-agent** and press **ENTER.**

3. Type **change network-managers** and press **ENTER.**

   The system displays the NETWORK MANAGERS screen.

4. Compare the data on the VMS001 form to the fields on the NETWORK MANAGERS screen:

   `Get Community String`: **public**

   `Set Community String`: **g3pa**

   If the data does not match, then change the fields to match the data on the VMS001 form.

5. For each network manager, grant READ/WRITE ACCESS TO MIB permission, as follows:

   a. In the **TYPE OF ACCESS** column, move the cursor to a blank line number.

   b. Press **Ctrl-Y.**

   c. Select **READ/WRITE ACCESS TO MIB**

   d. Press **ENTER** to display the selection in the field

   e. In the **IP ADDRESS** column, type the IP address in the field for the same line number.

6. For each network manager, grant RECEIVE TRAPS permission, as follows:

   a. In the **TYPE OF ACCESS** column, move the cursor to a blank line number.

   b. Press **Ctrl-Y.**

   c. Select **RECEIVE TRAPS**

   d. Press **ENTER** to display the selection in the field.

   e. In the **IP ADDRESS** column, type the **IP address** in the field for the same line number.

      The IP address should match the address in Step 5e for each network manager.

7. Repeat Steps 5 and 6 for each network manager.

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

   The system saves the data and displays the PROXY ADMIN menu.

9. Go to **Step 6** (on page 25) of "**Installation and Configuration Overview**."

6 Administering Default Login

The DEFAULT LOGIN screen lets you enter a system-wide default login and password or Access Security Gateway (ASG) key for MultiVantage solutions. You can change the default login data for individual MultiVantage solutions on page E of the MANAGED NODES screen. This feature reduces the time to administer large numbers of new MultiVantage solutions on Avaya MultiVantage Proxy Agent.

SECURITY ALERT:

When you enter the data in the Password/ASG Key field, the characters that appear are periods. The periods only appear in the field during the time that you are entering the password or ASG key. When you return to the screen, the system displays only the data in the Login field. For security reasons, MultiVantage Proxy Agent stores the password or ASG key but leaves the Password/ASG Key field blank.

ASG login

For MultiVantage solutions that are protected by the ASG system, MultiVantage Proxy Agent uses the default ASG Key to automatically generate a response to a challenge when connecting automatically to a MultiVantage solution.

Understanding the Default Login Screen

Field descriptions

The table below contains the field descriptions for the DEFAULT LOGIN screen.

Table 8. Default Login Screen

Field	Description
Login ID	Identifies the **login name** for the MultiVantage solution. MultiVantage Proxy Agent displays the login ID on this screen and on page E of the MANAGED NODES screen when you administer new MultiVantage solutions on MultiVantage Proxy Agent. Field size: 20 characters Validation: None Default: Blank
Password/ASG Key	Displays periods while entering the password or ASG key in this field for the default password or ASG key to access all MultiVantage solutions administered on MultiVantage Proxy Agent. MultiVantage Proxy Agent saves the default password or ASG key but leaves the fields blank on the DEFAULT LOGIN screen. On page E of the MANAGED NODES screen, MultiVantage Proxy Agent displays periods in the field. For MultiVantage solutions that are protected by the Access Security Gateway (ASG) system, MultiVantage Proxy Agent uses the default ASG Key to automatically generate a response to a challenge when connecting automatically to a MultiVantage solution. Field size: 20 characters Validation: None Default: Blank

Specifying the Default Login

This section contains the procedure to administer the default login and password or ASG key on the DEFAULT LOGIN screen.

Required materials

You will need the following information and materials:

- MultiVantage solution login name
- MultiVantage solution password or ASG secret key

SECURITY ALERT:

For security reasons, the VMS001 form does NOT contain the password or ASG secret key for the MultiVantage Solutions.

Procedure

Complete the following steps to administer login data for new MultiVantage solutions.

1. Access the PROXY ADMIN menu.
2. Stop MultiVantage Proxy Agent if it is running (page 38).
3. In the command line on the PROXY ADMIN menu, type **change default-login** and press **ENTER.**

   The system displays the DEFAULT LOGIN screen.
4. In the *Login ID* field, type the default login that you use when adding new supported systems to the MANAGED NODES screen.
5. In the *Password/ASG Key* field, type the corresponding password or ASG secret key.
6. Press **Ctrl-E** to submit the changes.

   The system saves the changes and displays the PROXY ADMIN menu.
7. Go to **Step 9** (on page 25) of "**Installation and Configuration Overview**."
8. Restart MultiVantage Proxy Agent (page 38).

7 Administering Default Location

By "administering default location," we mean choosing the map that you want to use to view managed nodes and their associated instances of MultiVantage Proxy Agent. The DEFAULT LOCATION screen lets you select this map.

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. Selecting a default using this screen means that you do not have to specify a submap for each individual node using the MANAGED NODES screen. When you specify a default using the DEFAULT LOCATION screen, any new managed node 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 that you specify there overrides the map selection that you made on the DEFAULT LOCATION screen, but only for that managed node.

Understanding NMS Maps

The HP OpenView NMS displays the submaps in a graphical format with icons that represent the managed nodes and MultiVantage Proxy Agent. You can monitor the health and status of all the managed nodes from the submaps.

Icons

The color of the managed node icons identifies the health status of the managed nodes. The icon color changes to indicate the highest severity level of any Fault and Performance Manager exception that has occurred on the managed node.

Connecting Lines

Broken or solid lines between MultiVantage Proxy Agent and managed nodes indicates either a static or dynamic connection. The color of the line indicates the connection status.

Understanding Types of SubMaps

You can organize managed nodes by selecting any combination of the following types of submaps.

- **Generic submap** -- Select the generic submap to view all the managed nodes and MultiVantage Proxy Agent computers on one submap. The generic submap is the system default.
- **USA submap** -- 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 submap** -- Select the custom submap to organize the managed nodes by categories, such as private networks, regions, functions, or international locations. Use the associated Submap Name to identify groups or locations within the categorizes, 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, Greece groups

Understanding the Default Location Screen

The fields that appear on the DEFAULT LOCATION screen depend on the type of submap that you select as the default.

Generic submap screen

The DEFAULT LOCATION screen for the generic submap contains the Submap Type field.

USA submap screen

The DEFAULT LOCATION screen for the USA submap has the following fields: Submap Type and State.

Custom submap screen

The DEFAULT LOCATION screen for the custom map has the following fields: Submap Type and Submap Name.

Field descriptions

The table below describes the fields for the DEFAULT LOCATION screen.

Table 9. Default Location Screen

Field	Description
Submap Type	Identifies the **type** of submap. Valid options for this field are: **generic** (default) **usa** **custom** The fields that appear depend on the type of submap: • If you select **usa**, the system displays the **State** field • If you select **custom**, the system displays the **Submap Name** field You can change the submap type for individual managed nodes on page **B** of the MANAGED NODES screen.
State	If you select **usa** in the *Submap Type* field, the system displays the **State** field. Valid options for this field are the **50** states. Select the state corresponding to the location of the managed nodes. When you administer the managed nodes on the MANAGED NODES screen, you can change the state location for individual managed nodes. System default: Alabama
Submap Name	If you select **custom** in the *Submap Type* field, the system displays the **Submap Name** field. You can type a default name for the custom submaps. When you administer the managed nodes on the MANAGED NODES screen, then you can change the submap name for individual managed nodes. Default: Blank Field size: 40 characters

Selecting a Default Submap

Complete the procedure below to select a default submap.

1. Access the PROXY ADMIN menu.
2. Stop MultiVantage Proxy Agent if it is running.
3. In the command line on the PROXY ADMIN menu, type **change default-location** and press **Enter.**

   The system displays the DEFAULT LOCATION screen.
4. In the *Submap Type* field, Press **Ctrl-Y** to display field options.
5. Select a submap type from the list.
6. Press **ENTER**.
7. Go to the appropriate step for the selected submap:
   - **usa** (go to **Step 8**)
   - **custom** (go to **Step 9**)
   - **generic** (go to **Step 10**)
8. **USA submap type.** In the *State* field,
   a. Press **Ctrl-Y** to display the field options.
   b. Select a state from the list
   c. Press **ENTER.**
   d. Go to **Step 10**.
9. **Custom submap type.** In the *Submap Type* field,
   a. Type a custom name for the default location.
   b. Go to **Step 10**.
10. Press **Ctrl-E** to submit the changes.

    The system saves the changes and displays the PROXY ADMIN menu.
11. Go to **Step 7** (on page 25) of "**Installation and Configuration Overview**."

8 Administering Alarm Services

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

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

- DEFINITY ECS, MCU, and Avaya MultiVantage™ S8100 Media Server with Avaya™ G600 Media Gateway systems
- DEFINITY AUDIX
- Intuity AUDIX
- Intuity AUDIX LX
- Intuity Interchange
- S8100 AUDIX
- Call Management System (CMS)
- CONVERSANT system

By default, MultiVantage 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 MultiVantage 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.

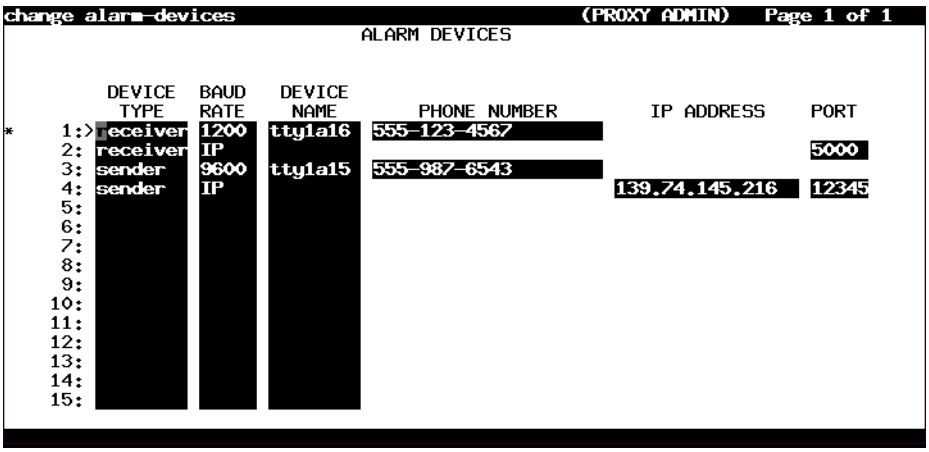
See also

To troubleshoot alarm problems, refer to "Viewing Alarm and Error Logs" on page 129.

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 3. Alarm Devices screen



Field descriptions

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

Table 10. 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
	(Sheet 1 of 2)

Table 10. Alarm Devices Screen

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
	(Sheet 2 of 2)

Specifying Alarm Devices

Complete the procedure below to administer the ALARM DEVICES screen to receive and forward alarms. Refer to the VMS001 form for the information that you need to complete the fields on the screen.

1. Access the PROXY ADMIN menu.
2. Stop MultiVantage Proxy Agent if it is running (page 38).
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 8** (on page 25) of "**Installation and Configuration Overview**."

12. Restart MultiVantage Proxy Agent (page 38).

Building Custom Alarm Scripts

MultiVantage Proxy Agent calls a script, located in the /usr/local/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 MultiVantage Proxy Agent are not set up. You must modify them to meet your needs.

Script directories

The following sample scripts are located in the **/usr/local/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.

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

— MultiVantage solutions

— MCU

— Avaya S8100 Media Server with Avaya™ G600 Media Gateway

— Avaya S8100 Media Server with CMC1 Media Gateway

Then MultiVantage 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 MultiVantage 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

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

- DEFINITY AUDIX
- Intuity AUDIX
- Intuity Interchanges

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

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

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

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

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

9 Administering Filter Sets

MultiVantage 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 MultiVantage 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, MultiVantage Proxy Agent compares each record in the filter set for a match against the alarm. If MultiVantage Proxy Agent finds a match for any filter record, then it does not forward the alarm to INADS. If MultiVantage 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 MultiVantage Proxy Agent blocks the alarm.

Default filter-set

When you install Release 1.2 of MultiVantage 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 MultiVantage 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, MultiVantage 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 MultiVantage 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 **/usr/local/avaya/mpa/agent/patterns** directory. The format for the pattern file contains a group character strings that MultiVantage 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 MultiVantage Proxy Agent to block alarms that do not match a specified pattern matching criteria.

If the boolean operator (BOOL OPER) field is blank, then MultiVantage 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)

MultiVantage 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). MultiVantage 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 MultiVantage 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.

MultiVantage 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 **/usr/local/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 MultiVantage software maintenance object names:

ANL_LINE

ANL_BD

DIG_LINE

MET_LINE

MET_BD

The trunk pattern file contains a list of MultiVantage software trunk maintenance object names:

AUX_TRK

CO_TRK

DID_TRK

TIE_TRK

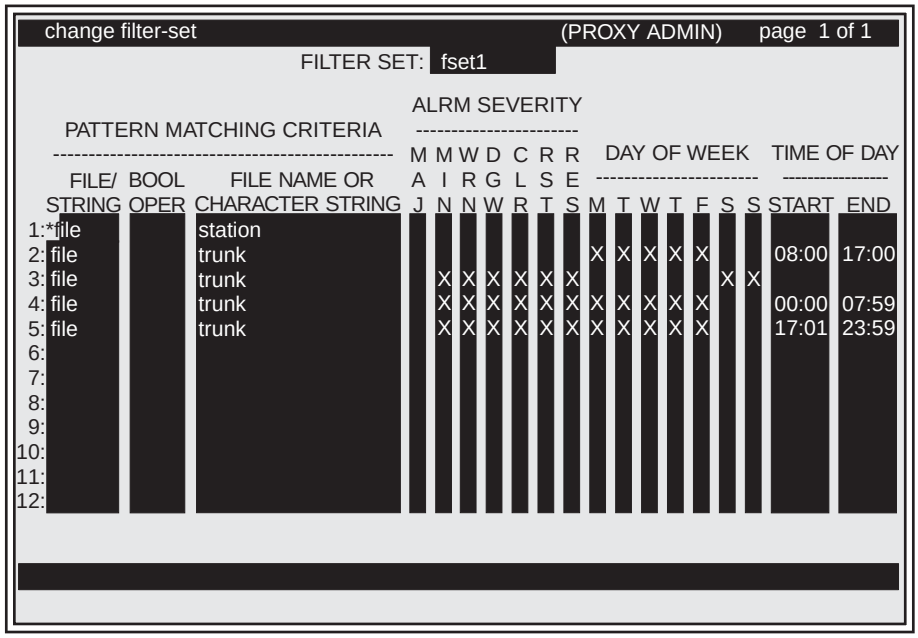
ISDN_TRK

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 4. Example of Filter Set 1 (fset1)



sdnmfst1 LJK 092399

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.)

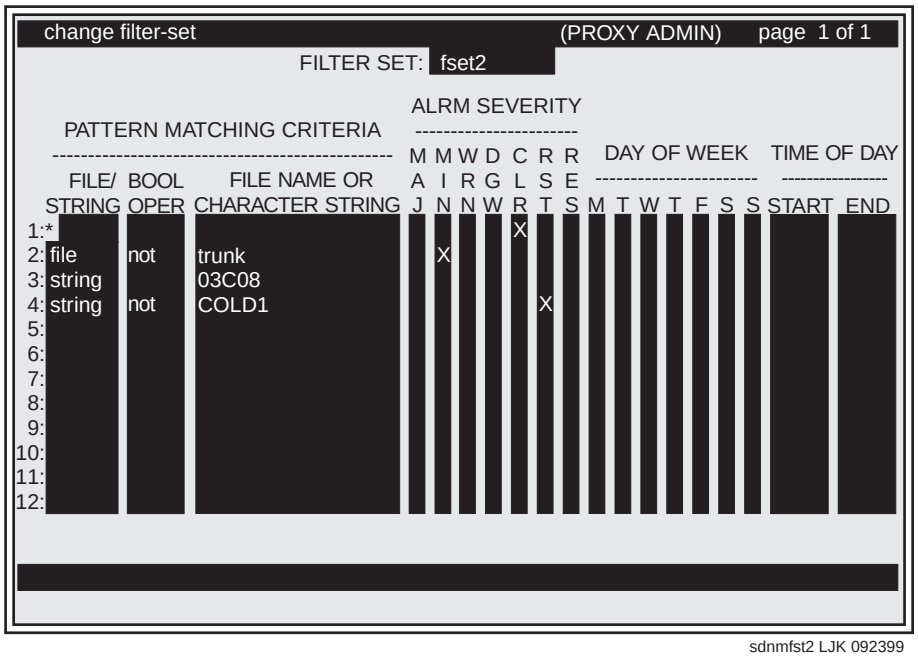
- Filters 3 through 5, together, block the forwarding of all **non-major trunk** alarms received during **off** hours:
  - — Filter 3 blocks non-major trunk alarms on Saturday and Sunday
  - — Filter 4 blocks non-major trunk alarms on Monday through Friday *before* working hours (0:00 to 07:59)
  - — 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 5. Example of Filter Set 2



sdnmfst2 LJK 092399

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.

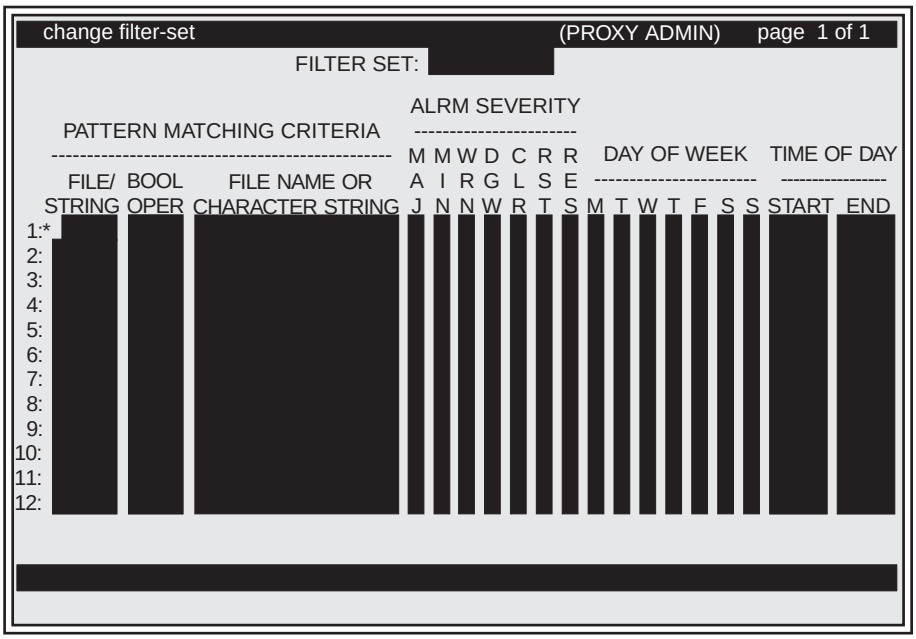
Each filter is explained below:

- 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 6. Blank Filter Set screen



sdnmfsbl LJK 092399

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 11. 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
	(Sheet 1 of 6)

Table 11. Filter Set Screen

Field	Description
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 **/usr/local/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 MultiVantage 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
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 MultiVantage Proxy Agent to block alarms that do not match a specified pattern matching criteria. If the boolean operator (BOOL OPER) field is blank, then MultiVantage 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
	(Sheet 2 of 6)

Table 11. Filter Set Screen

Field	Description
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 ***/usr/local/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
	(Sheet 3 of 6)

Table 11. Filter Set Screen

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
	(Sheet 4 of 6)

Table 11. Filter Set Screen

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
	(Sheet 5 of 6)

Table 11. Filter Set Screen

Field	Description
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).
	(Sheet 6 of 6)

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 MultiVantage 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 MultiVantage 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:

a. Leave the field blank.

b. 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:

a. If you selected **file**, then press **Ctrl-Y** and select a **pattern file** from the list. Press **ENTER**.

b. If you selected **string**, then type a **character string** in the field.

c. 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 steps 5 through 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.

11. **New Installation**. Complete the procedure to "Specifying the Default Login" on page 57.

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 MultiVantage Proxy Agent if it is running (page 38).
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:

   a. Leave the field blank.

   b. 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:

   a. If you selected **file**, then press **Ctrl-Y** and select a **pattern file** from the list. Press **ENTER**.

   b. If you selected **string**, then type a **character string** in the field.

   c. 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 steps 5 through 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.

11. Go to **Step 9** (on page 25) of "**Installation and Configuration Overview**."

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 MultiVantage 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

MultiVantage 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 MultiVantage Proxy Agent displays a warning message. The message explains that if you remove the filter set, MultiVantage 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 MultiVantage Proxy Agent.

1. Access the PROXY ADMIN menu.
2. Stop MultiVantage Proxy Agent if it is running (page 38).
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 MultiVantage Proxy Agent (page 38).
8. Display the STATUS screen, verify that MultiVantage Proxy Agent is active, and exit the screen (page 43).

10 Administering Managed Nodes

The MANAGED NODES screens contain the individual settings and options for each supported system that users administer on MultiVantage Proxy Agent. Generally, you administer all management tasks from the MANAGED NODES screen.

The MANAGED NODES screen contains the individual values for each managed node administered on MultiVantage Proxy Agent.

You access the MANAGED NODES screen to execute the tasks listed below:

- Add new managed nodes to MultiVantage Proxy Agent
- Change data for existing managed nodes
- Set the “forward alarms” option for managed nodes
- Select a filter set for individual managed nodes
- Select MultiVantage Proxy Agent connection type and “start state” for individual managed nodes
- Change the submap type for individual managed nodes
- Change the system parameters of communication devices for individual managed nodes
- Reset the statistics counter for the node being administered
- Select login ID and password/ASG key for new MultiVantage solutions administered on MultiVantage Proxy Agent

Default parameters

MultiVantage Proxy Agent automatically loads the system-wide default parameters in the applications listed below:

- DEFAULT LOGIN
- FILTER SET
- ALARM DEVICES
- DEFAULT LOCATION

When you add new managed nodes, the system displays the default parameters in the fields on the MANAGED NODES screens.

You can change the parameters on the MANAGED NODES screen for individual managed nodes. The changes override the system default values only for the specific managed node.

Static and Dynamic connections

MultiVantage Proxy Agent supports both static and dynamic connections. Additionally, MultiVantage Proxy Agent supports only the number of active connections specified during installation. The active connections can be any combination of both static and dynamic connections.

The number of static connections cannot be greater than the number specified during configuration.

The following are examples of scenarios for assigning static and dynamic connections if you specified 30 active connections and support for 150 managed nodes during installation:

- If you assign 25 **static** connections, the system allows you to add 125 managed devices with **dynamic** connections. This frees 5 ports to connect to the 125 managed nodes with dynamic connections.
- If you assign 10 **static** connections, then the system allows you to add 140 managed devices with **dynamic** connections. This frees 20 ports to connect to 140 managed devices with dynamic connections.

Avaya recommends that if you collect hourly data on certain MultiVantage solutions, you should administer only the number of static connections specified during installation. This will ensure continuous and accurate data collection for those systems.

You can resolve these limitations by adding additional MultiVantage Proxy Agent servers and then spreading the static connections across them.

Understanding the Managed Nodes Screen

The MANAGED NODES screen is similar to a spreadsheet. The screen contains 100 pages, with 15 lines per page. The lines are consecutively numbered 1 to 1500 to identify each managed node that is connected to a specific MultiVantage Proxy Agent.

The example below shows the line numbers on the pages:

- Page 1 contains numbered lines 1 through 15
- Page 2 contains numbered lines 16 through 30, etc.

In addition, each of the 100 pages contains 5 subpages (a through e). The subpages contain fields to administer each managed node.

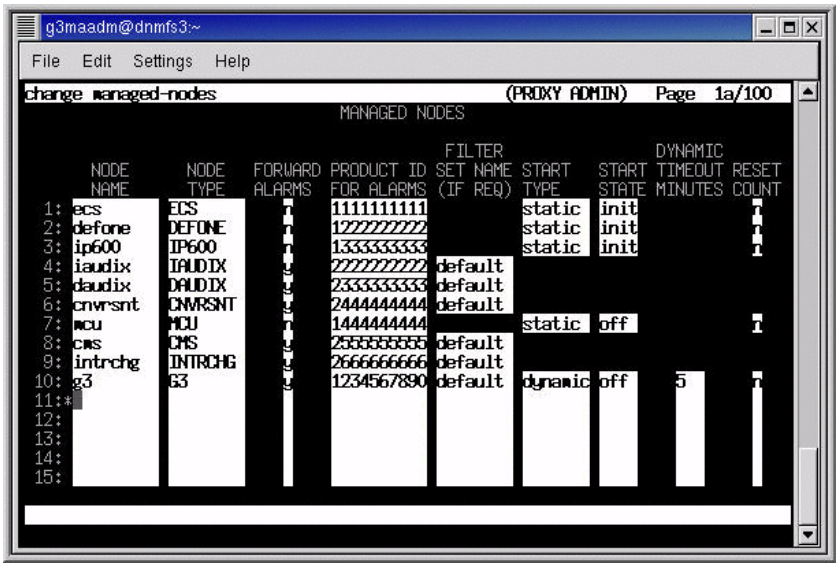
The example below shows the page number for subpages (1 through 100):

- Page 1 subpages are numbered: 1a/100, 1b/100, 1c/100, 1d/100, 1e/100
- Page 2 subpages are numbered: 2a/100, 2b/100, 2c/100, 2d/100, 2e/100, *etc.*

Fields on Page A

The figure below shows page **A** of the MANAGED NODES screen. Page **A** contains the basic fields to administer managed nodes and MultiVantage Proxy Agent.

Figure 7. Page A of the MANAGED NODES screen



Page A field descriptions

The table below contains the field descriptions for page **A** of the MANAGED NODES screen.

Table 12. Page A of the Managed Nodes screen

Field	Description
NODE NAME	Identifies the name of the system you administer on MultiVantage Proxy Agent as a managed node. The node name occupies the same line number on each of the five (5) lettered pages. Avaya recommends that you use all lower-case letters to define the Node Name. The node name on MultiVantage Proxy Agent must match the managed node name on the HP OpenView Network Management System (NMS). You can change the node name without having to re-enter data in the other fields. If you delete the NODE NAME field, the system automatically clears the data from all fields in the numbered row on each of the 5 lettered subpages. Field size: 9 characters. Required field.
	(Sheet 1 of 7)

Table 12. Page A of the Managed Nodes screen

Field	Description
NODE TYPE	Identifies the type of managed node that is associated with a specific instance of MultiVantage Proxy Agent. Valid options include: **ECS** (default) = DEFINITY release 5 and later **DEFONE** = Avaya MultiVantage™ S8100 Media Server **IP600** = Avaya MultiVantage™ S8100 Media Server with Avaya™ G600 Media Gateway **MCU** = Multipoint Conferencing Unit *** DAUDIX** = DEFINITY AUDIX *** IAUDIX** = Intuity AUDIX *** INTRCHG** = Intuity Interchange *** CMS** = Call Management System *** CNVRSNT** = CONVERSANT ***** If you select one of these systems, the screen does not display the following fields: Reset Count; Start State; Start Type; or Dynamic Timeout.
	(Sheet 2 of 7)

Table 12. Page A of the Managed Nodes screen

Field	Description
FORWARD ALARMS	Indicates the alarm forwarding feature is on or off for the individual managed nodes. Valid options include: **Y** = (yes) alarm forwarding is on **N** = (no) alarm forwarding is off The default values differ for type of managed nodes: **Y** = default for MCU, DAUDIX, IAUDIX, INTRCHG, CMS, and CNVRSNT **N** = default for DEFINITY ECS and Avaya MultiVantage™ S8100 Media Server with Avaya™ G600 Media Gateway *** Note:** If you turn on the FORWARD ALARM option, you should verify that the ALARM DEVICES screen is administered to receive alarms from managed nodes and to forward alarms to INADS. Forwarding is subject to filtering as defined in filter set field.
PRODUCT ID FOR ALARMS	Identifies the product identification (ID) number of the managed node. Size: 10 characters Required field.
	(Sheet 3 of 7)

Table 12. Page A of the Managed Nodes screen

Field	Description
FILTER SET NAME (IF REQ)	Identifies the name of the filter set that MultiVantage Proxy Agent applies to alarms received from the managed node. MultiVantage Proxy Agent assigns the default filter set to new managed nodes. To activate the filter set features, you must administer the screens described below: • You must administer the alarm source and alarm destination fields on the ALARM DEVICES screen. Refer to "Specifying Alarm Devices" on page 66. • You can add, change, or remove filters on the FILTER SET screen. For new installations, the default filter set is blank. You can add filtering criteria to the default filter set or leave it blank. Refer to "Specifying Filter Sets" on page 86. • You must also select "**Y**" (yes) in the FORWARD ALARM field on the page A of the MANAGED NODES screen. Refer to procedures to "Specifying Managed Nodes" on page 108. Size: 10 characters Default: "**default**" is the name of the default filter set.
	(Sheet 4 of 7)

Table 12. Page A of the Managed Nodes screen

Field	Description
START TYPE	Identifies the type of connection between MultiVantage Proxy Agent and a managed node. Valid options include: **static** (default) **dynamic** (see DYNAMIC TIMEOUT field) A static connection maintains a continuous link for 24 hours per day, 7 days per week. Select static connections to monitor critical managed nodes. A dynamic connection maintains a temporary link with the managed node on an as-needed basis. Select dynamic connections to monitor less critical managed nodes. A dynamic connection stays up as long as MultiVantage Proxy Agent is actively processing SNMP requests and then times-out after a specified period. The System Management Server does not poll for health data if a dynamic connection is assigned to a managed node.
	(Sheet 5 of 7)

Table 12. Page A of the Managed Nodes screen

Field	Description
START STATE	Identifies the connection state of the managed node at the time you start MultiVantage Proxy Agent. Valid options include: • **init** = initiates the connection types as defined below: — Starts the static connection to the managed node — Places the dynamic connection in an idle state to be initiated by minor or major alarms from the managed node • **off** = (default) indicates that the connections are turned off MultiVantage Proxy Agent supports only the number of active connections specified during installation. The number of active connections can be a combination of static and dynamic connections. The valid start states are: • **static init** or **static off** • **dynamic init** or **dynamic off**
DYNAMIC TIMEOUT	Identifies the number of minutes that a dynamic connection can be inactive before MultiVantage Proxy Agent drops the connection to a managed node. Valid options include: **5** (default) **15** **30** **60** **120**
	(Sheet 6 of 7)

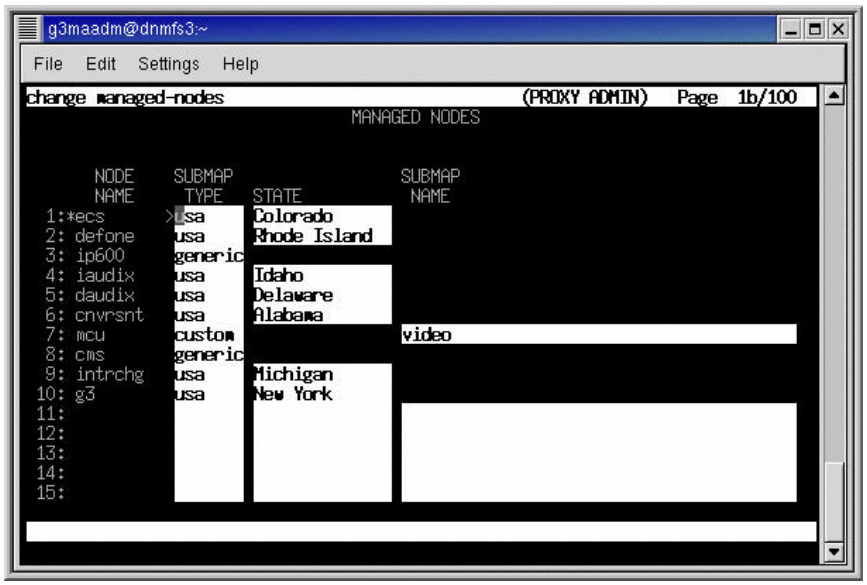
Table 12. Page A of the Managed Nodes screen

Field	Description
RESET COUNT	Allows you to reset the status counters to zero. While MultiVantage Proxy Agent is running, the counters track the number of attempts, connections, requests, responses, and errors that occur. MultiVantage Proxy Agent updates the numbers from the counters on the STATUS screen. Valid options include: **N** = no (default) -- do not reset counters **Y** = yes to reset the status counters to zero
	(Sheet 7 of 7)

Fields on Page B

The figure below shows page **B** of the MANAGED NODES *screen*. Page **B c**ontains the submap type and location of the individual managed nodes.

Figure 8. Page B of the MANAGED NODES screen



Page B field descriptions

The table below contains the field descriptions for Page **B** of the MANAGED NODES screen.

Table 13. Page B of the Managed Nodes screen

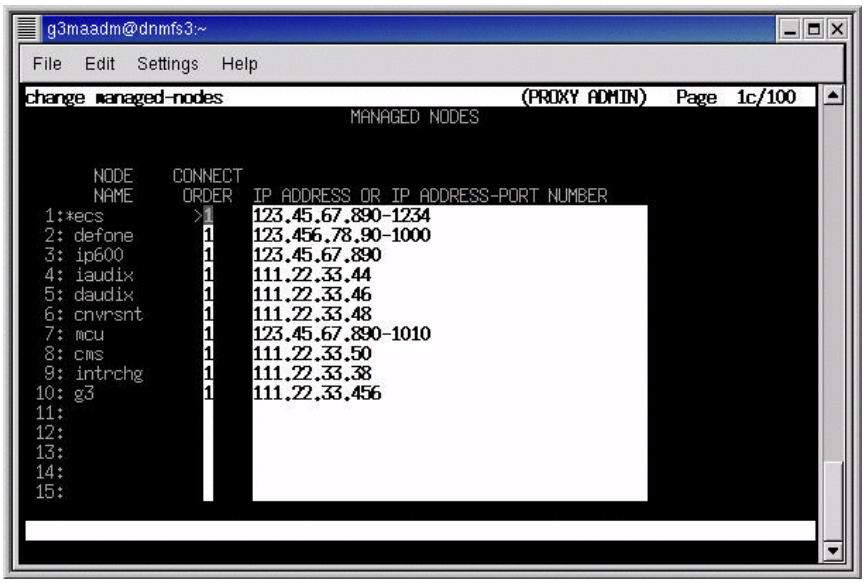
Field	Description
NODE NAME	Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages.
SUBMAP TYPE	Identifies the type of location map to display on the HP OpenView Network Management System (NMS). Valid options include: **generic** (default) **usa** (see associated STATE field) **custom** (see associated SUBMAP NAME field) Field size: 7 characters
STATE	Identifies the name of the state where a managed node is located on the USA map. The STATE field only displays if the user selects the **usa** option in the SUBMAP TYPE field. Valid options for this field include all **50** states. The default option is set on the DEFAULT LOCATION screen. You can change the *State* name for individual managed nodes Field size: 14 characters
SUBMAP NAME	Identifies the name of the custom location submap for individual managed nodes. The SUBMAP NAME field only displays if the user selects the **custom** option in the SUBMAP TYPE field. Field size: **40** characters. The system accepts any name that you type the in the SUBMAP NAME field.

Fields on Pages C and D

Pages **C** and **D** of the MANAGED NODES screen contain the same fields to administer the connections and IP address or IP address-Port numbers that MultiVantage Proxy Agent uses to connect with each managed node.

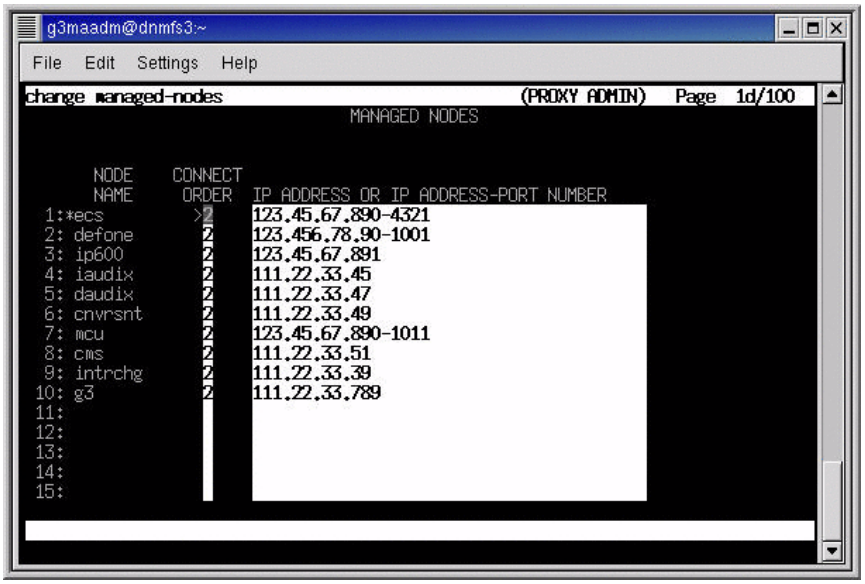
The figure below shows page **C** of the MANAGED NODES screen.

Figure 9. Page C of the MANAGED NODES screen



The figure below shows page **D** of the MANAGED NODES screen.

Figure 10. Page D of the MANAGED NODES screen



Pages C and D field descriptions

The table below contains the field description for pages **C** and **D** of the MANAGED NODES screen.

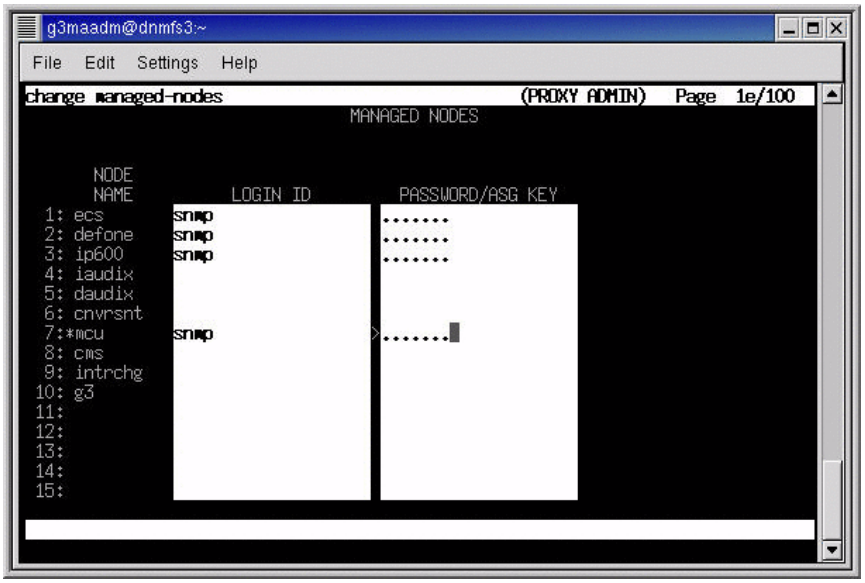
Table 14. Pages C and D of the Managed Nodes screen

Field	Description
NODE NAME	Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages.
CONNECT	Specifies which IP address or IP address-Port number MultiVantage Proxy Agent will use to connect to a managed node. MultiVantage Proxy Agent will always use the number **1** IP address or IP address-Port number first. If the number **1** IP address or IP address-Port number is busy or out-of-order, then MultiVantage Proxy Agent will use the number **2** IP address or IP address-Port number, if number **2** exists. Valid options include: **1** -- **required** field (default) **2** -- optional field Generally, users designate page **C** as the number **1** connect and page **D** as the number **2** connect. If you enter two IP addressees or IP address-Port numbers, you can change the connects between the subpages **C** and **D**. One of the IP address or IP address-Port numbers must contain the number **1** in the CONNECT column.
IP ADDRESS OR IP ADDRESS - PORT NUMBER	Specifies the IP address or IP address-Port number that MultiVantage Proxy Agent uses to connect to a managed node. The default port number for a TCP telnet connection is 23.

Fields on Page E

The figure below shows page **E** of the MANAGED NODES screen. Page **E** contains the **default** login ID for MultiVantage solutions from the DEFAULT LOGIN screen. The system does not display the password or ASG key entered on the DEFAULT LOGIN screen.

Figure 11. Page E of Managed Nodes screen



Page E field descriptions

The table below contains the field descriptions for Page E of the MANAGED NODES screen.

Table 15. Page E of the Managed Nodes screen

Field	Description
NODE NAME	Identifies the name of the managed node. The node name occupies the same line number on each of the lettered pages.
	(Sheet 1 of 2)

Table 15. Page E of the Managed Nodes screen

Field	Description
Login ID	Identifies the login name for the MultiVantage solution. The feature reduces the time to administer large numbers of new MultiVantage solutions on MultiVantage Proxy Agent. With this feature, you do not have to manually connect to the system on the COMMUNICATION MANAGER screen and save the login data. To override the default login ID from the DEFAULT LOGIN screen, you can change the login ID for individual MultiVantage solutions on page E. Field size: 20 characters Validation: None Default: Blank
Password/ASG Key	Displays periods in field as the password or ASG key is entered. MultiVantage Proxy Agent saves the default password or ASG key that users administered on the DEFAULT LOGIN screen. For security reasons, MultiVantage Proxy Agent displays periods in the field on the MANAGED NODES screen. For MultiVantage solutions that are protected by the Access Security Gateway (ASG) system, MultiVantage Proxy Agent automatically generates the response to the challenge when you administer new MultiVantage solutions on MultiVantage Proxy Agent. To override the default password or ASG Key from the DEFAULT LOGIN screen, you can change the password or ASG secret key for individual MultiVantage solutions on page E. Field size: 20 characters Validation: None Default: Blank
	(Sheet 2 of 2)

Specifying Managed Nodes

The MANAGED NODES screen provides an overview of the configuration for each managed node that users administer on MultiVantage Proxy Agent.

This section contains the procedures to:

- Add new managed nodes to MultiVantage Proxy Agent and save the login data
- Change data for individual managed nodes
- Delete existing managed nodes

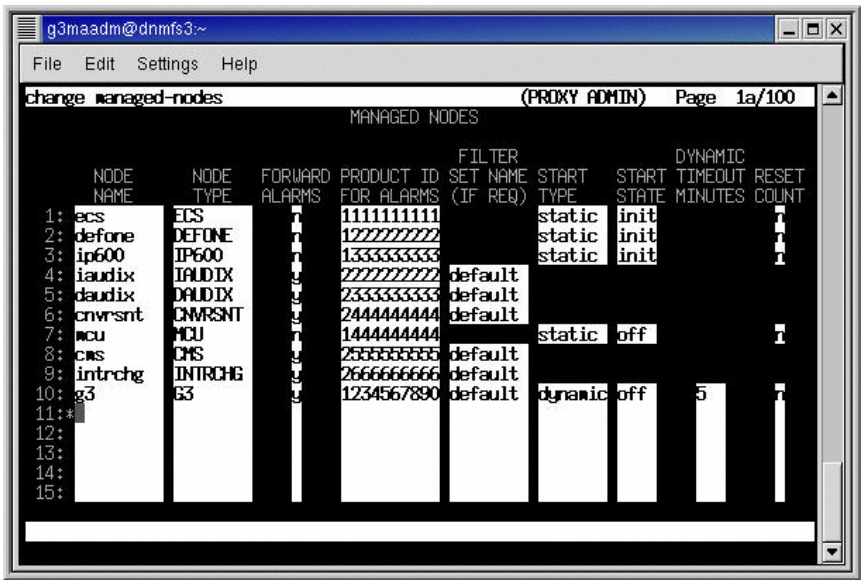
Procedure

The procedures below contain the steps to add or change managed nodes and one step to delete a managed node. The examples in the procedure below show default values in the fields. To complete the fields, refer to the Managed Nodes section of the VMS001 form.

1. Access the PROXY ADMIN menu.
2. Stop MultiVantage Proxy Agent if it is running (page 38).
3. In the command line on the PROXY ADMIN menu, type **change managed-nodes** and press **ENTER.**

   The system displays the page **A** of the MANAGED NODES screen.

Figure 12. Page A of the MANAGED NODES Screen



4. On page **A**, access the appropriate page number (1 through 100). In the NODE NAME column, execute one of the options below:

   — To ***add*** a new managed node: See **Step 5**.

   — To ***change*** a managed node: Go to the line number for that managed node. Then, go to the fields to be changed and make the appropriate changes on each subpage.

   — To ***delete*** an existing managed node: Go to the line number for that managed node. Press the **SPACE BAR**. The system deletes the managed node and clears the fields on all subpages for that line.

5. To add a new managed node, on page **A**, go to the first blank line and complete the fields below.

   a. In the NODE NAME field, type the system name.

   b. In the NODE TYPE field, select the default MultiVantage solution.

   c. In the FORWARD ALARMS field, type either

   —**n** (default for DEFINITY ECS, Avaya MultiVantage™ S8100 Media Server with Avaya™ G600 Media Gateway, and Avaya MultiVantage™ S8100 Media Server);

   —**y** (default for all other node types)

   d. In the PRODUCT ID FOR ALARMS field, type the **product/ alarm ID** for the node type.

   e. In the FILTER SET NAME, choose one of the options below:

   —To select a different filter name, press **Ctrl-Y** to display the options list; highlight a filter name; and press **ENTER**

   —To clear the field of any filter name, press the **SPACE BAR**

   f. In the START TYPE field, enter **static** (default).

   g. In the START STATE field, enter **off** (default) or **Ctrl-Y** and select **init** (initiate).

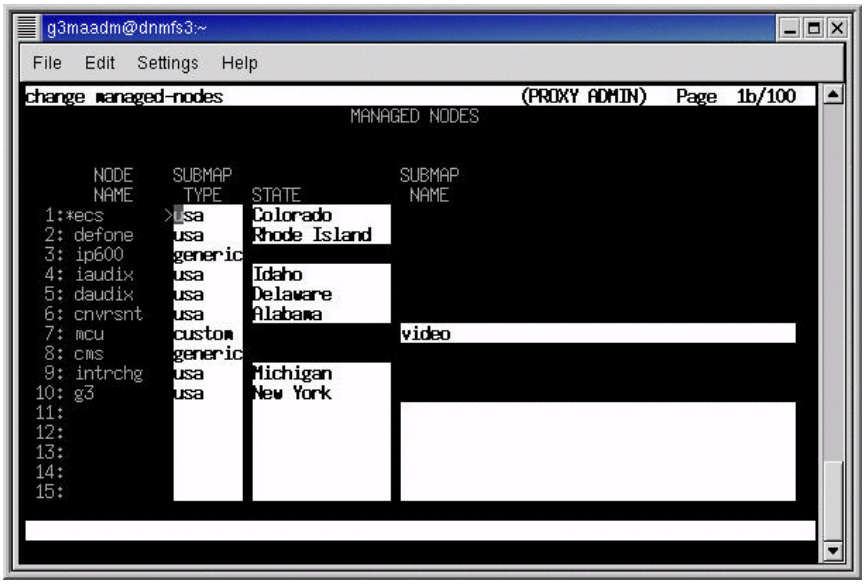
   h. In the DYNAMIC TIMEOUT MINUTES field, enter **5** (default) or press **Ctrl-Y** to select an option from the list. If you select **static**, the field is disabled.

   i. In the RESET COUNT field, enter **n** (default) or type **y** to reset, if necessary

6. Press **ENTER** to display page **B**.

   The system displays page **B** of the Managed Nodes screen.

Figure 13. Page B of the MANAGED NODES Screen



7. On page **B** change the location for each managed node, where appropriate.

   Generic location

   SUBMAP TYPE: **generic** (default)

   USA location

   SUBMAP TYPE: **usa**

   STATE: **Alabama** (default) Press **Ctrl-Y** to select a state from the list

   Custom location

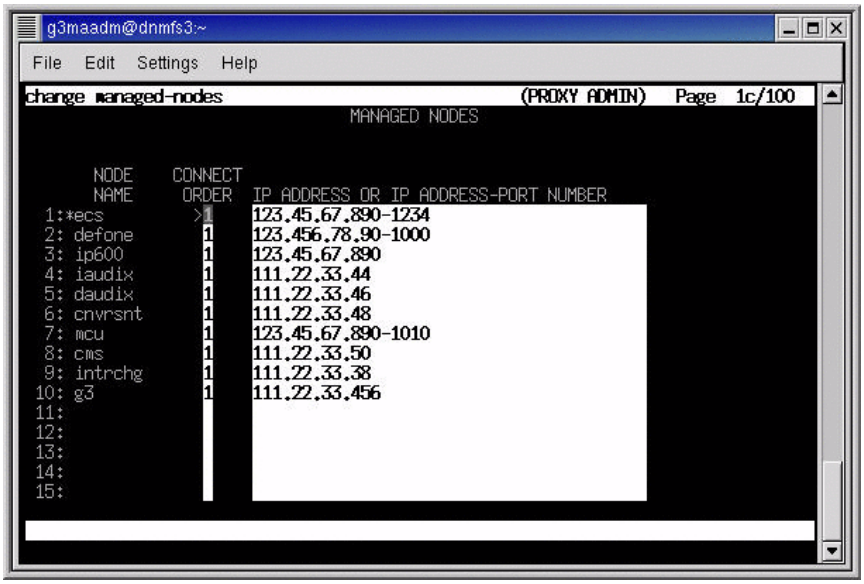
   SUBMAP TYPE: **custom**

   SUBMAP NAME: Type the **location name**

   Press **ENTER** to display page **C**.

   The system displays page **C** as shown in the example below.

Figure 14. Page C of the MANAGED NODES Screen



8. On page **C**, complete the fields for the primary communication device.

MultiVantage Proxy Agent uses this device to connect to the managed node.

`NODE NAME`: (carried over to each page)

`CONNECT`: **1**

9. Enter 1 (default) for the IP address or IP address-Port number used by SNMP or enter 2 to identify a different communication application.

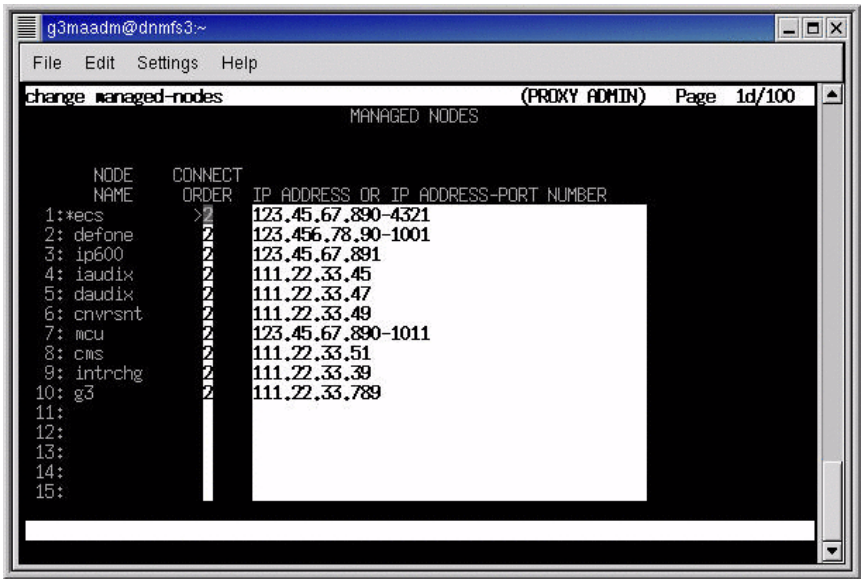
The IP addresses or IP address-Port numbers (devices) for Connect entries 1 and 2 must be different.

`IP ADDRESS OR IP ADDRESS- PORT NUMBER`: Type the **IP address or IP address-Port number** for the primary device. Go to the VMS001 form and refer to the IP address or IP address-Port number 1 field on the *Managed Nodes* section.

10. Press **ENTER** to display page **D**.

The system displays page D as shown in the example below.

Figure 15. Page D of the MANAGED NODES Screen



11. OPTIONAL. On page **D**, complete the fields for a secondary communication device.

MultiVantage Proxy Agent uses this device if the first device is not available.

NODE NAME: (carried over to each page)

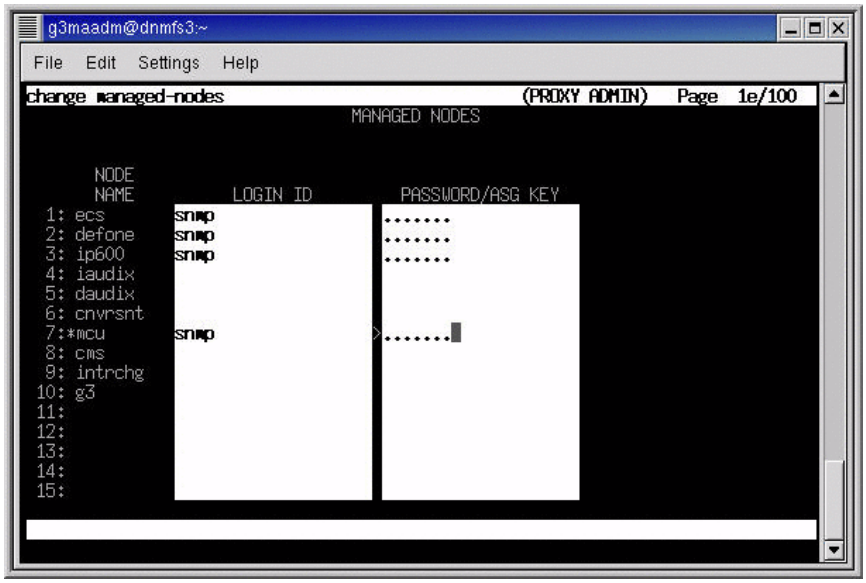
CONNECT: Type **2** in the field

IP ADDRESS OR IP ADDRESS- PORT NUMBER: Type the **IP address or IP address-Port number** for the secondary device. Go to the VMS001 form, and refer to the Optional. IP address or IP address-Port number 2 field on the *Managed Nodes* section.

12. Press **Ctrl-N** to display page **E**.

The system displays page E as shown in the example below.

Figure 16. Page E of the MANAGED NODES Screen



13. The fields on page **E** contain the default login data from the DEFAULT LOGIN screen for new MultiVantage solutions, as show in the example below.

NODE NAME: (carried over to each page)

LOGIN ID: **system name** for the new MultiVantage solution

PASSWORD/ASG KEY: **[**.....**]** periods are displayed as the password or ASG secret key is entered.

14. Press **Ctrl-E** to submit the data.

The system saves the data and displays the PROXY ADMIN menu.

15. From the PROXY ADMIN menu, start MultiVantage Proxy Agent (page 38).

16. Display the STATUS screen, verify that MultiVantage Proxy Agent is active, and close the screen (page 43).

11 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 MultiVantage Proxy Agent that are currently installed.

Field descriptions

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

Table 16. 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.
	(Sheet 1 of 2)

Table 16. DISPLAY SOFTWARE VERSION screen

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 MultiVantage 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.
	(Sheet 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 17. 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 MultiVantage Proxy Agent screens will be in color.

1. Access the MultiVantage 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 MultiVantage 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 MultiVantage Proxy Agent MAIN MENU.

12 Maintenance and Troubleshooting

This chapter contains utilities and logs to allow the system administrator to maintain MultiVantage 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).

MultiVantage 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 MultiVantage Proxy Agent after MultiVantage Proxy Agent has been installed
- Changing settings for SNMP access after MultiVantage 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)

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

*** Note:** To view the status of MultiVantage 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)

*** 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 MultiVantage Proxy Agent to managed nodes to troubleshoot connection problems. The procedures contain the login prompts to access managed nodes and MultiVantage solutions that are protected by the Access Security Gateway (ASG) software.

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

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

Connection procedures

This chapter contains two types of connection procedures to manually log in to the managed nodes.

- "Connecting to Managed Nodes" on page 123.
- "Connecting to MultiVantage Solutions with ASG" on page 125.

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

Saving login data

You should administer the DEFAULT LOGIN screen to save the login data for new MultiVantage solutions. Refer to the procedure to "Specifying the Default Login" on page 57.

When you administer new MultiVantage solutions, MultiVantage Proxy Agent displays the default login data on page E of the MANAGED NODES screen. You do not have to complete the procedures on the COMMUNICATION MANAGER screen to save new login data.

At the COMMUNICATION MANAGER screen, generally you should not save the login data unless the system prompts you to enter a new password. The prompt to resave login data displays if the “password aging” feature is enabled on the managed node. The system permanently stores the login data until you change and save login data at a later time.

Understanding the Communication Manager Screen

Field descriptions

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

Table 18. Communication Manager screen

Connection 1	Contains the first managed node that is currently connected to MultiVantage Proxy Agent. The field is **blank** if a managed node is NOT currently connected. Valid options include: • List of all **managed nodes** administered on MultiVantage 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.
	(Sheet 1 of 2)

Table 18. Communication Manager screen

Connection 2	Contains the second managed node that is currently connected to MultiVantage 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 MultiVantage 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 MultiVantage 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.
	(Sheet 2 of 2)

Connecting to Managed Nodes

This section contains the procedure to manually login to one or two managed nodes to troubleshoot connections between MultiVantage 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 MultiVantage 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 steps 5 through 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 MultiVantage 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 128.

Connecting to MultiVantage Solutions with ASG

This section contains the procedure to manually connect to MultiVantage solutions that are protected by Access Security Gateway (ASG) and to troubleshoot connections between MultiVantage 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 MultiVantage solution.

Required materials

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

— Login name for the MultiVantage solution

— ASG secret key to access the MultiVantage solution

— Challenge from the MultiVantage solution

— Hand-held ASG device to generate a response to the challenge from the MultiVantage solution

ASG Procedure

Complete the following procedure to manually login to ASG-protected MultiVantage solutions.

1. Access the MultiVantage 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 **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 MultiVantage 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 128.

Disconnecting from Managed Nodes

Complete the procedure below to manually disconnect the managed nodes.

1. Access the MultiVantage 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 MultiVantage Proxy Agent MAIN MENU.

Adding New Communication Devices

The root user can add new communication devices to MultiVantage 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 MultiVantage Proxy Agent" on page 29.
- "Uninstalling MultiVantage Proxy Agent" on page 35.

Changing Settings for SNMP Access

See"Configuring MultiVantage Proxy Agent" on page 29.

Viewing Alarm and Error Logs

MultiVantage 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 19. Alarm and error logs

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

Using Alarm Testing Tools

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

- Simulate the alarm reception on MultiVantage 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)

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

Trap Test scripts

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

Table 20. Trap Test Scripts

Command	Function
TrapTest	MultiVantage solution and MCU traps
CMSTrapTest	Call Management System (CMS) traps
ADXTrapTest	MultiVantage solution AUDIX traps
IADTrapTest	Intuity AUDIX traps
INTTrapTest	Intuity Interchange traps
CVSTrapTest	CONVERSANT traps

Procedure

The procedure below uses the MultiVantage solution 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, MultiVantage 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 **/usr/local/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 MultiVantage™ 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 MultiVantage solution. 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 MultiVantage™ 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.

13 Help Screens and Commands

MultiVantage 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 MultiVantage Proxy Agent menu or application screen.
- The help command (**Ctrl-Y**) displays a **help** window for the current MultiVantage 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 MultiVantage 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 MultiVantage Proxy Agent.

Table 21. 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.
	(Sheet 1 of 2)

Table 21. Commands and Hotkeys

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.
	(Sheet 2 of 2)

Glossary and Abbreviations

A

ATAC
See “Avaya Technology and Consulting (ATAC)” on page 11.

C

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

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.

MultiVantage software
The call processing software that runs on MultiVantage Solutions. Formerly known as DEFINITY software.

MultiVantage Solution
Any of the products that run MultiVantage software. Formerly known as DEFINITY system, DEFINITY ECS, switch, PBX, or voice system.

N

Network Management Server
This is the Windows box that you can install Windows-based VisAbility 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.

R

RNIS
See “Avaya Remote Network Implementation Services (RNIS)” on page 11.

S

supported systems
In this document, a “supported system” is any of the voice systems or adjuncts that MultiVantage Proxy Agent works with.
See “Supported Systems” on page 23.

SNMP
Simple Network Management Protocol.

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

T

TSO
See “Avaya Technical Service Organization (TSO)” on page 12.

Index