



Avaya Solution & Interoperability Test Lab

Application Notes for Micromuse Netcool/OMNIbus Event Management System with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to activate SNMP alarm notification on the Avaya Communication Manager and SNMP trap collection on the Micromuse Netcool/OMNIbus Event Management System. Micromuse Netcool/OMNIbus was compliance tested with an Avaya S8300 Media Server with a G700 Media Gateway and an Avaya S8700 Media Server with a G600 Media Gateway. The Avaya Media Servers and Gateways were configured to send event information to Netcool/OMNIbus using v1, v2c, and v3 SNMP traps. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to activate SNMP alarm notification on the Avaya Media Servers and Gateways and SNMP trap collection on the Micromuse Netcool/OMNIBus Event Management System. Upon detection of a failure, the Avaya Media Servers and Gateways can raise an alarm and send an SNMP trap over the IP network to the designated SNMP trap receiver(s). As a non-intrusive SNMP trap receiver, Netcool/OMNIBus can collect, store, and manage alarm information received from Avaya Communication Manager. Communication Manager running on the Avaya Media Server reports alarms via SNMP traps according to the configured alarm reporting options.

The configuration in **Figure 1** illustrates an enterprise network comprised of an Avaya S8300 Media Server with a G700 Media Gateway and an Avaya S8700 Media Server with a G600 Media Gateway that connect to the Layer 3 IP network over Avaya P333T-PWR Layer 2 switches. The Avaya Media Servers and Gateways send event and alarm information to the Micromuse Netcool/OMNIBus Event Management System on UDP port 162 using v1, v2c, or v3 SNMP traps. The Avaya S8300 and S8700 Media Servers and the G700 Media Gateway, including its P330 Switching Processor and Media Gateway Processor (MGP) components, have an internal SNMP agent that send SNMP traps directly to the Netcool/OMNIBus server. The S8700 Media Server sends all event and alarm information related to the Avaya G600 Media Gateway. In this configuration, all of the Netcool/OMNIBus software components used in the compliance test were installed in the same server using a Microsoft Windows 2000 Professional PC platform.

The Micromuse Netcool/OMNIBus components covered in the compliance test included the **MTTrapD Probe**, **ObjectServer**, and **Desktop Tools**. The **Flex License Manager** was also used to determine the licensed applications running on the Netcool/OMNIBus system. The Netcool Probe collects SNMP traps received on UDP port 162 and forwards them to the Netcool ObjectServer, which is a database server where all events are stored and managed. The ObjectServer is capable of consolidating repeated events collected by the Probe (also referred to as de-duplication) and correlating related events, such as link down/up events. The ObjectServer converts the traps to human-readable "events" to be viewed and acknowledged with the Desktop application. The Desktop is a graphical tool that is used to view and manage events and can provide a filtered view of color-coded alerts displayed in the Event List. By default, the Desktop application polls the ObjectServer for event information every 60 seconds, or upon demand.

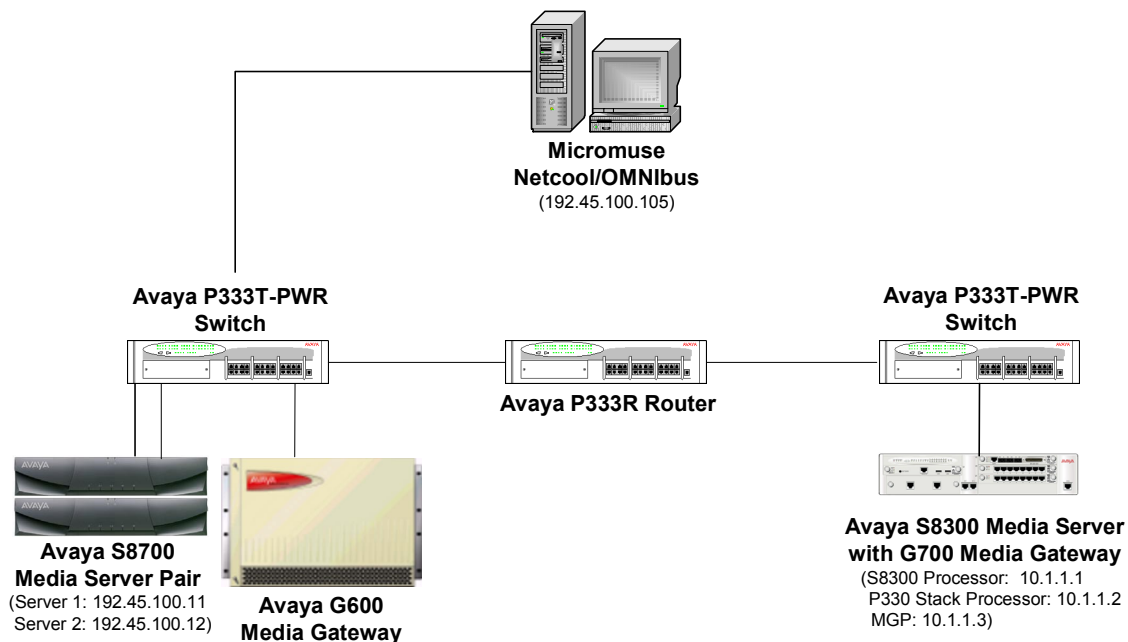


Figure 1: Avaya Media Servers and Gateways and Micromuse Netcool/OMNibus Network Configuration

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Media Server with Avaya G700 Media Gateway	Communication Manager 2.0 (R012x.00.0.219.0)
Avaya S8700 Media Server with Avaya G600 Media Gateway	Communication Manager 2.0 (R012x.00.0.219.0)
Micromuse Netcool/OMNibus for Windows 2000 Professional, including: <ul style="list-style-type: none"> ▪ MTTrapD Probe ▪ ObjectServer ▪ Desktop Tools ▪ Flex License Manager 	Version 3.6
Micromuse MIB2rules Utility	Version 4.0.6

3. Avaya Media Server SNMP Configuration

This section describes the procedure for configuring the Avaya S8300 and S8700 Media Servers to report alarms to an SNMP trap destination. The required steps are:

- Activating SNMP alarm notification on the Avaya S8300 and S8700 Media Servers,
- Allowing SNMP traps to be output from the Avaya Media Server on UDP port 162, and
- Checking that Avaya alarms that should generate SNMP traps are being reported according to the alarm reporting options. The alarm reporting options are specified in the **set options** form accessible through the System Access Terminal (SAT). See reference [2], *Maintenance Command Reference*, for a description of the **set options** form.

Note: Warning alarms raised by the Avaya Communication Manager are not reported via SNMP traps. However, warning and informational level traps could be generated directly by the G700 Media Gateway for events and alarms related to the P330 stack processor and MGP.

3.1. Configuring SNMP Trap Destinations

The SNMP trap destinations for the Avaya S8300 and S8700 Media Servers are configured through the server's web interface. To access the web interface, launch a web browser and connect to the media server by specifying its IP address in the URL (e.g., type <http://192.45.100.11> or <http://192.45.100.12> in the URL for the Avaya S8700 Media Servers). For an S8700 Media Server pair, the SNMP trap destinations need to be configured on each media server. Supply the login and password for an account with super-user privileges. After logging in, a main menu is presented along the left hand side of the screen. In the **Alarms** section, click on **SNMP Traps** to display the **Change Trap Destination** screen shown in **Figure 2**.

In the **Change Trap Destination** screen, enter the IP address of the Micromuse Netcool/OMNIbus server (i.e., 192.45.100.105) and enable this SNMP trap destination. Select **SNMP version 1** and set the community name to *public*, as shown in **Figure 2**. For SNMP v2c or v3, set the **Notification Type** field to *Trap* and set the **Community Name** or **User Name** field to a valid string. Click on the **Change** button to submit the form.

The **SNMP Traps** configuration allows the Avaya Media Server to send traps for alarms raised by Communication Manager and alarms related to the media server's operating system and support software. Certain alarms related to the Stack Processor and the Media Gateway Processor (MGP) in the G700 Media Gateway are not detected or raised by the Avaya Media Server. Therefore, the SNMP agents in those components of the G700 Media Gateway are responsible for sending those traps directly to the configured SNMP trap destination(s). See reference [1] for the SNMP traps generated by G700 Media Gateway. Avaya Communication Manager running on the S8700 Media Server detects internal failures in the G600 Media Gateway and sends all traps when it controls a G600 Media Gateway.

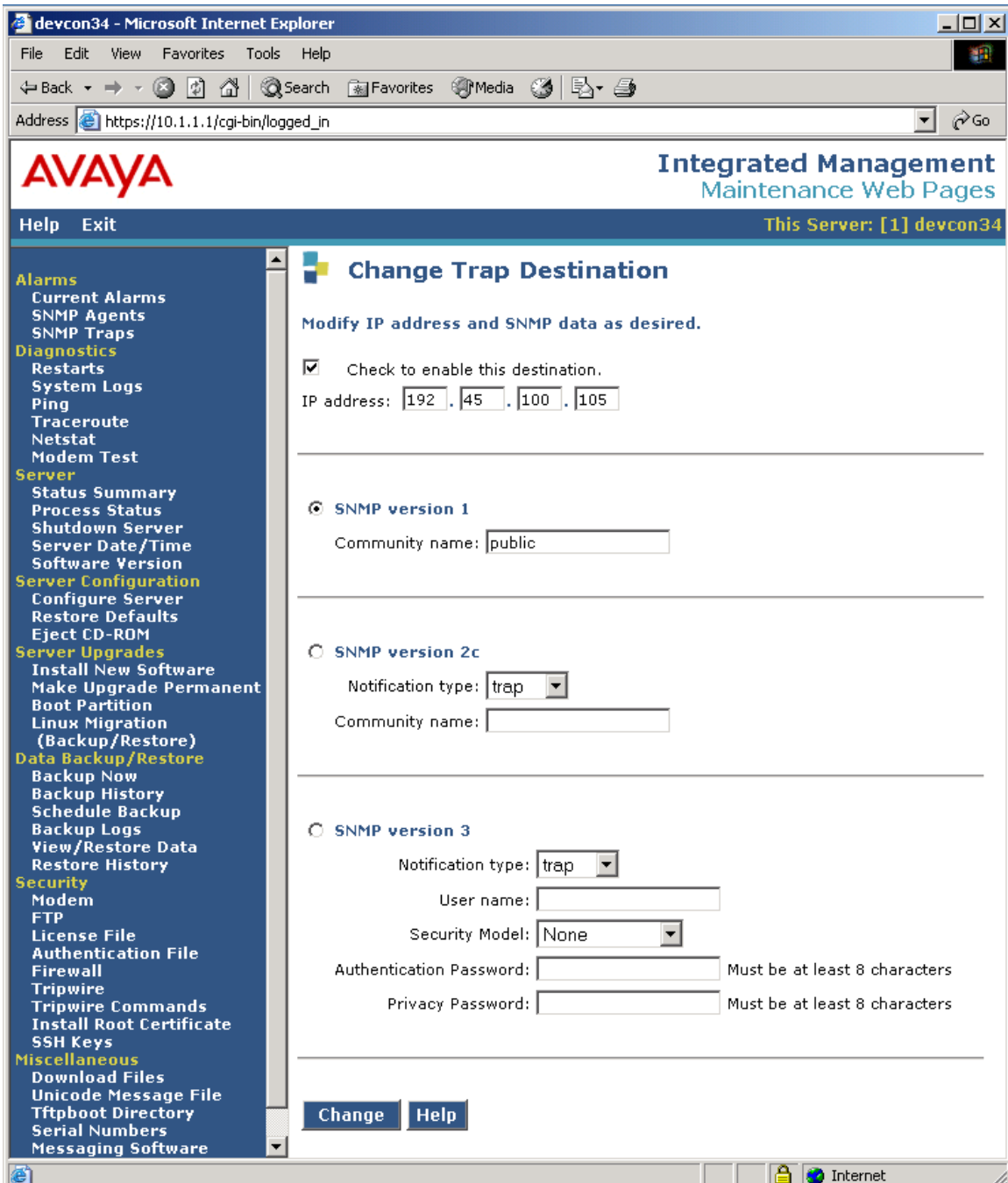


Figure 2: SNMP Traps Configuration

3.2. Firewall Configuration

The firewall in the Avaya Media Server must allow SNMP traps to be sent on UDP port 162. Click on the **Firewall** option in the **Security** section of the menu to display the **Firewall Configuration** screen. At the bottom of the screen, click on the **Advanced Settings...** button to display the screen shown in **Figure 3**. Click on the **Output from Server** checkbox (2nd column) for **snmptrap 162/udp** and submit the form. This is the only port that needs to be enabled for the media server to send SNMP traps. For an S8700 Media Server pair, the **Firewall** configuration should be performed on each media server.

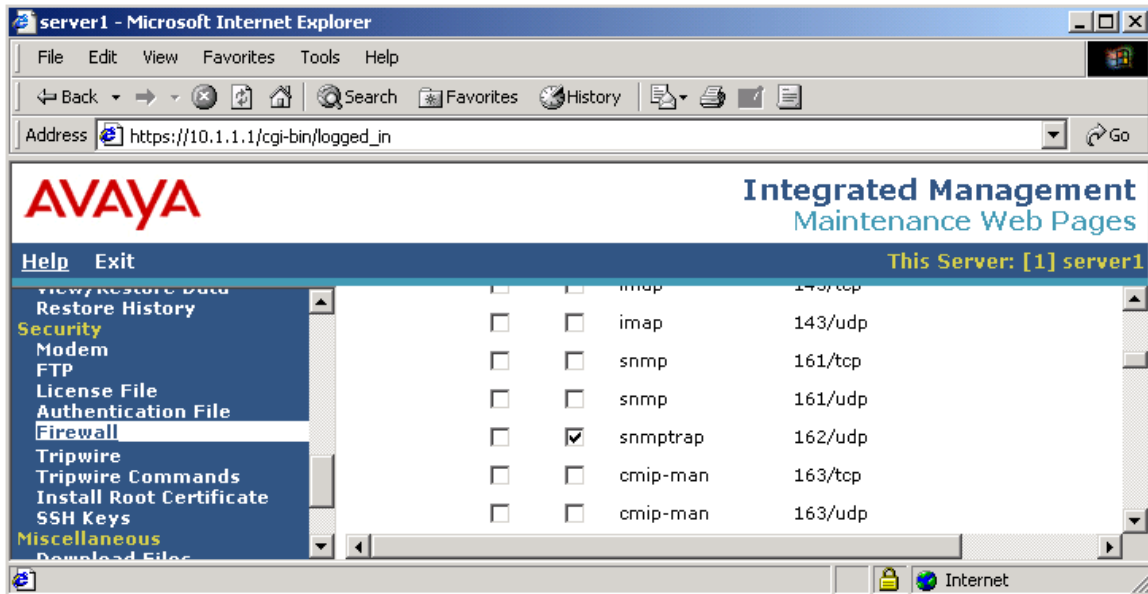


Figure 3: Firewall Configuration (Advanced Settings...)

3.3. Configuring Alarm Reporting Options

Ensure that the alarms the customer would like to have reported to Netcool/OMNIBus have not been downgraded to a warning alarm; otherwise, these alarms will not be reported via an SNMP trap. Enter the **set options** command on the media server's SAT to display the form in **Figure 4**, and check the **Major** and **Minor** columns for each alarm type. In summary, if the **Major** or **Minor** column is set to **[w]arning**, **[r]eporting**, or **[n]o**, then that alarm type has either been downgraded to warning severity or alarm reporting has been suppressed. However, if the column is set to **[y]es** or **[m]inor**, then an SNMP trap is sent. See reference [2] for more details on the **set options** form.

Note: The settings in the set options form do not affect the SNMP traps generated by the G700 Media Gateway, which always sends warning and informational level traps, if an SNMP trap destination is configured.

set options	ALARM REPORTING OPTIONS		Page 1 of 22
		Major	Minor
	On-board Station Alarms:	y	y
	Off-board Station Alarms:	y	y
	On-board Trunk Alarms (Alarm Group 1):	y	y
	Off-board Trunk Alarms (Alarm Group 1):	y	y
	On-board Trunk Alarms (Alarm Group 2):	w	w
	Off-board Trunk Alarms (Alarm Group 2):	w	w
	On-board Trunk Alarms (Alarm Group 3):	w	w
	Off-board Trunk Alarms (Alarm Group 3):	w	w
	On-board Trunk Alarms (Alarm Group 4):	w	w
	Off-board Trunk Alarms (Alarm Group 4):	w	w
	On-board Adjunct Link Alarms:	y	y
	Off-board Adjunct Link Alarms:	y	y
	Off-board MASI Link Alarms:		y
	Off-board DS1 Alarms:	y	y
	Off-board TCP/IP Link Alarms:	y	y
	Off-board Alarms (Other):	y	y
	Off-board ATM Network Alarms:		y

Figure 4: Set Options Form (Page 1)

Page 2 of the set options form continues with the alarm reporting options for other alarm types, such as Signaling Group alarms.

set options	ALARM REPORTING OPTIONS		Page 2 of 22
		Major	Minor
	Off-board Firmware Download Alarms:		y
	Off-board Signaling Group Alarms:		y
	Remote Max Alarms:		y

Figure 5: Set Options Form (Page 2)

4. Avaya G700 Media Gateway SNMP Configuration

This section describes the procedure for configuring SNMP trap destinations on the G700 Media Gateway, including the P330 Stack Processor and the Media Gateway Processor (MGP).

Log in to the P330 Stack Processor of the G700 Media Gateway and enter the appropriate login and password credentials. In the configuration described herein, the IP address is 10.1.1.2. First, add the SNMP trap receiver and then enable SNMP traps to that address, as shown in **Figure 6**. This configuration allows the P330 Stack Processor to send events and alarms directly to the SNMP trap receivers. By default, all traps are enabled.

```
                Welcome to P330
                SW version 4.0.17
Login: root
Password:
Password accepted.

P330-1(super)# set snmp trap 192.45.100.105
SNMP trap receiver added.
P330-1(super)# set snmp trap 192.45.100.105 enable
SNMP traps are enabled for this address.
```

Figure 6: Configuring SNMP Trap Destinations on the P330 of the G700 Media Gateway

Enter the **show snmp** command to view the SNMP trap destinations and their status, the community names, and the traps that have been enabled for the associated trap destination.

```
P330-1(super)# show snmp

Authentication trap disabled

Community-Access      Community-String
-----
read-only             public
read-write           public
trap                  public

Trap-Rec-Address      Status      Traps Configured
-----
192.45.100.105      Enabled
                    config
                    fault
                    trafic_threshold
                    module_De-Enrollment
                    module_Enrollment
                    delete_SW_redundancy_entry
                    create_SW_redundancy_entry
                    temperature_warning
                    general_threshold
                    cam_change
                    duplicate_ip
                    ip_vlan_violation
                    link_aggregation_connection_fault
                    link_aggregation_connection_return
                    link_aggregation_partial_fault
                    link_aggregation_partial_return
                    delete_lag
                    create_new_lag
                    active_policy_list_change
                    policy_access_control_violation
                    BUPS_module_fault
                    BUPS_module_fault_return
                    BUPS_fans_module_fault
                    BUPS_fans_module_fault_return
                    fans_module_fault
                    fans_module_fault_return
                    cascade_up_connection_fault
                    Cascade_up_connection_fault_return
```

Figure 7: SNMP Status on the P330 Stack Processor of the G700 Media Gateway

Open a session to the Media Gateway Processor (MGP) using the **session mgp** command. Enter configuration mode and configure the SNMP trap destination using the **set snmp trap** command, as shown in **Figure 8**. This configuration allows the MGP to send events and alarms directly to the SNMP trap receivers. By default, all traps have been enabled.

```
P330-1(super)# session mgp

                               Welcome to Media Gateway Processor
                               FW version 21.20.1

MG-001-1(super)# configure
MG-001-1(configure)# set snmp trap 192.45.100.105 enable
```

Figure 8: Configuring SNMP Trap Destinations on the MGP of the G700 Media Gateway

Enter the **show snmp** command in the MGP CLI to view the SNMP trap receivers and their status, the community names, and the traps that have been enabled for the associated trap destination. The MGP in the G700 Media Gateway has the responsibility to report errors associated with the VoIP resources in the G700 Media Gateway.

```
MG-001-1(configure)# show snmp

COMMUNITY ACCESS      COMMUNITY STRING
-----
read-only             public
read-write           public
trap                  public

TRAP RECEIVER        RECEIVER STATUS    TRAP ENABLED
-----
192.45.100.105      Enabled           P,T,M,C,V,O,A

TRAP CODE/NAMES REFERENCE
-----
P=Power    T=Temp    A=Application
M=Module   C=Config  O=Operations
V=Voice
```

Figure 9: SNMP Status on the MGP of the G700 Media Gateway

5. Micromuse Netcool/OMNIBus Configuration

This section describes the procedure for configuring the Micromuse Netcool/OMNIBus Event Management System to capture SNMP traps. The steps required are:

- Install the Flex license key file,
- Import/load the Avaya MIB files into Netcool/OMNIBus,
- Configure the Netcool Probe to receive SNMP traps on UDP port 162,
- Configure the Netcool ObjectServer,
- Start the Netcool/OMNIBus applications in Windows Services, and
- Start the Netcool Desktop application to view alerts in the ObjectServer.

It is assumed that the Micromuse Netcool/OMNIBus software and the Flex License Manager have already been installed on a Microsoft Windows PC. During the installation, the user was prompted for the License Server Name and the ObjectServer configuration, including the name of the ObjectServer, the hostname or IP address of the system on which the ObjectServer is running, and the UDP port that the ObjectServer uses to communicate with the other Netcool/OMNIBus applications, such as the probe and desktop clients. These parameters can be changed or verified after the installation as shown in the steps below. For more details on the Netcool/OMNIBus installation process, see reference [3].

5.1. Install Flex License Key File

Obtain the Flex license keys from Micromuse Support and copy it to the `license.lic` file in the `C:\Program Files\Netcool\common\license\etc` directory. Verify that there is only one file with the `.lic` extension in this directory. Edit the file and verify the information on the **SERVER** line in the file. This line should specify the hostname (or IP address) and MAC address of the server where the Flex License Manager is running. The Flex License Manager communicates with other Netcool/OMNIBus applications on TCP port 27000. The format of the **SERVER** line is:

```
SERVER <Hostname/IP Address> <MAC Address> 27000
```

Figure 10 displays the content of a sample license file. Restart the Flex License Manager after copying the license file to the aforementioned directory. The license manager log file, `license.log`, is located in the `C:\Program Files\Netcool\common\license\log` directory and can aid in troubleshooting problems where the Netcool applications fail to start.

Note: The license keys are generated for the MAC address of the NIC on the Netcool/OMNIBus server.

```

SERVER 192.45.100.105 000cf1aa51ce 27000
VENDOR netcool
USE_SERVER
FEATURE nco_event_nt netcool 20030430 11-apr-2004 10 ck=209 \
SIGN=3B282736318A
FEATURE nco_ove_nt netcool 20030430 11-apr-2004 10 ck=187 \
SIGN=FF63BF9C160E
FEATURE nco_users_nt netcool 20030430 11-apr-2004 10 ck=25 \
SIGN=CF68BF4E400C
FEATURE nco_nco_nt netcool 20030430 11-apr-2004 10 ck=194 \
SIGN=A607F092429C
FEATURE nco_p_mttrapd netcool 20030430 11-apr-2004 10 ck=147 \
SIGN=8B52B50A887C
FEATURE nco_objserv netcool 20030430 11-apr-2004 10 ck=161 \
SIGN=2B56AF767778
FEATURE nco_ov_nt netcool 20030430 11-apr-2004 10 ck=170 \
SIGN=D0B9EB709AD6

```

Figure 10: Flex License File Example

5.2. Import the Avaya SNMP MIBs

The traps that the Avaya Media Servers and Gateways are capable of sending are defined in the Avaya SNMP MIBs. These MIBs must be loaded/imported into Netcool/OMNIbus so that it can understand the traps that it receives. The SNMP MIB files required for the Avaya S8300 and S8700 Media Servers and the Avaya G700 Media Gateway are listed in **Appendix A**.

The Mib2Rules (M2R) utility tool from Micromuse is a GUI based tool for reading (importing) SNMP MIBs and storing them. The M2R utility generates the `avaya.m2r.include.rules` and `m2r.varbind.lookup` files. The rules file defines how the probe should process Avaya event data to create meaningful OMNIbus alerts and the lookup file assigns values to variables used in the rules file. See **Appendix B** for a high-level description on how to use the M2R utility to import the Avaya SNMP MIBs. More detailed information about generating the rules file can be found in reference [6].

Important Note: The customer should contact Micromuse Support to obtain a copy of the Mib2Rules (M2R) utility tool and for assistance with the custom development of trap rules. The rules file impacts the behavior of Netcool/OMNIbus in terms of how event data is presented and processed. Therefore, careful consideration should be given to the settings of the trap attributes.

After creating the `avaya.m2r.include.rules` and the `m2r.varbind.lookup` files, follow these steps:

- Copy the `avaya.m2r.include.rules` and `m2r.varbind.lookup` files to the `C:\Program Files\Netcool\OMNIbus\probes\nt351\include-snmplib` directory.
- Add the “`table VarbindValtable=...`” line near the top of the `mttrapd.rules` file, as shown in **Figure 11**.
- Include the path to the `avaya.m2r.include.rules` file, which is located in the `C:\Program Files\Netcool\OMNIbus\probes\nt351` directory, in the `mttrapd.rules` file, as shown in **Figure 11**.

- Verify that the **RulesFile** parameter in the Probe's property file, `mttrapd.props`, is set correctly to the location of the `mttrapd.rules` file, as described in Section 5.3.

```
#####
# Enter lookup table Includes below with the following syntax:
#
# include "$OMNIHOME/probes/<arch>/include-snmp/<lookuptable>.include.snmp
# .lookup"
#####

table VarbindValTable="c:\Program Files\Netcool\OMNIbus\probes\nt351\include-
snmp\m2r.varbind.lookup"

                                ...

#####
# End of SNMPv2 to SNMPv1 conversion
#####
if (match($generic-trap, "6")) ### (Enterprise Specific Trap)
{
    switch($enterprise)
    {
        case "dummy case statement": ### This will prevent syntax errors in case no
includes are added below.

        #####
        # Enter rules file Includes below with the following syntax:
        #
        # include "$OMNIHOME/probes/<arch>/include-snmp/
        # <rulesfile>.include.rules"
        #####

        include "c:\Program Files\Netcool\OMNIbus\probes\nt351\include-snmp\
        avaya.m2r.include.rules"
```

Figure 11: Snippet of the Probe Rules File (mttrapd.rules)

5.3. Configure the Netcool MTTTrapD Probe

The Probe properties file defines the environment in which the probe runs. For example, it includes the location of the rules file, the UDP port that it receives SNMP traps on, and the ObjectServer name, amongst other parameters. The `mttrapd.props` property file contains all of the probe's default parameter settings (lines commented out) and is located in the `C:\Program Files\Netcool\OMNIbus\probes\nt351\include-snmp` directory. To override a value, add a line at the end of the file with the parameter name, followed by a colon, and then the parameter value. See **Figure 12** for an example of the **RulesFile** parameter being overridden.

Verify that all of the default settings are being used, including UDP port 162, the ObjectServer name "NCOMS", and the default path to the rules file. The default probe rules file is called `mttrapd.rules` and it is located in the `C:\Program Files\Netcool\OMNIbus\probes\nt351\include-snmp` directory. **No changes are required to the properties file unless the user deviates from the default values.**

```
#####
#
# Add your settings here
#
#####
RulesFile: 'C:\\Program Files\\Netcool\\OMNIBus\\probes\\nt351\\mttrapd.rules'
```

Figure 12: Snippet of Probe Property File (mttrapd.props)

5.4. Configure the Netcool ObjectServer

The ObjectServer configuration specifies the host name (or IP address) and port number that the Probe and the Desktop clients should use to establish a connection to the ObjectServer. Two entries, indexed by the ObjectServer’s name (e.g., NCOMS), were created during the installation and should be checked for appropriate values. The ObjectServer’s configuration details can be updated through the **Server Editor**. There should be two entries in the Server Editor for the ObjectServer, a client entry and a listener entry. The client entry, highlighted in **Figure 13**, specifies the host name (or IP address) and port number that the MTTrapD Probe and Desktop clients should use to connect to the ObjectServer. The Listener entry, highlighted in **Figure 14**, is used by the ObjectServer to respond to client requests. For the client and listener entries, the IP address of the server machine, 192.45.100.105, and TCP port number 4100 were specified. To access the Server Editor, select Start→Programs→Netcool OMNIBus→System Utilities→Servers Editor.

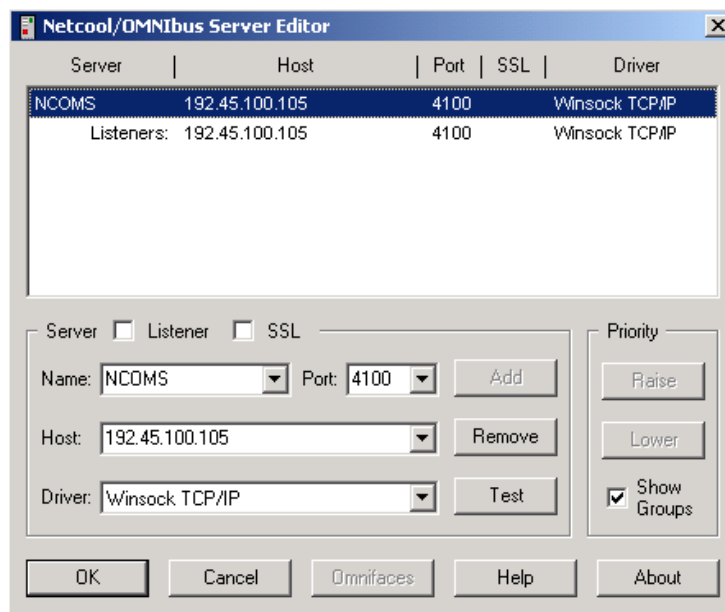


Figure 13: Server Editor (Client Entry)

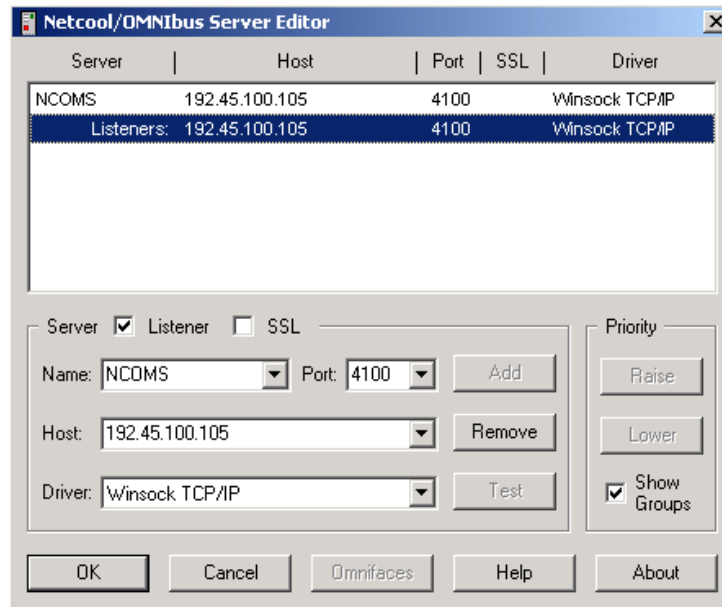


Figure 14: Server Editor (Listener Entry)

5.5. Start the Netcool/OMNIBus Applications

After the installation of the Netcool/OMNIBus software, the following three Components are added to the Windows Services.

- NCO MTTrapD Probe
- NCO Object Server
- Netcool Flex License Manager

These software components need to be running, as indicated by the **started** state in **Figure 15**, to capture and view SNMP traps. Each application can be started manually or can be configured to start automatically upon system startup by changing the **Startup Type** from *Manual* to *Automatic*. To start the applications manually, they must be started in the following order: Flex License Manager, Object Server, and then MTTrapD Probe. **Figure 15** shows that the three Netcool/OMNIBus components have been started manually. If any of the Netcool/OMNIBus applications fail to start, check the license key file. If the MTTrapsD Probe does not start successfully, check the `avaya.m2r.include.rules` rules file and the `m2r.varbind.lookup` file in the `C:\Program Files\Netcool\OMNIBus\probes\nt351\include-snmp` directory for syntax errors. See Appendix B for more information on checking the rules and lookup files for syntax errors. The application log files are located in the `C:\Program Files\Netcool\OMNIBus\log` directory and may assist in troubleshooting.

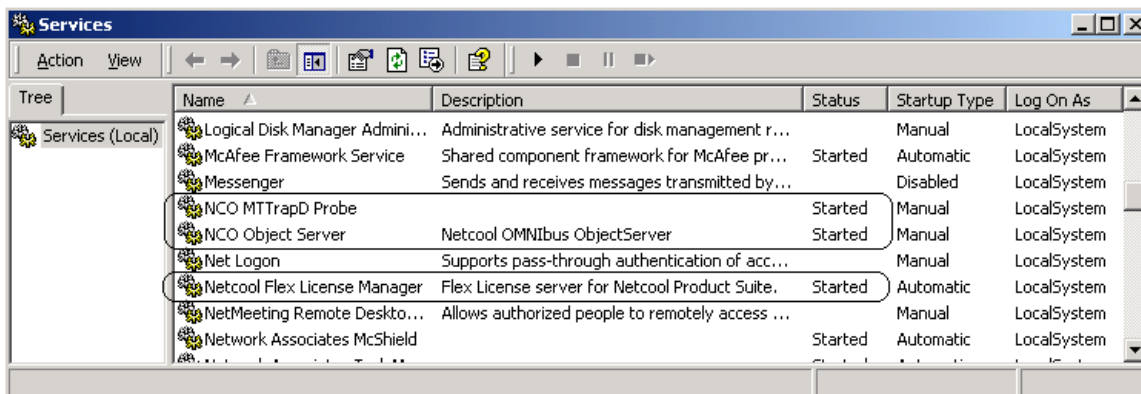


Figure 15: Netcool/OMNibus Applications in Windows Services

5.6. Start the Event List Application

The alert or event information stored in the Netcool ObjectServer can be viewed through the Event List application in the Desktop Tools. To start the Event List application, select Start→Programs→Netcool OMNibus→Event List. Log in with the appropriate username and password. In the Event List Login window, specify the ObjectServer to connect to, which is NCOMS in this case. Click on the **OK** button.

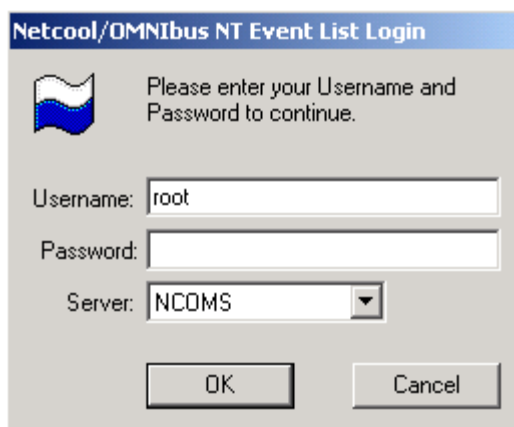


Figure 16: Event List Login Window

After logging in, the Monitor Box window is displayed, as shown in **Figure 17**. The **Monitor Box** window contains monitor boxes that represent a list of events that match a particular criteria or filter. A monitor box is identified by its name located at the top of each monitor box, such as “All Events” or events captured in the “Last 10 Min...”. To view the event information for a particular monitor box, click on the ellipsis button. The Event List illustrated in **Figure 18** is displayed. The Event List displays event information in a scrollable list that is color-coded based on the severity of the alert or event. The colors and severity levels supported by Netcool/OMNibus are summarized in **Table 1**. Events captured by the Netcool Probe are assigned a severity in the rules file generated in Section 5.2. For more information on using the Event List application, refer to reference [5].

Severity	Description	Desktop Color
5	Critical	Red
4	Major	Orange
3	Minor	Yellow
2	Informational	Blue
1	Indeterminate	Purple
0	Clear	Green

Table 1: Netcool/OMNIBus Severity Levels

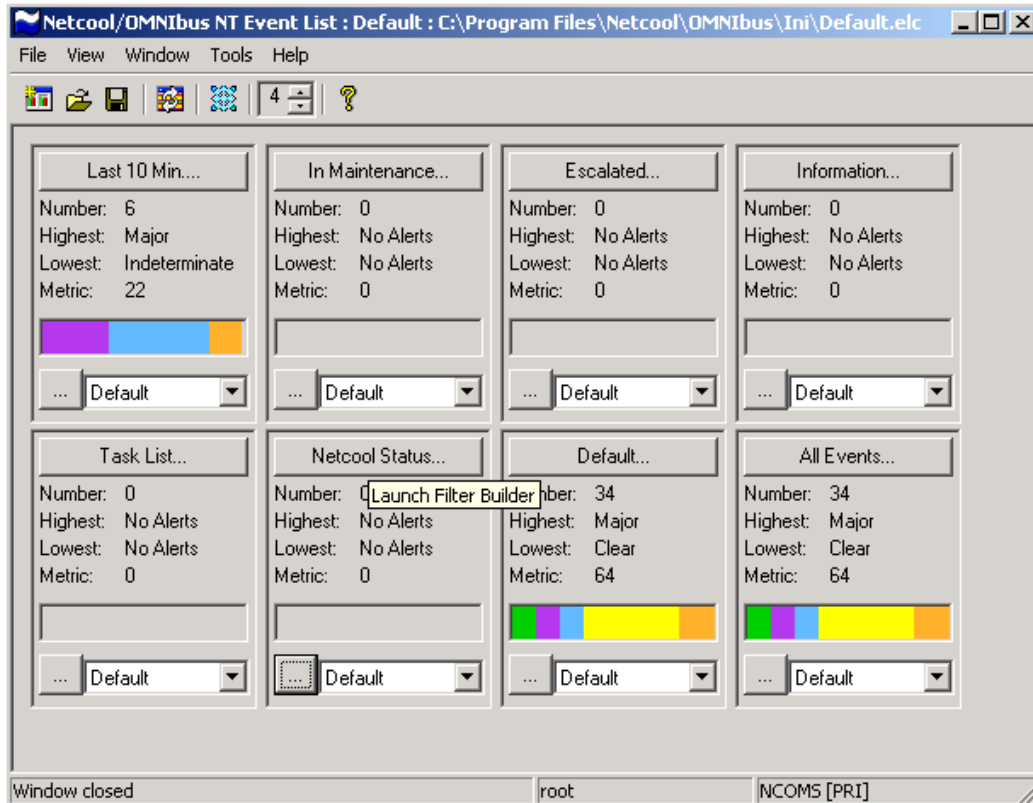


Figure 17: Event List - Monitor Box Window

Node	Alert Group	Summary
10.1.1.3	cmgModule	[QuietOutput NOT SET!!!] Media module VoIP successfully inserted
server1	proxy	[QuietOutput NOT SET!!!] proxyUp: The user has issued a start proxy-agent comman
10.1.1.3	cmgModule	[QuietOutput NOT SET!!!] Media module T1E1 has been removed
10.1.1.3	cmgModule	[QuietOutput NOT SET!!!] Media module DCP has been removed
10.1.1.3	cmgModule	[QuietOutput NOT SET!!!] Media module VoIP has been removed
10.1.1.3	cmgManagementManual...	[QuietOutput NOT SET!!!] A media module is beginning a user-requested reset operati
10.1.1.3	cmgSyncSignal	[QuietOutput NOT SET!!!] Synchronization signal lost
10.1.1.3	cmgModule	[QuietOutput NOT SET!!!] Media module T1E1 has been removed
10.1.1.3	cmgManagementManual...	[QuietOutput NOT SET!!!] A media module is beginning a user-requested reset operati
10.1.1.3	cmgH248Link	[QuietOutput NOT SET!!!] The H.248 link between the media gateway and its control
10.1.1.3	cmgRegistration	[QuietOutput NOT SET!!!] The media gateway has successfully registered with a cont
10.1.1.3	cmgManagementManual...	[QuietOutput NOT SET!!!] A media module is beginning a user-requested reset operati
10.1.1.3	cmgVoipManualReset	[QuietOutput NOT SET!!!] A VoIP engine is beginning a user-requested reset operati
server1	proxy	[QuietOutput NOT SET!!!] proxyDown: The user has issued a stop proxy-agent comm
10.1.1.3	cmgIccMissing	[QuietOutput NOT SET!!!] The Internal Communications Controller expected in slot 1 i
10.1.1.3	cmgIccMissing	[QuietOutput NOT SET!!!] An Internal Communications Controller expected in slot 1 is
10.1.1.3	cmgH248Link	[QuietOutput NOT SET!!!] The H.248 link between the media gateway and its control
definity1 (1000000000)	Internal Switch Alarms	[QuietOutput NOT SET!!!] IPMEDPRO (1079385278) (OnBoard)
definity1 (1000000000)	Internal Switch Alarms	[QuietOutput NOT SET!!!] IPMEDPRO (1079381775) (OnBoard)
definity1 (1000000000)	Internal Switch Alarms	[QuietOutput NOT SET!!!] IPMEDPRO (1079381725) (OnBoard)
definity1 (1000000000)	Internal Switch Alarms	[QuietOutput NOT SET!!!] IPMEDPRO (1079381693) (OnBoard)
definity1 (1000000000)	Internal Switch Alarms	[QuietOutput NOT SET!!!] IPMEDPRO (1079381523) (OnBoard)

6 4 7 16 7 0

0 rows selected 03/15/2004 03:03:35 PM root NCOMS [PRI]

Figure 18: Event List Window

6. Interoperability Compliance Testing

The objective of the interoperability compliance test was to verify that the Micromuse Netcool/OMNIBus Event Management System could receive v1, v2c, and v3 SNMP traps from the Avaya S8300 and S8700 Media Servers, and v1 SNMP traps from the Avaya G700 Media Gateway. The collected SNMP traps were viewed with the Netcool Event List application.

6.1. General Test Approach

All test cases were performed manually. The general test approach used for the compliance testing included:

- Generating v1, v2c, and v3 SNMP traps from the Avaya S8300 and S8700 Media Servers and v1 SNMP traps from the Avaya G700 Media Gateway, including the P330 Stack Processor and the MGP.
- Using a protocol analyzer to verify that SNMP traps were sent from the Avaya Media Server and Gateways to the Netcool/OMNIBus system.
- Viewing the SNMP traps with the Netcool Desktop application.

6.2. Test Results

All tests were completed successfully. Netcool/OMNIBus successfully captured and processed the event information sent by the Avaya Media Servers and Gateways using v1, v2c, and v3 SNMP traps. Importing the Avaya SNMP MIBs using a Netcool rules file is necessary to achieve interoperability between the Avaya Media Servers and Gateways and

Netcool/OMNIBus. The customer should contact Micromuse Support for assistance in developing the trap rules.

7. Verification Steps

To verify the network management solution using the Micromuse Netcool/OMNIBus Event Management System to capture SNMP traps from the Avaya Media Servers and Gateways, the following steps were performed:

- Check IP communication between the Avaya Media Servers and Gateways and Netcool/OMNIBus server using the “ping” command.
- Verify that the Netcool/OMNIBus applications are running under Windows Services.
- Generate an event or alarm, such as restarting the Master SNMP Agent on the web interface, from each Avaya Media Server and Gateway and verify that the SNMP trap was received. A protocol analyzer may be used to verify that the Avaya Media Server sent the SNMP trap to the Netcool/OMNIBus server.

If the event or alarm is not displayed in the Netcool Event List, check the following items:

- Check that the Event List application is not incorrectly filtering out events/alarms.
- Check that the alarm reporting options in the Avaya Communication Manager **set options** form is allowing the appropriate alarms to be reported.
- Check the SNMP trap destinations in the Avaya Media Servers and Gateways.
- Check that the firewall in the Avaya Media Server is allowing SNMP traps to be sent on UDP port 162.
- Check that the MTTrapd Probe is listening for SNMP traps on UDP port 162.

8. Support

	Address	Telephone	Fax	World Wide Web/Email
USA	Micromuse Inc. Customer Support Services 139 Townsend Street San Francisco, CA 94107 USA	1-800-Netcool +1 415 538 9090	+1 415 538 9091	http://www.micromuse.com support@micromuse.com
EUROPE	Micromuse Ltd. Customer Support Services Disraeli House 90 Putney Bridge Road London SW18 1DA United Kingdom	+44 (0) 20 8877 0073	+44 (0) 20 8875 0991	http://www.micromuse.com support@micromuse.com

9. Conclusion

These Application Notes illustrate the configuration steps required to enable the Micromuse Netcool/OMNIBus Event Management System to monitor a network of Avaya Media Servers and Gateways for significant events and alarms. Compliance testing was successful as

Netcool/OMNIBus captured v1, v2c, and v3 SNMP traps sent by the Avaya Media Servers and Gateways. Netcool/OMNIBus also processed the event information and displayed it in a meaningful way.

10. Additional References

This section references the Avaya and Micromuse product documentation relevant to these Application Notes. The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] Maintenance Alarms Reference, Issue 1, November 2003; Document Number 555-245-102.
- [2] Maintenance Command Reference, Issue 1, November 2003; Document Number 555-245-102.

The following Micromuse product documentation was referenced during the interoperability compliance test.

- [3] Netcool/OMNIBus 3.6 Installation and Deployment Guide
- [4] Netcool/OMNIBus 3.6 Administration Guide
- [5] Netcool/OMNIBus 3.6 User Guide
- [6] Micromuse Standards for Probe Rules Files (MUSE-STD-RF-02e, July 2002)

Appendix A: Avaya SNMP MIB Files

This appendix lists the SNMP MIB files required for the Avaya S8300 and S8700 Media Servers and the Avaya G700 Media Gateway. The G700 Media Gateway requires the MIB files for the Avaya P333T Gigabit Ethernet Switch.

Server or Device	MIB and *trapd files	Purpose of MIB files
Avaya S8300 and S8700 Media Servers	g3mib.asn1 g3proxy.trapd	MIB definition for Avaya Communication Manager
Avaya G600 Media Gateway	N/A	Covered by the Avaya S8700 Media Server
Avaya G700 Media Gateway	CMG.MIB Avaya P333T Gigabit Ethernet Switch MIBs (see below)	MIB definition for the Avaya G700 Media Gateway
Avaya P333T Gigabit Ethernet Switch	LOAD-MIB.MY	Defines upload/download of application
	Applic.mib	Information related to the applications that manage the packet switching family of Avaya products
	Config.mib	Generic information for the management of the Avaya switches (modules, ports)
	Gen.mib	OIDs that identify the Avaya switches and modules
	genlic.mib	Information related to licensing
	mdgstack.mib	Control on agent versions and upload of new versions
	Xswtch.mib	Specific information for the management of the Avaya switches (modules, ports)
	Policy.mib	MIB for policy control
	rfc1493.mib	bridge mib
	rfc12313.mib	interfaces mib
	rfc1757.mib	RMON MIB
	rfc1513.mib	Token Ring RMON mib
	rfc2021.mib	RMON2 mib
	rfc2613.mib	RMON mib for switched networks
P330traps113.mib	Trap definition	

Table 2: Avaya SNMP MIB Files

Appendix B: Using the Mib2Rules Utility Tool

Note: This appendix provides high-level instructions for generating a Netcool rules file from the Avaya SNMP MIB files using the Mib2Rules utility provided by Micromuse. The customer should contact Micromuse Support for a copy of the Mib2Rules utility and for assistance in the custom development of the trap rules. The rules file impacts the behavior of Micromuse Netcool/OMNIbus and modifications to the rules file should be considered carefully. See reference [6] for more information on rules file development.

The Mib2Rules (M2R) utility tool from Micromuse is a GUI based tool for reading (importing) SNMP MIBs and storing them. The Mib2Rules (m2r) utility is a Perl script, so Perl is required on the server where the utility will be run. The instructions below are for running the utility on a Windows 2000 PC. Expand the m2r distribution file into any directory. Locate the m2r file and add the 'pl' extension (m2r.pl). Finally, set the following environment variable in Windows:

Variable:	M2RHOME
Value:	\Program Files\m2r (or the directory where the Perl script is stored)

Follow these steps to create the `avaya.m2r.include.rules` file and the `m2r.varbind.lookup` file. For this example, the m2r files were copied to the `C:\Program Files\m2r` directory.

1. Create a subdirectory under `C:\Program Files\m2r\mibs` called "Avaya".
2. Copy all of the Avaya MIB files into that directory (see **Appendix A** for list of MIB files).
3. Run the m2r utility. The **Mib2rules** screen shown below is displayed.
4. Set the **Input Directory** to `C:\Program Files\m2r\mibs`.
5. Ensure that the **Traverse Subdirectories** radio button is selected.
6. Click on the **Import ALL** button.
7. Once the entire MIB tree is built and displayed, scroll down to the Avaya enterprise section by searching for "6889 Avaya".
8. Under the **Export** section, enter a directory path for the **Export Directory**.
9. Ensure that the **Selected subtree only** radio button is selected.
10. Click on the **Export** button.
11. Two files are created in the export directory: `avaya.m2r.include.rules` and `m2r.varbind.lookup`.

The m2r utility generates the `avaya.m2r.include.rules` file that should be used as a starting point for the rules file. The rules file will require modifications to some of the trap attributes so that the event summary is descriptive and meaningful and so de-duplication and correlation of events are performed correctly by Netcool/OMNIbus. Some of the attributes in the rules file that may require modification are:

- The **Summary** field that provides the 'descriptive' text used to identify the real nature of the problem.
- The **Severity** field that specifies the severity of the event or alarm.
- The **AlertGroup**, **AlertKey**, and **Type** fields that are used for correlating alarms.
- The **Identifier** field that is used for de-duplicating events or alarms.

The table entries in the `m2r.varbind.lookup` file should be added to the `VarbindValTable` table of the original `m2r.varbind.lookup` file.

Once the `avaya.m2r.include.rules` file and the `m2r.varbind.lookup` file have been completed, the `nco_p_syntax.exe` program may be used to check the files for syntax errors. To check for syntax errors, open a command prompt window and go to the `C:\Program Files\Netcool\OMNIbus\probes\nt351` directory. Type the `nco_p_syntax -rulesfile mttrapd.rules` command at the prompt and verify that the output did not identify any lines with a syntax error. Note that the default rules filename is used.

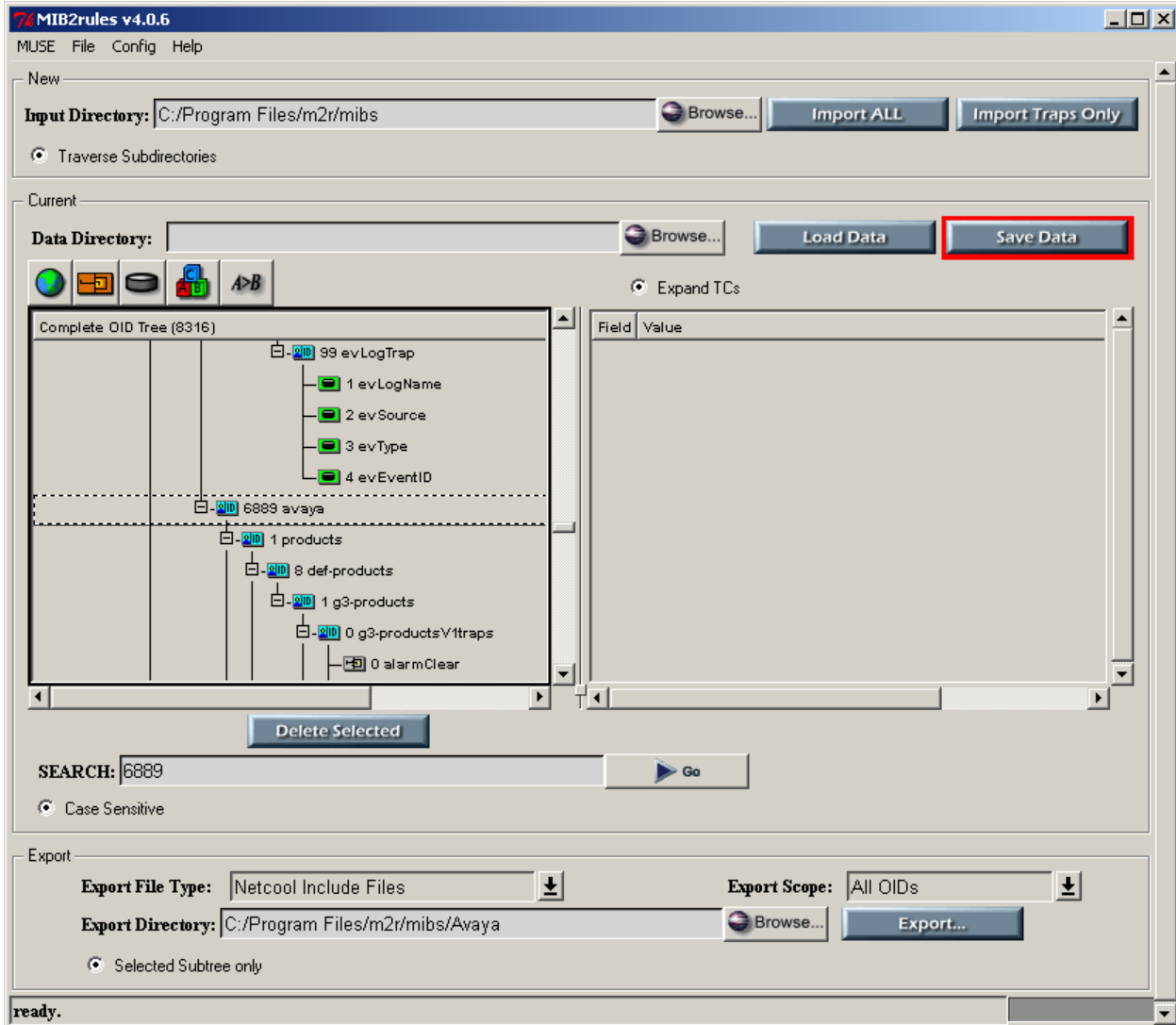


Figure 19: Mib2rules Window

©2004 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.