

# **Service Managed Gateway™**

## **How to Configure SNMP on an SMG**

Issue 1.2

Date 19 June 2010

---

<b>1</b>	<b>About this document .....</b>	<b>3</b>
<b>1.1</b>	<b>Scope .....</b>	<b>3</b>
<b>1.2</b>	<b>Readership .....</b>	<b>3</b>
<b>1.3</b>	<b>More information.....</b>	<b>3</b>
<b>1.4</b>	<b>Terminology .....</b>	<b>3</b>
<b>2</b>	<b>Introduction .....</b>	<b>4</b>
<b>2.1</b>	<b>How does the SMG implement SNMP? .....</b>	<b>4</b>
<b>3</b>	<b>Configuring the SMG.....</b>	<b>5</b>
<b>3.1</b>	<b>Configuring SNMP on the SMG.....</b>	<b>5</b>
3.1.1	Configure the SNMP agent .....	6
3.1.2	Configure SNMP managers.....	8
3.1.3	Modify a configured SNMP manager .....	11
3.1.4	Delete a configured SNMP manager .....	12
<b>4</b>	<b>Diagnostics.....</b>	<b>13</b>
<b>4.1</b>	<b>Trace analyzer.....</b>	<b>13</b>
<b>4.2</b>	<b>Tracing using the command line.....</b>	<b>14</b>
4.2.1	Command line syntax .....	14

---

Copyright 2010 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. Third party trademarks are the property of the third parties.

# 1 About this document

This document describes how to configure the Service Managed Gateway (SMG) for setting up an SNMP agent.

## 1.1 Scope

This document explains how to:

- configure an SNMP agent on the SMG;
- configure SNMP managers on the SMG; and
- utilise the diagnostic and trace analyser tools on the SMG.

## 1.2 Readership

This document is for engineers who have previous experience configuring and managing networks.

## 1.3 More information

For more information about managing the SMG, read the Service Managed Gateway documentation. The current documentation is available online at <http://virtualaccess.com/smgdocs/>

## 1.4 Terminology

<b>ASCII</b>	American Standard Code for Information Interchange
<b>IP</b>	Internet Protocol
<b>LAN</b>	Local Area Network
<b>MIB</b>	Management Information Base
<b>PC</b>	Personal Computer
<b>SLA</b>	Service Level Agreement
<b>SMG</b>	Service Managed Gateway
<b>SNMP</b>	Simple Network Management Protocol
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide Area Network

## 2 Introduction

Simple Network Management Protocol (SNMP) is a set of protocols used to communicate network management information between a management station and a software module, known as an SNMP agent, running on a network entity. For example, a network entity can be a host, server, or router. A management station can be any station running an application that allows it to monitor or control an SNMP agent.

The agent will provide the management station with access to information about the network device the agent is running on. The information that is available to the management station depends on the Management Information Base (MIB). The MIB is a virtual hierarchical structure that allows the agent to store and organise data on a network device.

### 2.1 How does the SMG implement SNMP?

The SMG allows you to configure a local SNMP agent and up to 10 remote SNMP management stations that the agent can communicate with.

The communication between the agent and the management station is through SNMP. The agent supports both MIB version I and version II and vendor specific MIBs.

The SMG supports the use of the SNMP TRAP operation. This allows the SMG to send events to a configured SNMP manager.

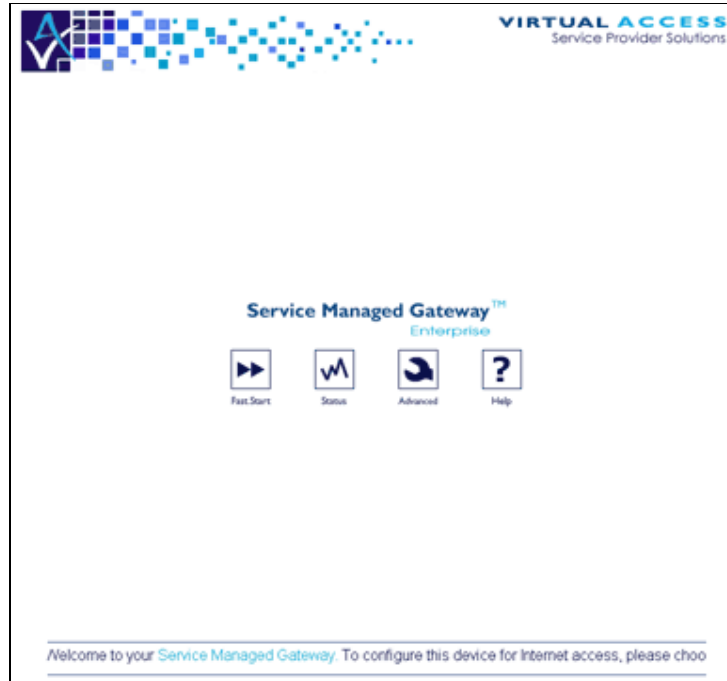
To configure the SMG to send an event SNMP as a trap, read 'How to Configure an Event Filter on an SMG'.

It is not possible to control the SMG from a management station. The SMG only supports 'get' commands. No SNMP 'set' commands are supported. So configuration updates cannot be made from the management station.

## 3 Configuring the SMG

The Service Managed Gateway (SMG) contains an internal web server that is used to configure the SMG. Before you can access the internal web server and start the SMG configuration, you must ensure that your PC has the correct networking set up.

When your Service Managed Gateway is correctly connected to your PC, type `fast.start` into the URL line of your browser to display the Start page.



**Figure 1: The SMG start page**

If a login page appears type in the login password you received from your administrator.

If you have not received a password, contact the Virtual Access Support team.

Access the Fast Start Wizard by clicking the Fast.Start icon on the Start page of the embedded web.

The Fast Start Wizard will guide you through a series of forms that you must complete to configure your SMG.

### 3.1 Configuring SNMP on the SMG

To configure SNMP on the SMG, click **Advanced** on the SMG Start page. The Advanced menu appears.

In the left-hand menu, click **Expert View**.

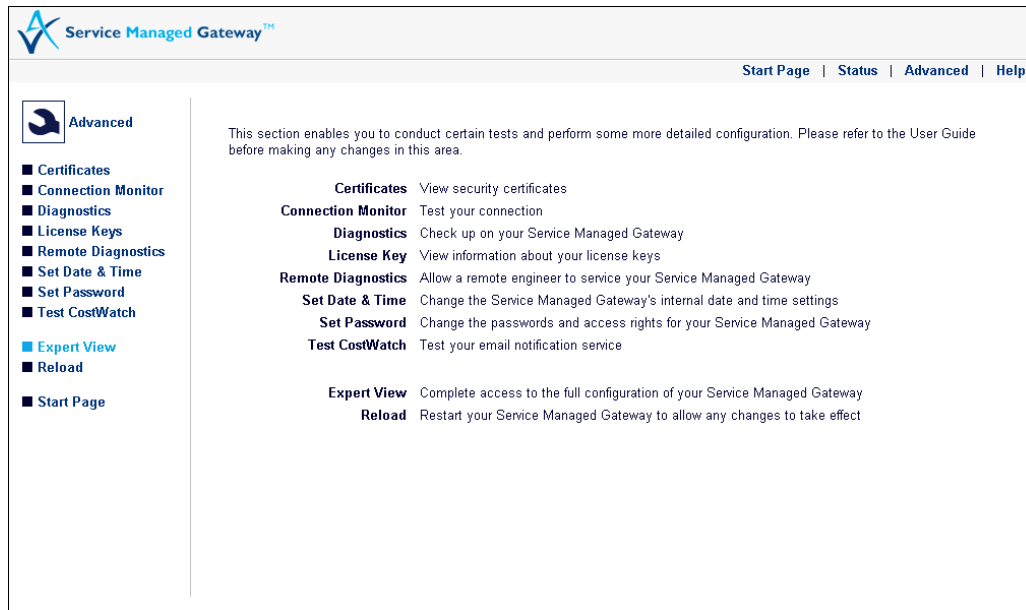


Figure 2: The advanced menu showing the expert view

### 3.1.1 Configure the SNMP agent

The SNMP agent is the device responsible for performing the network management operations requested by the SNMP manager. The SNMP Agent form contains the options required to configure an SNMP agent. The options in this form are used in conjunction with the SNMP Manager form and Local Password form to allow remote monitoring of the instant access router.

In the Expert View menu, select **System -> snmp -> snmp agent**. The SNMP Agent page appears. To access the advanced options, click **Advanced**.

Figure 3: The advanced SNMP agent page

Field	Description	Command Line								
<b>Enabled</b>	<p>This option enables or disables SNMP on the selected device. Select <b>yes</b> if the SMG is to be managed in an SNMP environment.</p> <table border="1"> <tr> <td><b>yes</b></td> <td>Allows SNMP messages to be generated by this device.</td> </tr> <tr> <td><b>no</b></td> <td>Disables SNMP on the device.</td> </tr> </table>	<b>yes</b>	Allows SNMP messages to be generated by this device.	<b>no</b>	Disables SNMP on the device.	Set SNMP System Enabled =				
<b>yes</b>	Allows SNMP messages to be generated by this device.									
<b>no</b>	Disables SNMP on the device.									
<b>Name</b>	<p>Enter a name to associate with the system for SNMP. The SNMP name is an ASCII string containing up to 64 alphanumeric characters. Spaces and control characters are not supported; other ASCII characters such as dash (-) or underscore (_) are allowed. This string appears in the sysName variable of the SNMP MIB system group. This field is mandatory.</p> <table border="1"> <tr> <td><b>Minimum length</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>Unspecified</td> </tr> <tr> <td><b>Maximum length</b></td> <td>255</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum length</b>	0	<b>Default value</b>	Unspecified	<b>Maximum length</b>	255	<b>Units</b>	String	Set SNMP System Name =
<b>Minimum length</b>	0									
<b>Default value</b>	Unspecified									
<b>Maximum length</b>	255									
<b>Units</b>	String									

<b>Contact</b>	<p>Enter the name or email address of the person responsible for the system. You can enter up to 64 alphanumeric characters in length. Spaces and control characters are not supported; printable ASCII characters such as the 'at' sign (@) or full stop (.) are allowed. Contact is stored in the sysContact variable of the SNMP MIB System group.</p> <table border="1" data-bbox="500 405 1019 604"> <tr> <td><b>Minimum length</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>Unspecified</td> </tr> <tr> <td><b>Maximum length</b></td> <td>255</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum length</b>	0	<b>Default value</b>	Unspecified	<b>Maximum length</b>	255	<b>Units</b>	String	Set SNMP Contact =
<b>Minimum length</b>	0									
<b>Default value</b>	Unspecified									
<b>Maximum length</b>	255									
<b>Units</b>	String									
<b>Location</b>	<p>Enter a string that describes the location, such as a city or building where the SNMP manager resides. This field allows up to 64 alphanumeric characters. Spaces are allowed. Location information is stored in the sysLocation variable of the SNMP MIB System group.</p> <table border="1" data-bbox="500 804 1019 947"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>Unspecified</td> </tr> <tr> <td><b>Maximum value</b></td> <td>255</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum value</b>	0	<b>Default value</b>	Unspecified	<b>Maximum value</b>	255	<b>Units</b>	String	Set SNMP Location =
<b>Minimum value</b>	0									
<b>Default value</b>	Unspecified									
<b>Maximum value</b>	255									
<b>Units</b>	String									
<b>IP Address</b>	<p>The local IP address of the SNMP agent. It is the source IP address that is used when sending SNMP traps to the SNMP manager. The default is 0.0.0.0, which uses the IP address of the port that the packet goes out on. Format a.b.c.d</p>	Set SNMP System IP Address =								

**Table 1: SNMP system fields and their descriptions**

### 3.1.2 Configure SNMP managers

An SNMP management station is identified by its IP address and 'Read Community' string.

Each SNMP manager index allows you to configure either a single IP address, or a range of IP addresses.

The SMG will only respond to polls from SNMP managed stations whose IP address matches the configured IP address, or whose IP address falls within the configured range of IP addresses.

**Note:** if a range of IP addresses are configured, any SNMP traps that are sent from the SMG event system will only be sent to the **first** IP address in the range.

In the Expert View menu, select **System -> snmp -> snmp manager**. The SNMP Manager List page appears. This list identifies the configured SNMP Managers.

Index	Enabled	Name	IP Address	Operation
1	Yes	monitor	135.196.203.82	<a href="#">modify/delete</a>
2	Yes	SNMP Test	0.0.0.0	<a href="#">modify/delete</a>
3	unconfigured	-	-	<a href="#">add</a>
4	unconfigured	-	-	<a href="#">add</a>
5	unconfigured	-	-	<a href="#">add</a>
6	unconfigured	-	-	<a href="#">add</a>
7	unconfigured	-	-	<a href="#">add</a>
8	unconfigured	-	-	<a href="#">add</a>
9	unconfigured	-	-	<a href="#">add</a>
10	unconfigured	-	-	<a href="#">add</a>

**Figure 4: The SNMP manager list**

Use the SNMP Managers page to view, create, or modify the characteristics of the SNMP management stations that have access to the selected device.

To create a new SNMP Manager, in the Operation column, click **add**. The SNMP Manager Entry page appears.

To access the advanced SNMP Manager configuration fields, click **Advanced**.

## Snmp Manager Entry 3

---

**Enabled**

**Name**

**IP Address**

**IP Address End**

**Agent IP Address**

**Read Community**

**Write Community**

**Trap Community**

**Trap IP Address**

Figure 5: The advanced SNMP manager entry page

Field	Description	Command Line								
<b>Enabled</b>	<p>This option enables or disables SNMP on the selected device. This is required when the SMG is to be managed in an SNMP environment.</p> <table border="1"> <tr> <td><b>yes</b></td> <td>Enable SNMP management station.</td> </tr> <tr> <td><b>no</b></td> <td>Disable SNMP management station.</td> </tr> </table>	<b>yes</b>	Enable SNMP management station.	<b>no</b>	Disable SNMP management station.	Set SNMP Manager Configured =				
<b>yes</b>	Enable SNMP management station.									
<b>no</b>	Disable SNMP management station.									
<b>Name</b>	<p>Identifies the manager by entering an ASCII string of up to 16 characters. Spaces are not allowed.</p> <table border="1"> <tr> <td><b>Minimum length</b></td> <td>1</td> </tr> <tr> <td><b>Default value</b></td> <td>Unspecified</td> </tr> <tr> <td><b>Maximum length</b></td> <td>16</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum length</b>	1	<b>Default value</b>	Unspecified	<b>Maximum length</b>	16	<b>Units</b>	String	Set SNMP Manager Name =
<b>Minimum length</b>	1									
<b>Default value</b>	Unspecified									
<b>Maximum length</b>	16									
<b>Units</b>	String									
<b>IP Address</b>	<p>Defines the IP address of the SNMP management server, in dotted decimal notation. Format a.b.c.d</p>	Set SNMP Manager IP Address =								
<b>IP Address End</b>	<p>Defines the end IP address of a range of SNMP management servers. The SNMP agent will only respond to SNMP management servers within this range of IP addresses. If set to 0.0.0.0 then only one SNMP management server applies (as defined by the IP address field above).</p> <p><b>Note:</b> If a range of SNMP management servers is configured, SNMP traps will only be sent to the <b>first</b> SNMP management server in the range.</p>	Set Snmp Manager Ip Address End								

<b>Agent IP Address</b>	This field allows the user to set the source IP address of an SNMP Packet to a non WAN IP Address. This is useful when users want to send SNMP information through a VPN tunnel and the traffic must have a source IP address of the Local LAN. Format: <b>a.b.c.d</b>	Set SNMP Manager Agent IP Address =								
<b>Read Community</b>	This advanced configuration option specifies the community name to be used by the SNMP Manager to access the router MIB for SNMP Get and Get-Next requests. Read Community is entered as an ASCII string. <table border="1"> <tr> <td><b>Minimum length</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>public</td> </tr> <tr> <td><b>Maximum length</b></td> <td>64</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum length</b>	0	<b>Default value</b>	public	<b>Maximum length</b>	64	<b>Units</b>	String	Set SNMP Manager Read Community Name =
<b>Minimum length</b>	0									
<b>Default value</b>	public									
<b>Maximum length</b>	64									
<b>Units</b>	String									
<b>Write Community</b>	This advanced configuration option specifies which community name the SNMP Manager uses to access the router MIB for SNMP Set requests. Write Community is entered as an ASCII string. <table border="1"> <tr> <td><b>Minimum length</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>netman</td> </tr> <tr> <td><b>Maximum length</b></td> <td>64</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum length</b>	0	<b>Default value</b>	netman	<b>Maximum length</b>	64	<b>Units</b>	String	Set SNMP Manager Write Community Name =
<b>Minimum length</b>	0									
<b>Default value</b>	netman									
<b>Maximum length</b>	64									
<b>Units</b>	String									
<b>Trap Community</b>	This option specifies the community name the device uses when issuing SNMP Traps. Trap Community is entered as an ASCII string. <table border="1"> <tr> <td><b>Minimum length</b></td> <td>1</td> </tr> <tr> <td><b>Default value</b></td> <td>public</td> </tr> <tr> <td><b>Maximum length</b></td> <td>64</td> </tr> <tr> <td><b>Units</b></td> <td>String</td> </tr> </table>	<b>Minimum length</b>	1	<b>Default value</b>	public	<b>Maximum length</b>	64	<b>Units</b>	String	SET SNMP Manger Trap Community Name
<b>Minimum length</b>	1									
<b>Default value</b>	public									
<b>Maximum length</b>	64									
<b>Units</b>	String									
<b>Trap IP Address</b>	This field allows users to specify the address which is present in the SNMP header. For some SNMP Managers the SNMP header address must match the IP source address. If the source address is configured to meet a VPN configuration then this IP address can also be set to the local LAN IP address. Format: <b>a.b.c.d</b>	Set SNMP Manager Trap IP Address =								

Table 2: SNMP manager fields and their descriptions

### 3.1.3 Modify a configured SNMP manager

In the Expert View menu, select **System -> snmp -> snmp manager**. The SNMP Manager List page appears.

### SNMP Manager List

Index	Enabled	Name	IP Address	Operation
1	Yes	monitor	135.196.203.82	<a href="#">modify/delete</a>
2	Yes	SNMP Test	0.0.0.0	<a href="#">modify/delete</a>
3	unconfigured	-	-	<a href="#">add</a>
4	unconfigured	-	-	<a href="#">add</a>
5	unconfigured	-	-	<a href="#">add</a>
6	unconfigured	-	-	<a href="#">add</a>
7	unconfigured	-	-	<a href="#">add</a>
8	unconfigured	-	-	<a href="#">add</a>
9	unconfigured	-	-	<a href="#">add</a>
10	unconfigured	-	-	<a href="#">add</a>

Figure 6: The SNMP manager list

In the Operation column on the SNMP Manager List, beside the manager you want to modify. Click **modify/delete**. The SNMP Manager Entry page appears.

Make the required changes and then click **Update**.

### 3.1.4 Delete a configured SNMP manager

In the Expert View menu, select **System -> snmp -> snmp manager**. The SNMP Manager List page appears. Click **modify/delete**. The SNMP Manager Entry page appears.

### Snmp Manager Entry 2

<b>Enabled</b>	<input type="text" value="yes"/>
<b>Name</b>	<input type="text" value="SNMP Test"/>
<b>IP Address</b>	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Advanced"/>	

Figure 7: The SNMP manager entry page

To delete the manager, click **Delete**.

## 4 Diagnostics

The Service Managed Gateway supports extensive remote diagnostics, status and SLA monitoring capabilities.

The status and diagnostics tools are provided as a series of Java applets.

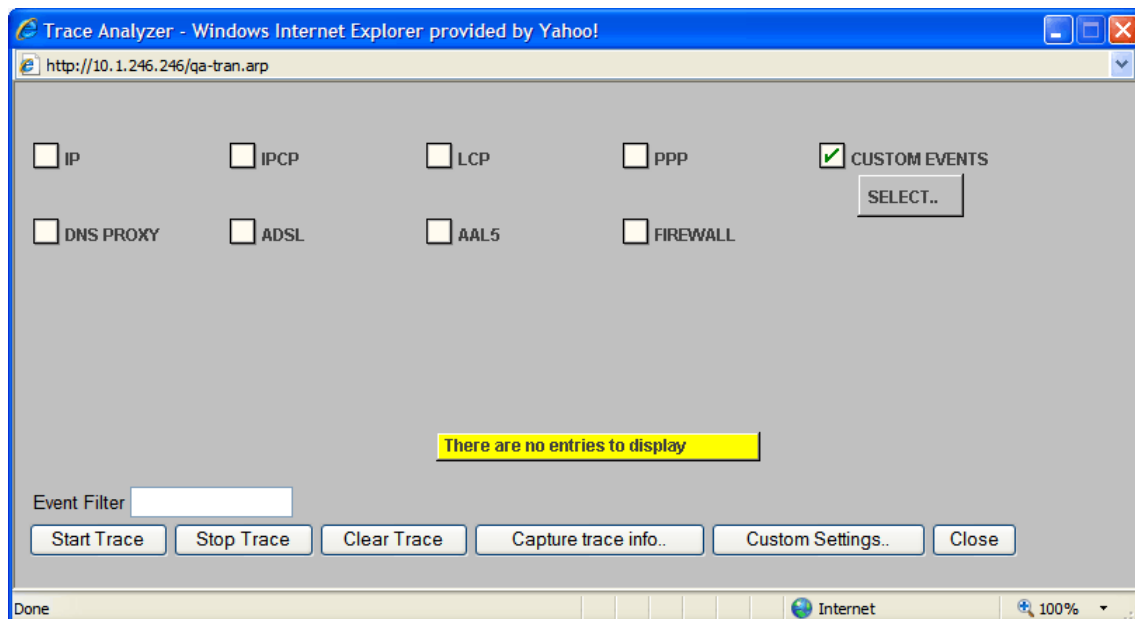
### 4.1 Trace analyzer

The Trace Analyzer provides a web interface to event tracing allowing you to quickly locate and analyze problems.

To view the Trace Analyzer, from the SMG start page, click **Advanced**.

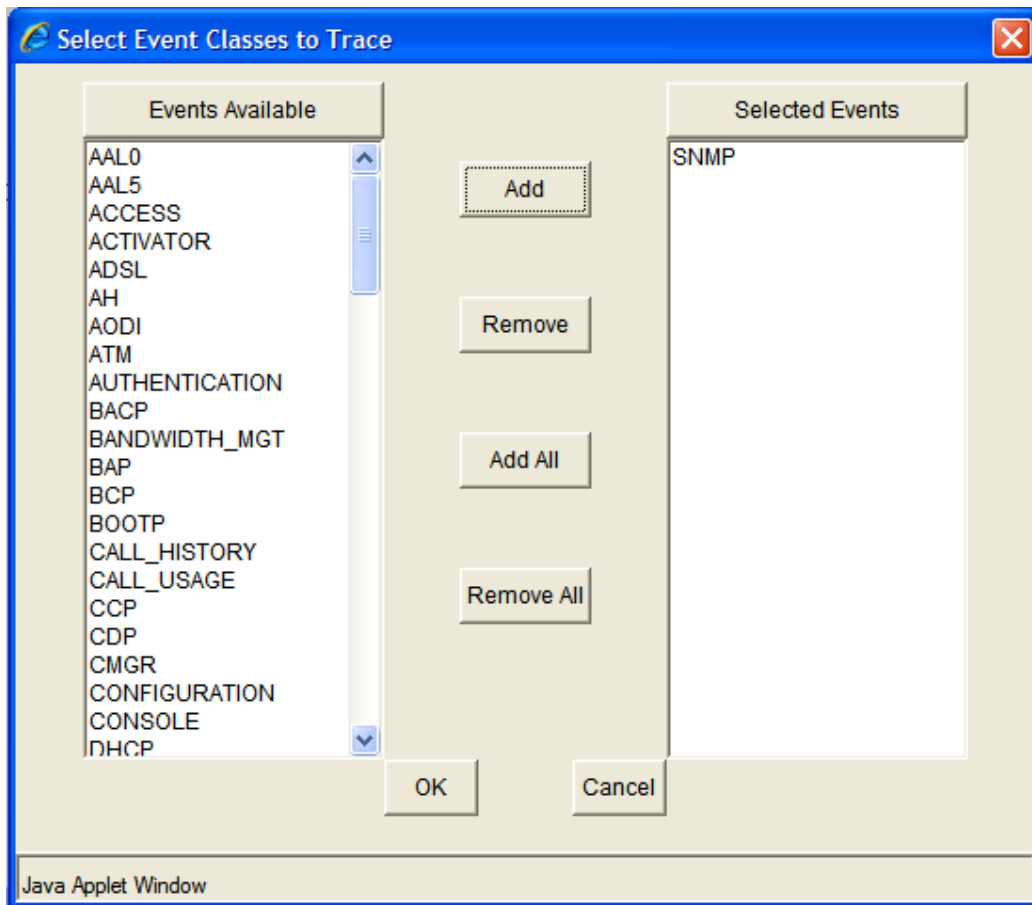
In the **Advanced** menu, click **Diagnostics**.

On the Diagnostics page, click **Trace Analyzer**. The Trace Analyzer pop-up window appears.



To view the SNMP traces, check **Custom Events** and then click **Select**. The Select Events to Trace pop-up window appears.

In the Events Available window, scroll to the bottom of the list and select **SNMP**. Click **ADD** and SNMP appears in the Selected Events window.



**Figure 8: The trace analyzer pop-up window**

Click **OK** to save. The pop-up window closes automatically.

When you have added the events, the Trace Analyzer will capture SNMP events. Click **Start Trace**.

## 4.2 Tracing using the command line

For information on logging on to the command line interface, read the quick guide 'Using the CLI to Manage an SMG'

Tracing through the command line is more flexible than using the trace analyser as you can specify the event severity and use the all class event to trace all event classes.

Command line tracing also allows you to trace to a log file for examining events over a protracted period of time.

If you enter no event severity, all event severities are displayed.

If you chose an event severity, all events of your chosen severity and greater are displayed.

### 4.2.1 Command line syntax

To stop tracing, entering - (minus) followed by the event class will stop tracing for this event class. Entering - (minus) on its own will stop all tracing.

---

<b>Syntax</b>	<b>Description</b>
<b>++snmp</b>	Starts tracing SNMP events
<b>-snmp</b>	Stops SNMP tracing
<b>++ip::161 :162.</b>	SNMP uses UDP ports 161 and 162. To trace SNMP IP packets via the command line, use this syntax.
<b>-- ip</b>	Stops IP tracing.

**Table 3: The command line tracing syntax and their descriptions**

For more information on how to configure diagnostics for the SMG, read the guide 'General Diagnostics'.