

# Service Managed Gateway™

## How to Configure a Syslog Client on an SMG

Issue 1.1

Date 22 July 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 a syslog?.....</b>	<b>4</b>
<b>3</b>	<b>Configuring the SMG.....</b>	<b>5</b>
<b>3.1</b>	<b>Configuring syslog client on the SMG .....</b>	<b>5</b>
3.1.1	Configure the syslog system .....	6
<b>4</b>	<b>Severity definitions .....</b>	<b>9</b>
<b>5</b>	<b>Diagnostics.....</b>	<b>10</b>
<b>5.1</b>	<b>Trace analyzer.....</b>	<b>10</b>
<b>5.2</b>	<b>Tracing using the command line.....</b>	<b>11</b>
5.2.1	Command line syntax .....	11

---

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) or setting up a syslog client.

## 1.1 Scope

This document explains how to:

- configure the SMG for a syslog client; and
- utilise the diagnostic and trace analyzer tools in 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>SLA</b>	Service Level Agreement
<b>SMG</b>	Service Managed Gateway
<b>TCP</b>	Transmission Control Protocol
<b>UDP</b>	User Datagram Protocol

## 2 Introduction

The syslog protocol is an event-based logging service used to forward log messages over a network. It is a client/server standard, with clear text messages sent via UDP (User Datagram Protocol) or TCP (Transmission Control Protocol).

Syslog is used for computer system management and security auditing. It is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

### 2.1 How does the SMG implement a syslog?

The SMG can act as a syslog client and send events to the syslog server. The syslog server can be on the same LAN as the router or on a remote site. The syslog client forwards events based on the event severity to be monitored.

For detailed information on severity levels and their descriptions, read section 4 'Severity definitions'.

In addition to severity-based forwarding, the event filtering system can be configured to forward specific events to the syslog server. For more information on the event filtering system, read '[How to Configure Event Filters on an SMG](#)' guide.

The Syslog Configuration page on the SMG web interface allows you to:

- Enable or disable the syslog client
- Specify the IP address of the syslog server
- Specify the severity on which the events are to be monitored
- Set the process name

## 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.

To enable and configure connections on your SMG, the gateway must be correctly installed, and a valid service must be configured on it.

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.

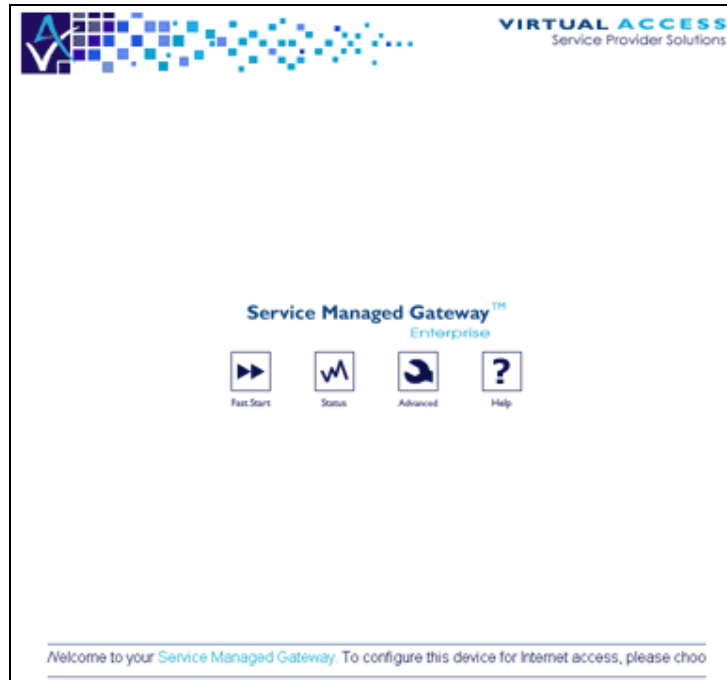


Figure 1: The SMG start page

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 syslog client on the SMG

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

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

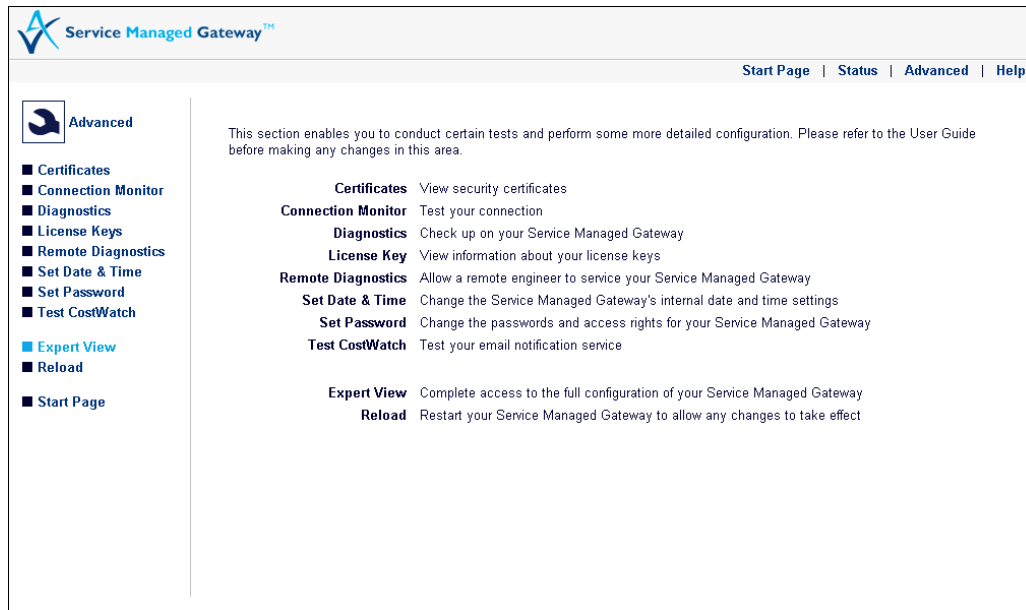


Figure 2: The advanced menu showing expert view

### 3.1.1 Configure the syslog system

In the Expert View menu, select **system -> local clients -> syslog**. The Syslog page appears. To view the advanced options, click **Advanced**.

Figure 3: The advanced syslog client page

Field	Description	Command Line				
<b>Enabled</b>	<p>Enables or disables the syslog client. When syslog is enabled, any events generated by the router having a severity greater than, or equal to, the selected severity level will be sent to the server identified in the Server IP Address field.</p> <p>Select <b>yes</b>.</p> <table border="1"> <tr> <td><b>yes</b></td> <td>Enables the syslog client.</td> </tr> <tr> <td><b>no</b></td> <td>Disables the syslog client.</td> </tr> </table>	<b>yes</b>	Enables the syslog client.	<b>no</b>	Disables the syslog client.	Set Syslog System Enabled =
<b>yes</b>	Enables the syslog client.					
<b>no</b>	Disables the syslog client.					
<b>Server IP Address</b>	<p>Sets the IP address of the syslog server in dotted-decimal notation. Format: a.b.c.d Type in the server IP address.</p>	Set Syslog System Server IP Address =				
<b>Severity</b>	<p>When the syslog system is enabled, any events with a severity greater than, or equal to, the severity level selected in this field are sent to the syslog server. Severity levels are listed in order. Emergency is the highest severity and Debug-Level Messages is the lowest.</p> <p>For detailed information on severity levels, read section 4, 'Severity definitions'.</p>	Set Syslog System Severity =				
<b>Process Name</b>	<p>Sets the name of the process to be sent with the event to the syslog server.</p> <table border="1"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> </table>	<b>Minimum value</b>	0	Set Syslog System Process Name String =		
<b>Minimum value</b>	0					

	<table border="1"> <tr> <td><b>Default value</b></td> <td>\$\$</td> </tr> <tr> <td><b>Maximum value</b></td> <td>32</td> </tr> <tr> <td><b>Units</b></td> <td>Unspecified</td> </tr> </table>	<b>Default value</b>	\$\$	<b>Maximum value</b>	32	<b>Units</b>	Unspecified			
<b>Default value</b>	\$\$									
<b>Maximum value</b>	32									
<b>Units</b>	Unspecified									
<b>Server Port</b>	<p>Sets the application port number on which the Syslog server is listening.</p> <table border="1"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>514</td> </tr> <tr> <td><b>Maximum value</b></td> <td>65535</td> </tr> <tr> <td><b>Units</b></td> <td>Unspecified</td> </tr> </table>	<b>Minimum value</b>	0	<b>Default value</b>	514	<b>Maximum value</b>	65535	<b>Units</b>	Unspecified	<p>Set Syslog System Server Port =</p>
<b>Minimum value</b>	0									
<b>Default value</b>	514									
<b>Maximum value</b>	65535									
<b>Units</b>	Unspecified									
<b>RFC3164 Format</b>	<p>Uses RFC3164 frame.</p> <table border="1"> <tr> <td><b>yes</b></td> <td>Enables RFC3164 format</td> </tr> <tr> <td><b>no</b></td> <td>Disables RFC3164 format</td> </tr> </table>	<b>yes</b>	Enables RFC3164 format	<b>no</b>	Disables RFC3164 format	<p>Set Syslog System RFC3164 Format =</p>				
<b>yes</b>	Enables RFC3164 format									
<b>no</b>	Disables RFC3164 format									
<b>Client IP Address</b>	<p>Sets the local IP address of the syslog client. This is the source IP address that is used when sending IP packets to a syslog server. 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>	<p>Set Syslog System Client IP Address =</p>								

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

## 4 Severity definitions

The following table shows the eight severity levels and their descriptions.

<b>Option</b>	<b>Description</b>
<b>Emergency</b>	A severe service-affecting condition has occurred. Requires immediate corrective action.
<b>Alert</b>	Service or status change has occurred.
<b>Critical</b>	A fault occurred, resulting in severe degradation in capability of system or service. Urgent.
<b>Error</b>	Malfunction or failure not critical to system operation. Take corrective action as soon as possible.
<b>Warning</b>	Potential or pending fault. Correct problem as soon as possible before it becomes a severe, service-affecting fault.
<b>Notice</b>	Service or system notice.
<b>Informational</b>	Service or system status information.
<b>Debug-Level Messages</b>	Troubleshooting and debug messages.

## 5 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.

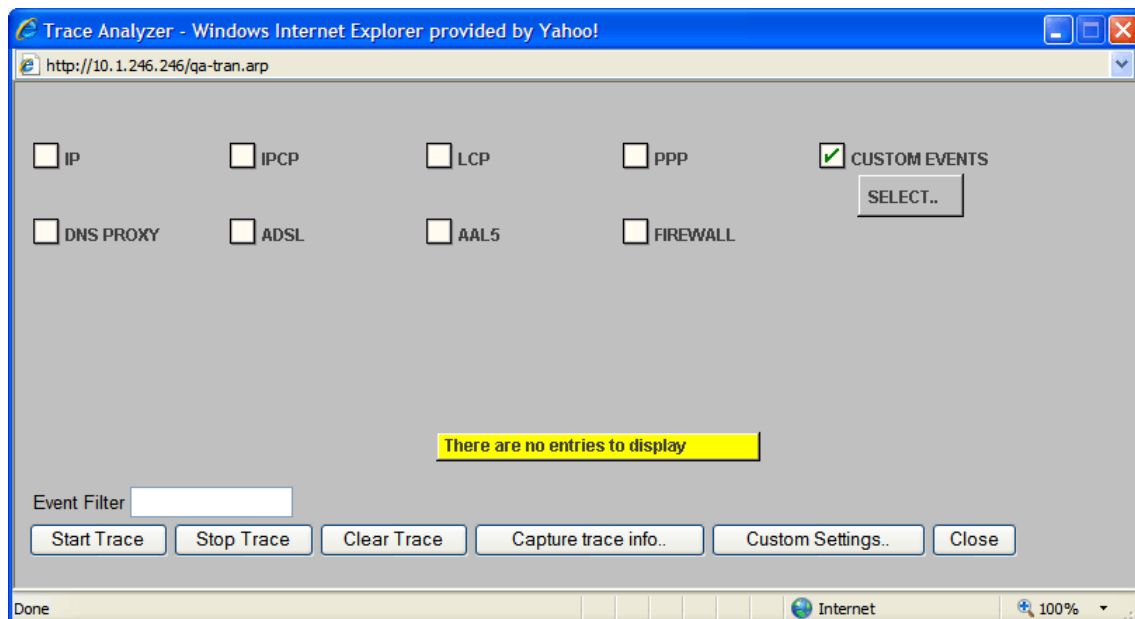
### 5.1 Trace analyzer

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**.

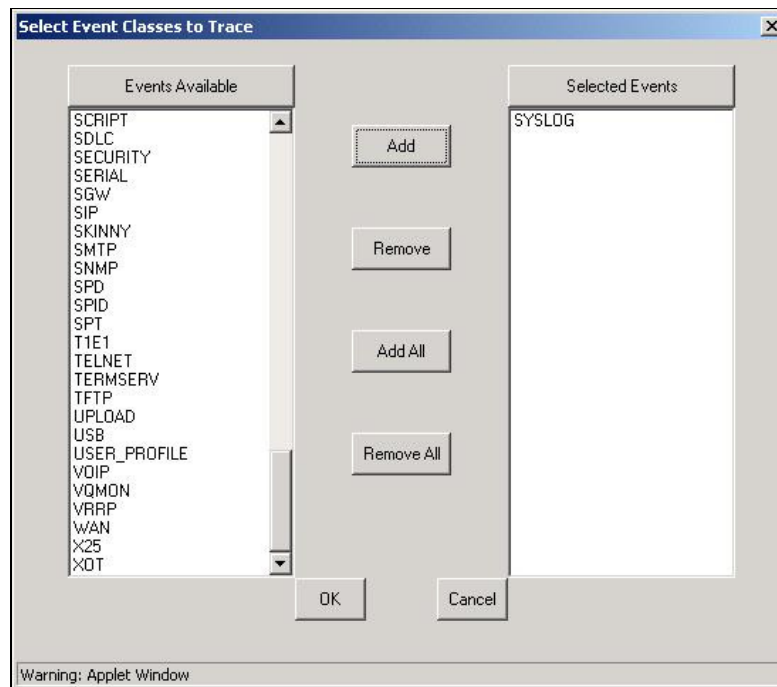
On the Diagnostics page, click **Trace Analyzer**. The Trace Analyzer pop-up window appears.



To view the syslog 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 **SYSLOG**. Click **ADD**. SYSLOG appears in the Selected Events window.

Click **OK** to save.



**Figure 4: The select event classes to trace pop-up window**

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

## 5.2 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 via 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.

### 5.2.1 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.

Syntax	Description
<b>++syslog</b>	Starts tracing Syslog events
<b>-syslog</b>	Stops Syslog tracing

**Table 2: The command line tracing syntax and their descriptions**