



# **Service Managed Gateway™**

## **Configure the Event System for Activator on an SMG**

Issue      CL1  
Date        19 March 2009

<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>3</b>	<b>Configuring the SMG.....</b>	<b>5</b>
<b>3.1</b>	<b>Configuring the HTTP client on the SMG .....</b>	<b>5</b>
<b>4</b>	<b>Diagnostics.....</b>	<b>9</b>

Copyright 2009 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 to enable the event filtering system to connect with Activator.

## 1.1 Scope

This document explains how to:

- configure the SMG for HTTP Client; and
- utilise the diagnostic and trace analyzer 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>SLA</b>	Service Level Agreement
<b>SMG</b>	Service Managed Gateway
<b>VRID</b>	Virtual Router Identifier
<b>HDL</b>	Hardware Description Language

## 2 Introduction

The SMG's event filtering system provides the ability to send events to Activator. You can configure this feature using the HTTP client on the SMG. This document outlines how to configure the HTTP client to connect to Activator, with reference to event filtering.

For more information on how to configure the Event Filtering system, read the 'How to Configure Event Filters on an SMG' guide.

## 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.

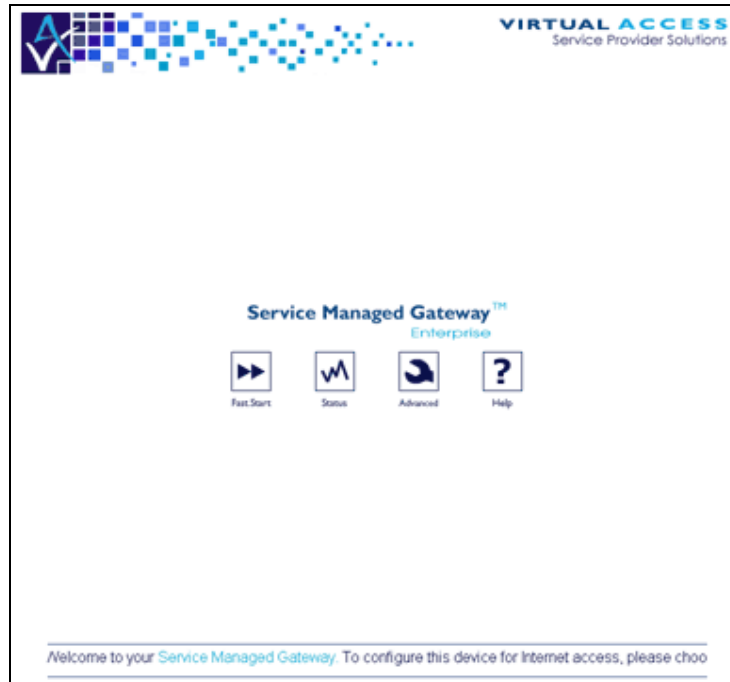


Figure 1: The SMG start page

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 the HTTP client on the SMG

The HTTP client is primarily intended to be used to receive updates from Activator. You can also use the client to push events up to Activator over HTTP or HTTPS.

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

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

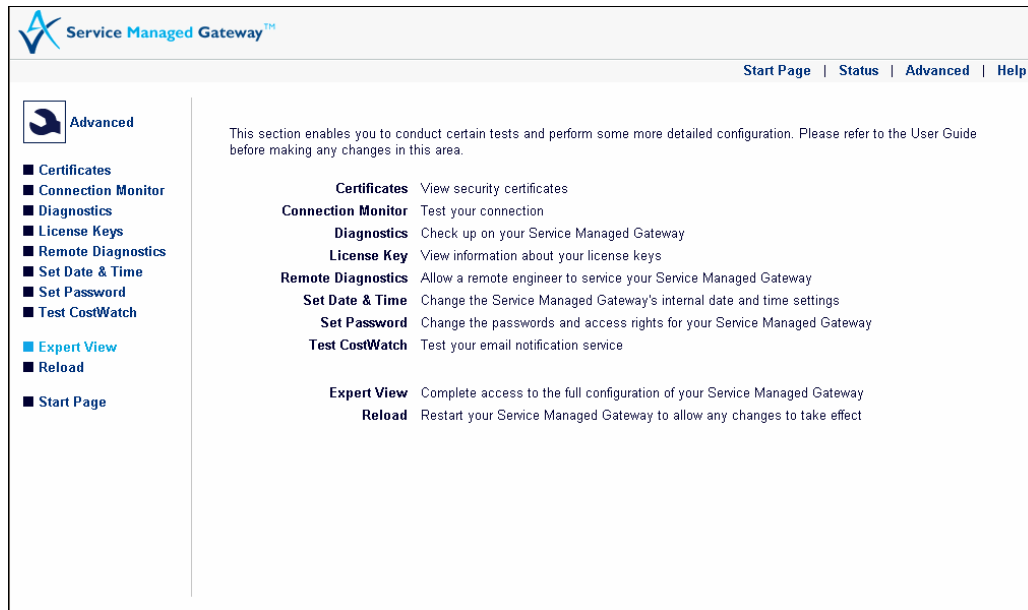


Figure 2: The advanced menu showing expert view

In the Expert View menu, select **System -> local clients -> http client**. The Http Client page appears. To view advanced options, click **Advanced**.

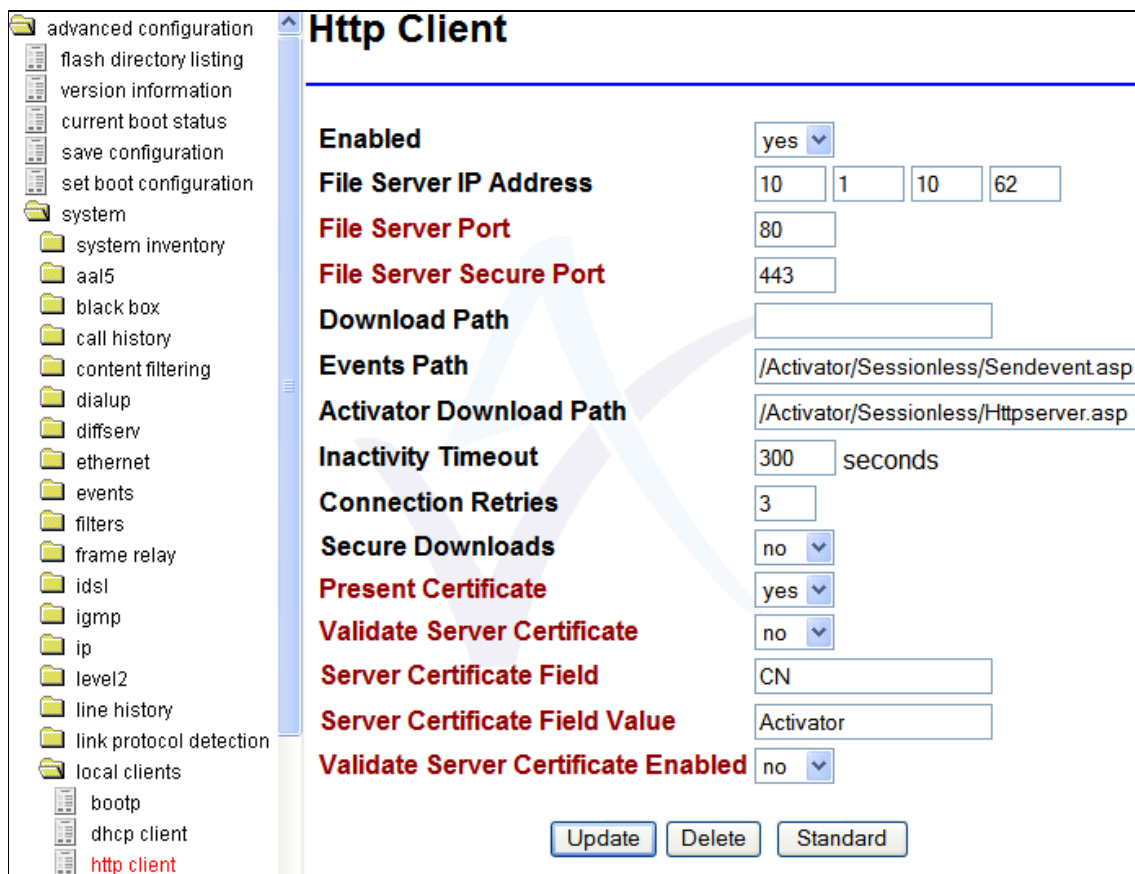


Figure 3: The advanced HTTP client page

Field	Description	Command Line
<b>Enabled</b>	Enables or disables the HTTP client.	Set HTTP Client Enabled =
	<b>yes</b> Enables the HTTP client.	
	<b>no</b> Disables the HTTP client.	
<b>File Server IP Address</b>	The file server IP address is the address of the web server, usually an Activator, from which the client will retrieve files and to which it will send events. Format: a.b.c.d	Set HTTP Client File Server IP Address =
<b>Download Path</b>	This option allows you to use a download path from an alternative server.	Set HTTP Client Download Path =
	Enter the name of the download path in HDL. This name is prepended to your specified filename.	
	Leave this field blank if the filename contains \$\$, or begins with a /. \$\$ denotes a special Activator request.	
	<b>Minimum value</b> 0	
	<b>Default value</b> Unspecified	
<b>Events Path</b>	Specify the full URL to which events are to be sent, such as <i>/Activator/Sessionless/Sendevent.asp</i> .	Set HTTP Client Events Path =
	<b>Minimum value</b> 0	
	<b>Default value</b> /Activator/Sessionless/Sendevent.asp	
	<b>Maximum value</b> 32	
	<b>Units</b> Unspecified	
<b>Activator Download Path</b>	Specify the full URL to which Activator download requests are to be issued, such as <i>/Activator/Sessionless/Httpserver.asp</i> .	Set HTTP Client Activator Download Path =
	<b>Minimum value</b> 0	
	<b>Default value</b> /Activator/Sessionless/Httpserver.asp	
	<b>Maximum value</b> 63	
	<b>Units</b> Unspecified	
<b>Inactivity Timeout</b>	Specify the number of seconds after which an idle connection will time out.	Set HTTP Client Inactivity Timeout =
	<b>Minimum value</b> 1	
	<b>Default value</b> 300	
	<b>Maximum value</b> 3600	
	<b>Units</b> Seconds	
<b>Connection Retries</b>	Select the number of times to retry the connection before considering the connection failed. Retries will be attempted after a timeout.	Set HTTP Client Connection Retries =
	<b>Minimum value</b> 1	
	<b>Default value</b> 3	
	<b>Maximum value</b> 20	
	<b>Units</b> Unspecified	
<b>Secure Downloads</b>	Specifies whether downloads will be performed over HTTP or HTTPS.	Set HTTP Client Secure Downloads

	<table border="1"> <tr> <td><b>Yes</b></td> <td>Downloads over HTTPS</td> </tr> <tr> <td><b>No</b></td> <td>Downloads over HTTP</td> </tr> </table>	<b>Yes</b>	Downloads over HTTPS	<b>No</b>	Downloads over HTTP		=				
<b>Yes</b>	Downloads over HTTPS										
<b>No</b>	Downloads over HTTP										
<b>File Server Port</b>	<p>Defines the port number of the web server. The default value is 80.</p> <table border="1"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>80</td> </tr> <tr> <td><b>Maximum value</b></td> <td>1024</td> </tr> <tr> <td><b>Units</b></td> <td>Unspecified</td> </tr> </table>	<b>Minimum value</b>	0	<b>Default value</b>	80	<b>Maximum value</b>	1024	<b>Units</b>	Unspecified		Set HTTP Client File Server Port =
<b>Minimum value</b>	0										
<b>Default value</b>	80										
<b>Maximum value</b>	1024										
<b>Units</b>	Unspecified										
<b>File Server Secure Port</b>	<p>Defines the port number of the secure server. The default value is 443.</p> <table border="1"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>443</td> </tr> <tr> <td><b>Maximum value</b></td> <td>1024</td> </tr> <tr> <td><b>Units</b></td> <td>Unspecified</td> </tr> </table>	<b>Minimum value</b>	0	<b>Default value</b>	443	<b>Maximum value</b>	1024	<b>Units</b>	Unspecified		Set HTTP Client File Server Secure Port =
<b>Minimum value</b>	0										
<b>Default value</b>	443										
<b>Maximum value</b>	1024										
<b>Units</b>	Unspecified										
<b>Present Certificate</b>	<p>Determines whether or not the router presents a client certificate to the server.</p> <table border="1"> <tr> <td><b>Yes</b></td> <td>Presents a client certificate.</td> </tr> <tr> <td><b>No</b></td> <td>Does not present a client certificate.</td> </tr> </table>	<b>Yes</b>	Presents a client certificate.	<b>No</b>	Does not present a client certificate.		Set HTTP Client Present Certificate Enabled =				
<b>Yes</b>	Presents a client certificate.										
<b>No</b>	Does not present a client certificate.										
<b>Validate Server Certificate</b>	<p>Determines whether or not the router validates the certificate held by the server.</p> <table border="1"> <tr> <td><b>Yes</b></td> <td>Enables server certificate validation.</td> </tr> <tr> <td><b>No</b></td> <td>Does not enable server certificate validation.</td> </tr> </table>	<b>Yes</b>	Enables server certificate validation.	<b>No</b>	Does not enable server certificate validation.		Set HTTP Client Validate Server Certificate Enabled =				
<b>Yes</b>	Enables server certificate validation.										
<b>No</b>	Does not enable server certificate validation.										
<b>Server Certificate Field</b>	<p>Sets the field to be compared for authentication when Validate Server Certificate Field Enabled is turned on.</p> <table border="1"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>CN</td> </tr> <tr> <td><b>Maximum value</b></td> <td>30</td> </tr> <tr> <td><b>Units</b></td> <td>Unspecified</td> </tr> </table>	<b>Minimum value</b>	0	<b>Default value</b>	CN	<b>Maximum value</b>	30	<b>Units</b>	Unspecified		Set HTTP Client Server Certificate Field =
<b>Minimum value</b>	0										
<b>Default value</b>	CN										
<b>Maximum value</b>	30										
<b>Units</b>	Unspecified										
<b>Server Certificate Field Value</b>	<p>Sets the value in the field that is compared when the Validate Server Certificate Field is enabled.</p> <table border="1"> <tr> <td><b>Minimum value</b></td> <td>0</td> </tr> <tr> <td><b>Default value</b></td> <td>Activator</td> </tr> <tr> <td><b>Maximum value</b></td> <td>30</td> </tr> <tr> <td><b>Units</b></td> <td>Unspecified</td> </tr> </table>	<b>Minimum value</b>	0	<b>Default value</b>	Activator	<b>Maximum value</b>	30	<b>Units</b>	Unspecified		Set HTTP Client Server Certificate Field Value =
<b>Minimum value</b>	0										
<b>Default value</b>	Activator										
<b>Maximum value</b>	30										
<b>Units</b>	Unspecified										
<b>Validate Server Certificate Enabled</b>	<p>Determines whether an extra level of authentication is provided using server certificate field validation.</p> <table border="1"> <tr> <td><b>Yes</b></td> <td>Enables server certificate validation.</td> </tr> <tr> <td><b>No</b></td> <td>Does not enable server certificate validation.</td> </tr> </table>	<b>Yes</b>	Enables server certificate validation.	<b>No</b>	Does not enable server certificate validation.		Set HTTP Client Validate Server Certificate Field Enabled =				
<b>Yes</b>	Enables server certificate validation.										
<b>No</b>	Does not enable server certificate validation.										

Table 1: HTTP client fields and their descriptions

## 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.

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