



Service Managed Gateway™

How to Configure a Telnet Server on an SMG

Issue 1.0
Date 19 February 2009

1	About this document	3
1.1	Scope	3
1.2	Readership	3
1.3	More information.....	3
1.4	Terminology	3
2	Introduction	4
2.1	Setting up the telnet client.....	4
3	Configuring the SMG.....	6
3.1	Configuring the telnet server on the SMG.....	6
3.1.1	Configure the telnet server system	7
3.1.2	Advanced configuration settings for the telnet server	7
4	Diagnostics.....	10
4.1	Trace analyzer.....	10
4.2	Tracing using the command line.....	12
4.2.1	Command line syntax	12

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 (SMG) to act as a Telnet server.

1.1 Scope

This document explains how to:

- Configure a Telnet server on an SMG
- 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/>

For more information on CLI commands read the following guides: http://www.virtualaccess.com/smgdocs/ApConfigGuides/Using_the_CLI_to_Manage_SMG.pdf

http://www.virtualaccess.com/smgdocs/ApConfigGuides/SMG_Commands_for_CLI.pdf

1.4 Terminology

SMG	Service Managed Gateway
IP	Internet Protocol
URL	Uniform Resource Locator
CLI	Command Line Interface

2 Introduction

The Telnet server on the SMG allows you to control the router and issue configuration and diagnostic commands. You must use a remote Telnet client to create a session. The router's username and password is supplied via the client to start the Telnet session. When the session has commenced, all commands entered on the client will be executed on the SMG.

By default the Telnet server on the SMG is enabled. For detailed information on managing the SMG via the command line interface read the user guide, 'Using SMG commands for the CLI'.

2.1 Setting up the telnet client

Choose the Telnet client that will be used to connect to the SMG's Telnet server. Most operating systems will have a Telnet client pre-installed. Please refer to your operating systems guidelines for activating the Telnet client.

For **Microsoft Windows 98, 2000, ME, Server 2003 and XP**, type telnet <server ip address> in the Run dialog box and click **OK**.

NOTE: By default, Windows Vista operates with the Telnet client deactivated. You can activate the Telnet client using the Services window.

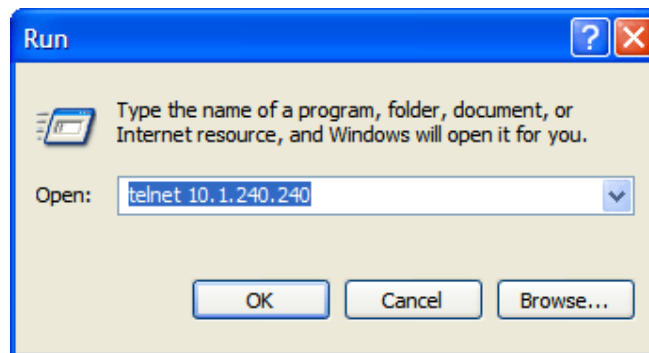


Figure 1: Create a telnet session

Ensure the Telnet client has IP connectivity with the SMG.

If the Telnet client is directly connected to the SMG, the IP addresses of both the client and the connected server interface, such as eth-0, should be on the same IP subnet.

The Telnet client requires the IP address of the server to establish a connection.

When the Telnet connection has been successfully established, you will be prompted for a username and password. Enter the default value **super**, unless you have configured the username and password to your own specification.

A successful login is greeted with information specific to the connected SMG.

```
Username : super
Password :
User login successful.

    Serial Number:
    Hardware Model:
    Provider:
    Customer:
    Boot Image:
    Boot Configuration:
    Current Time:

super>
```

Figure 2: The telnet login screen

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 3: 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 telnet server on the SMG

To configure the Telnet Server, click **Advanced** on the SMG start page. The Advanced menu appears.

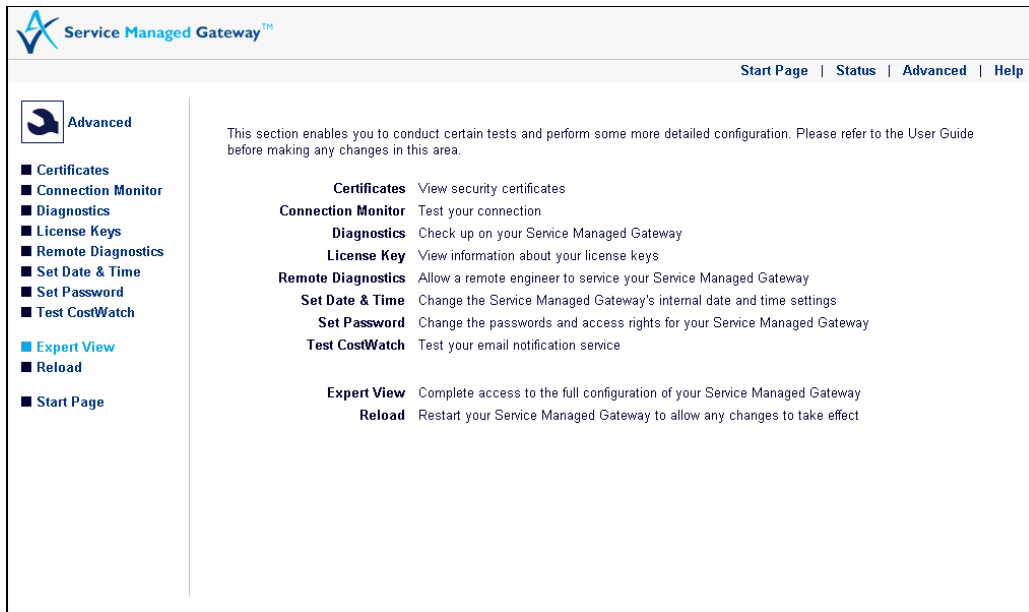


Figure 5: The advanced menu showing the expert view

In the Advanced menu, click **Expert View**. The Expert View menu appears.

3.1.1 Configure the telnet server system

In the Expert View menu, select **system -> local servers -> telnet server**. The Telnet Server page appears.

3.1.2 Advanced configuration settings for the telnet server

To view the advanced configuration settings, click **Advanced** on the Telnet Server page. The options available are described in Table 2.

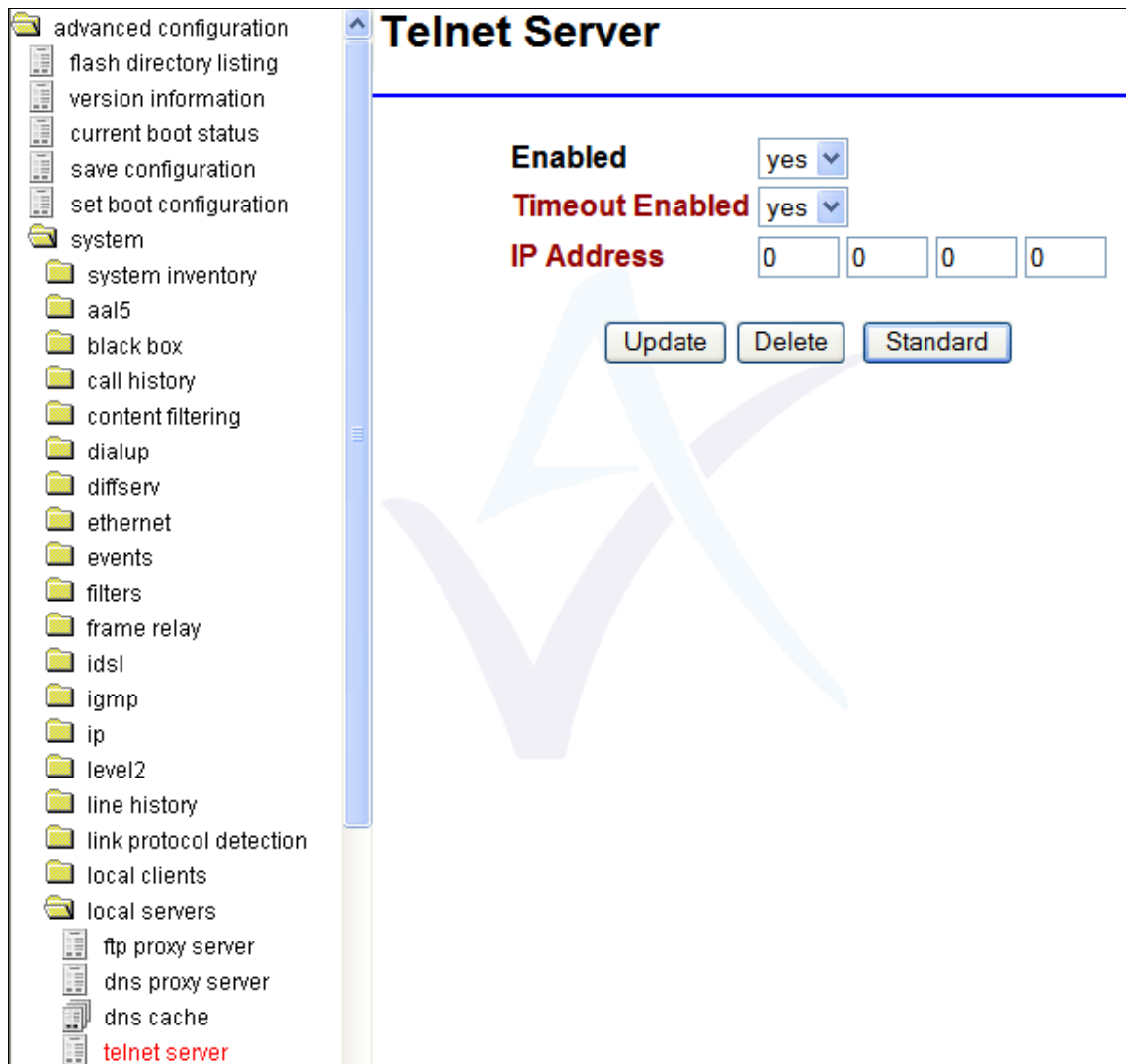


Figure 7: The advanced telnet server page

Field	Description	Command Line		
Enabled	Enables or disables access to the selected device via Telnet.	Set Telnet Server Enabled = yes		
	<table border="1"> <tr> <td>yes</td> <td>Allows you to connect to Telnet via the local console. This is the default setting.</td> </tr> <tr> <td>no</td> <td>Denies Telnet access.</td> </tr> </table>		yes	Allows you to connect to Telnet via the local console. This is the default setting.
yes	Allows you to connect to Telnet via the local console. This is the default setting.			
no	Denies Telnet access.			
Timeout Enabled	Specifies whether the device uses an inactivity timer to monitor Telnet sessions. When the inactivity timer expires, the Telnet session exits.	Set Telnet Server Timeout Enabled = yes		
	<table border="1"> <tr> <td>yes</td> <td>Enables the activity timer for Telnet (default).</td> </tr> <tr> <td>no</td> <td>Disables the activity timer for Telnet.</td> </tr> </table>		yes	Enables the activity timer for Telnet (default).
yes	Enables the activity timer for Telnet (default).			
no	Disables the activity timer for Telnet.			
IP Address	Specifies the IP address of the Telnet server. The IP address must be an IP address assigned to a router interface. When the IP address is set to 0.0.0.0, the Telnet server IP	Set Telnet Server IP Address = <IP address>		

	address is the Ethernet interface (eth-0). This field may be set to an IP address with format: A.B.C.D	
--	--	--

Table 2: Advanced telnet server system fields and their descriptions

4 Diagnostics

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.

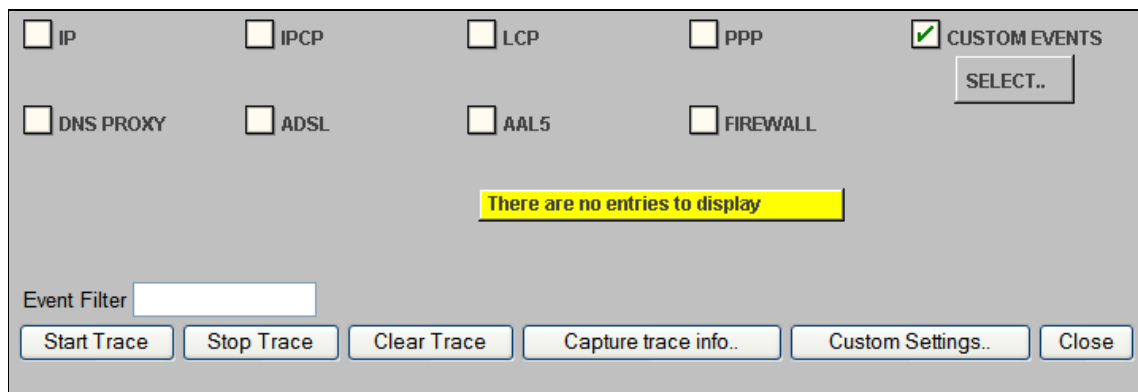


Figure 4: The trace analyzer window

To view the Telnet server traces check **Custom Events** and then click **Select**. The Select Events to trace pop-up window appears.

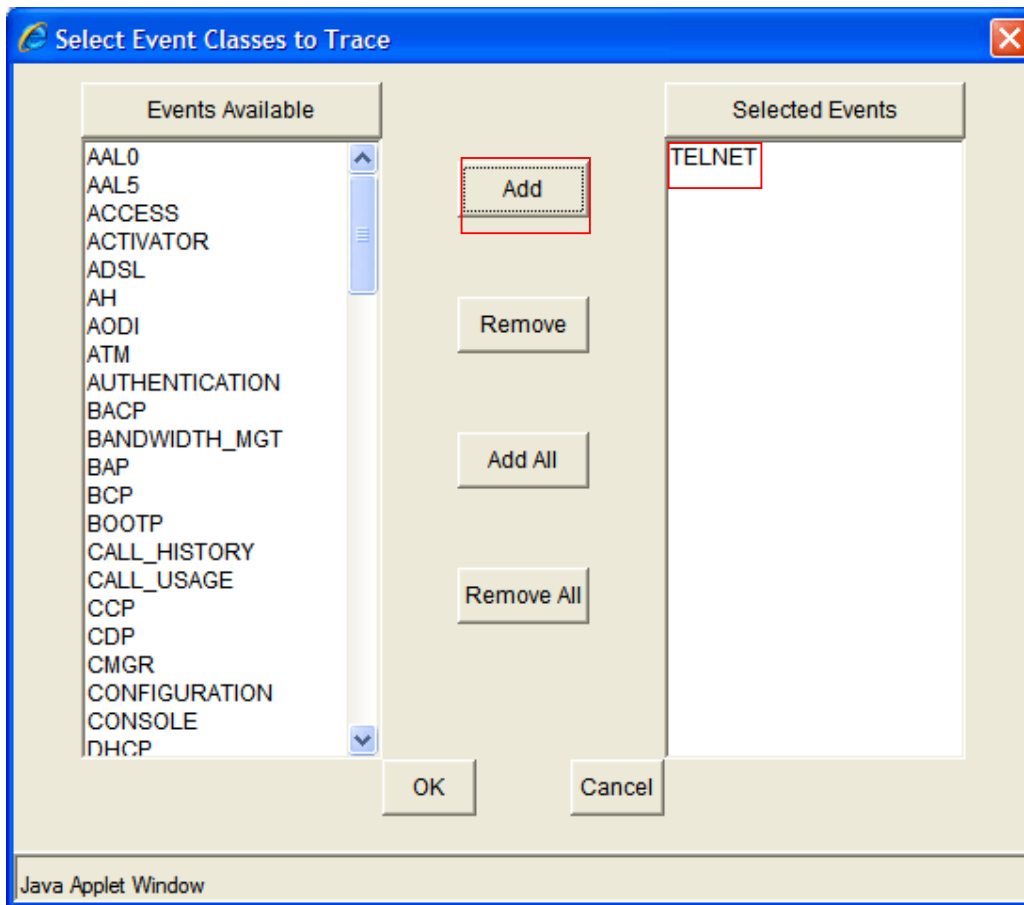


Figure 8: The select event classes to trace pop-up window

In the Events Available window, scroll to the bottom of the list and select **TELNET**.

Click **ADD**. TELNET appears in the Selected Events window.

When you have added the events, the Trace Analyzer will capture Telnet events.

Click **OK** to close the Select Event Classes to trace pop-up window.

In the Trace Analyzer window, click **Start Trace**. The Trace analyzer displays all Telnet events that have occurred since the trace started.

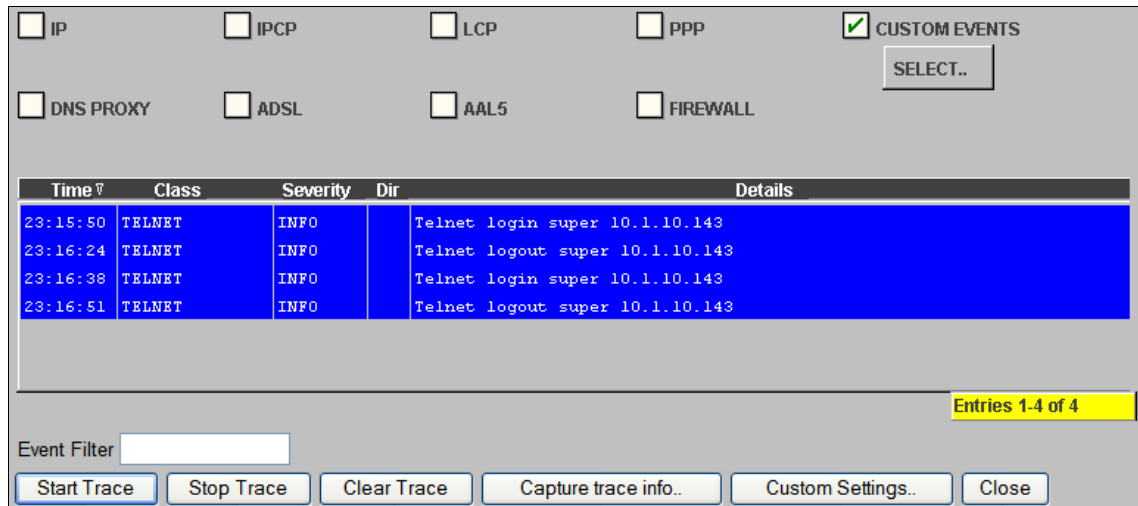


Figure 9: Captured telnet events in the trace analyzer window

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 via the command line is more flexible than using the trace analyzer 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 the 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.

Syntax	Description
++telnet	Starts tracing telnet events
-telnet	Stops telnet tracing

Table 3: The command line tracing syntax and their descriptions