![Hypermedia logo]

Hypermedia HG-7000 Product Manual

3U and 6U SMS Pro Gateways

Hypermedia Systems Ltd.

2b, Professor Bergman St., Rabin Science Park, Rehovot,

7670504, Israel

Telephone: (+972)-77-4445050

Fax: (+972)-8-936-3066

For general inquiries: info@hyperms.com

For sales inquiries: sales@hyperms.com

For Technical Support: support@hyperms.com Web

site: http://www.hyperms.com/

Hypermedia Systems Ltd.

Hypermedia Systems Ltd. LICENSE AGREEMENT AND WARRANTY

IMPORTANT — READ CAREFULLY

This Hypermedia Systems Ltd. License Agreement (the "AGREEMENT") is a legal agreement between you (either an individual or a single entity) and Hypermedia Systems Ltd. for the product accompanying this AGREEMENT. The product includes computer software, associated media and printed materials, and may include "online" or electronic documentation (the "SOFTWARE"). The PRODUCT may also include hardware (the —HARDWAREǁ). The SOFTWARE and the HARDWARE are referred to, collectively, as the PRODUCT.

BY INSTALLING AND/OR USING THE PRODUCT YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY ERASE ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION, AND RETURN THE SOFTWARE AND ANY ACCOMPANYING HARDWARE TO THE PLACE FROM WHICH YOU OBTAINED IT.

COPYRIGHT

All title and copyrights in and to the PRODUCT are owned by Hypermedia Systems Ltd. The PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

GRANT OF LICENSE FOR THE SOFTWARE

The SOFTWARE is licensed, not sold. Hypermedia Systems Ltd. grants to you a non-exclusive, non-transferable, royalty-free right to install and use the SOFTWARE, provided that the SOFTWARE will be used by a single person on a single computer and for personal non-commercial, internal use only. If accompanied by a proof-ofpurchase document specifying "site license," "company license," or any other multiple-user type license scheme, then the terms of that document shall override this single-user restriction. Any rights not expressly granted herein are retained by Hypermedia Systems Ltd.

OTHER RESTRICTIONS

This AGREEMENT is your proof of license to exercise the rights granted herein and must be retained by you. You may not rent, lease, reverse engineer, decompile, modify, or disassemble the PRODUCT, or create derivative works based on the PRODUCT.

LIMITED HARDWARE WARRANTY

The HARDWARE is protected against defects in material and workmanship, under normal use, for one (1) year from the original purchase date.

If the HARDWARE fails to perform within the abovementioned warranty period, you must return the PRODUCT to Hypermedia Systems Ltd. and prepay any shipping charges, export taxes, custom duties and taxes, or any charges associated with transportation of the Product. In addition, you are responsible for insuring the PRODUCT shipped or returned and assume the risk of loss during shipment.

All returned PRODUCTS must be accompanied by a description of the problem, a proof of the place and date of purchase, and the original shipping and packing materials.

Hypermedia Systems Ltd. shall, at its sole discretion, either repair the PRODUCT or replace it with a product of the same functionally. Replacement products may be refurbished or contain refurbished materials. If Hypermedia Systems Ltd. cannot repair or replace the PRODUCT, Hypermedia Systems Ltd. will refund the depreciated purchase price of the PRODUCT.

This limited warranty does not apply to any PRODUCT not purchased from Hypermedia Systems Ltd., or from a Hypermedia Systems Ltd. authorized reseller, or on which the serial number has been removed or defaced. This limited warranty also does not cover any PRODUCT that has been damaged or rendered defective as a result of

(a) improper transportation or packing when returning the PRODUCT to Hypermedia Systems Ltd.; (b) use of the PRODUCT other than in accordance with its instructions, or other misuse or abuse of the PRODUCT; (c) modification of the PRODUCT; (d) service by anyone other than a Hypermedia Systems Ltd.-approved agent; (e) unusual physical or electrical stress or interference, failure or fluctuation of electrical power, lightning, static electricity, improper temperature or humidity, fire, or acts of God.

The maximum liability of Hypermedia Systems Ltd. under this limited warranty is limited to the purchase price of the PRODUCT covered by the warranty.

Hypermedia Systems Ltd. reserves the right to refuse PRODUCTS (i) that are not covered by the warranty; or (ii) for which there is no problem found. Such PRODUCTS shall be returned to the purchaser at purchaser's expense.

DISCLAIMER

EXCEPT AS EXPRESSLY STATED ABOVE OR AS REQUIRED BY LAW, Hypermedia Systems Ltd. DISCLAIMS ANY WARRANTY FOR THE PRODUCT. THE PRODUCT IS PROVIDED "AS IS" WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. Hypermedia Systems Ltd. ASSUMES NO RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE PRODUCT.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES

IN NO EVENT SHALL Hypermedia Systems Ltd., ITS AGENTS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL OR INCIDENTAL DAMAGES; DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING DIRECTLY OR INDIRECTLY OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF Hypermedia Systems Ltd. HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Because some states or jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

U.S. GOVERNMENT RESTRICTED RIGHTS

For purchases made in the United States: The SOFTWARE and any accompanying documentation are provided with restricted rights. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (b) (3) and (c) (1) (ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable.

AMENDMENTS

Hypermedia Systems Ltd. may amend these terms and conditions at any time by posting a notice on one or more of its websites. Your continued use of the PRODUCT shall constitute your acceptance of such amended terms. Accordingly, we urge you to visit our websites periodically to review the current and effective terms and conditions for use of our products. Certain provisions of these terms and conditions may be superseded by expressly designated legal notices or terms outlined on our websites.

GOVERNING LAW

This AGREEMENT and any and all claims relating to the PRODUCT shall be governed by the laws of the State of Israel, without regard to or application of choice of law or principles, and the courts of Tel-Aviv Jaffa shall have sole and exclusive jurisdiction over any dispute arising in connection with this Agreement and/or the use of the PRODUCT.

NO WAIVER

No delay or failure to take action under these terms and conditions will constitute a waiver by Hypermedia Systems Ltd. unless expressly waived in writing by a duly authorized officer of Hypermedia Systems Ltd.

Table of Contents

This page is intentionally blank

Before You Begin

Conventions

The following symbols have been inserted on the left hand side of the operating instructions in order to make it easier for the User to perform procedures:

Symbol	Description
➡	**Note:** Information given in a note describes how the System functions or provides a tip on how best to use it.
⚠	**Caution:** Information given in a message labeled —caution‖ refers to the safe operation of the System and provides warnings where the possibility for loss of data or damage to the equipment exists.
✋	**Danger:** Information given in a message labeled —danger‖ warns of possible hazard to personnel and extreme hazard to the System.

Notice

Information given in this document is subject to change without any notice.

1 Hardware and Installation

➡ **Note:** Hardware and installation vary depending upon the features included with the Hypermedia Gateway system. Skip the sections that do not apply to your system.

This section contains:

- Package Contents (section 1.1.1   )
- Safety Information (section 1.2   )
- System Components (section 1.3   )
- Typical Board Configurations (see 1.4   )
- Pre-Installation Preparations (section 1.5   )
- Cable Connections (section 1.6   )
- Inserting the SIM Cards (section 1.7   )

Hardware and Installation

- Powering Up and LEDs Status (section 1.8   )

1.1 Overview

Hypermedia Gateways provide integrated voice and SMS communications for both on-site and remote users of small-to-large enterprises.

The Hypermedia HG-7000 SMS Pro Gateway is part of the HyperGateway family of flexible, scalable platforms which empower cost-effective corporate telephony over fixed, cellular and IP networks.

The HG-7000 Pro SMS gateway enables sending text-messages via SMS, two-way SMS texting, SMS to email, PC to SMS, and reception of text messages via SMS. It is supplied with a built-in SMS server software package and easy-to-use client API tools, which enable third-party applications to send and receive SMS messages. Additional applications are also available.

1.1.1 Package Contents

Depending upon configuration, the package should contain some or all of the following:

- The Hypermedia Gateway unit
- Ethernet cables
- 1 or 2 power cords, depending upon the configuration
- 1 to 8 indoor antennas, depending upon the configuration
- Hypermedia Software CD-ROM
- The warranty certificate
- 1 SD card (standard gateway)

1.2 Safety Information

Hypermedia Gateway works with a nominal mains supply voltage of 110–240V AC. Hazardous voltages are present inside of this equipment. Some of the parts can also have high operating temperatures.

To avoid injury and prevent equipment damage, observe the following safety precautions:

- Installation, service, and maintenance of the Hypermedia Gateway should be done by qualified technicians only.
- Do not connect the Hypermedia Gateway to any power source other than the indicated nominal source.
- The power supply cord must be connected to a socket with a valid ground. This equipment should only be used in buildings with proper safety ground.

- When connecting the equipment, first, ensure that the ground connection is connected to the rack ground or building ground.

- When disconnecting the equipment, disconnect the ground connection last.

- Opening the housing may be dangerous and invalidates the warranty. Only a qualified technician should open the housing. Before opening, disconnect the power cable from the equipment.

- The Hypermedia Gateway complies with all necessary safety standards. Equipment connected to the Hypermedia Gateway must also comply with the applicable safety standards.

- The packaging is designed to protect against mechanical damage and should be stored. Do not ship equipment unless it is properly packed in its original wrapping and shipping containers.

- Make sure that the equipment top and bottom are not blocked to air movement. Leave 1U under and on top of the equipment for proper ventilation.

- Do not operate the Hypermedia Gateway in close proximity to potentially hazardous areas. These includes areas such as, but not exclusively, fuel stations, fuel depots, chemical works or during blasting.

- The operation of radio transmitters, which includes cellular engines, can impair the function of medical devices that have not been properly shielded. Please ask the advice of your doctor or the manufacturer of the medical device.

- To avoid moisture condensation, allow time for the unit to adapt to the ambient temperature before switching it on.

1.3 System Components

The Hypermedia Gateway unit is a 19" × 6U or 19" × 3U rack-mountable box that connects to the local network. The HG-7000 Gateway comes in two main series.

Standard: designed for the enterprise user; based on an embedded CPU.

Heavy-Duty: designed for high volumes of SMSs; based on a PC board.

The Hypermedia system contains the following:

- A single **power supply** module. A dual power supply module is also available.

- A **backplane** with slots for the boards. The position of the boards varies according to the product series.

- The **Hypermedia Server**, which is an application that is embedded on the HBN or on the PC1/2 board (depending upon system configuration). The

Hypermedia Server is controlled and managed by the browser-based Hypermedia Management Console.

- The **Hypermedia Management Console** (HMC), which is used by the system administrator for remote configuration and monitoring of the Hypermedia Gateway system. It connects to the gateway using TCP/IP and is accessed via a standard WEB browser.

1.4 Typical Board Configurations

The placement of the HG-7000 boards varies according to the product series. The names and function of the boards are described in the following table.

Table 1. HG-7000 Boards and Function

Board Name	Description
Standard Gateway Board	
HBN This	Hybrid board provides the gateway management function as well as the SMS server functionality.
Heavy-Duty Gateway Boards	
PC1/PC2	The PC board runs the HyperGateway server along with an MG 2.1 board.
MG 2.1	This board provides the media matrix functionality.
Cross-Gateway Boards	
CG41/CC41/CU41	CG41 for GSM, CC41 for CDMA and CU41 for UMTS is a single-slot board that contains four (4) cellular channels with inbound and outbound SMS capabilities for the various cellular networks.
S-HUB	This board provides SIM server connectivity.

1.4.1 3U Series

The following Figure 1 shows the 3U SMS Gateway supporting up to 12 ports with API

CG Boards

3U

HBN Board

Power Supply
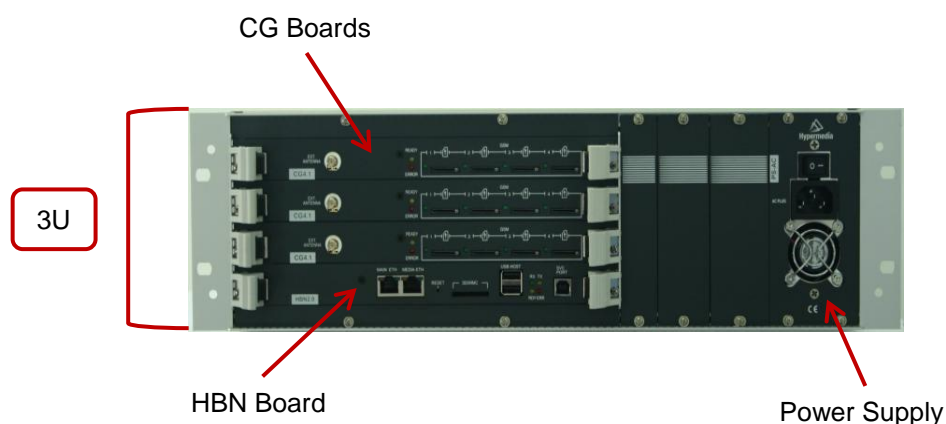
Figure 1. 3U SMS Gateway

1.4.2 6U Series

The following Figure 2 shows the 6U SMS Gateway, supporting up to 32 ports
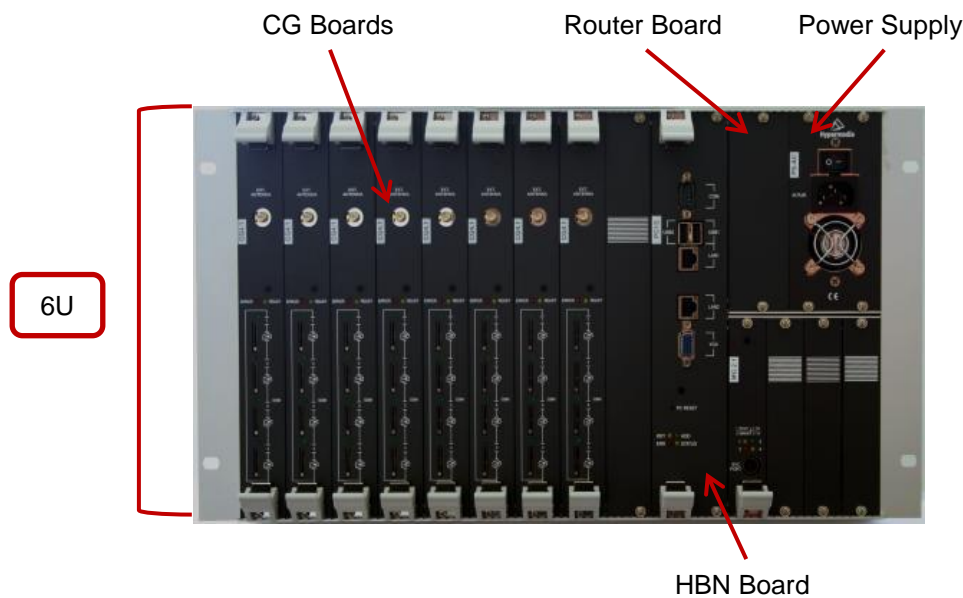
Figure 2. 6U SMS Gateway, 32 ports

1.5 Pre-Installation Preparations

➡ **Note:** The installation procedure depends on the boards included with the Hypermedia Gateway system. Skip the sections that do not apply to your system.

1. Install the Hypermedia Gateway in a 19‖ rack. Depending upon the physical configuration, the unit requires a height of either 3U or 6U. In addition, we recommend:

   ▪ Avoid installing the device near computer rooms, computer monitors, electrical cabinets, metal objects, and windows with fold aluminum sheet.

   ▪ Perform a cellular signal check before mounting the system. This can be done by checking the Signal Strength and the Bit Error Rate ratio on another mobile phone's display from the same operator and system.

   ▪ Ensure the device is protected against direct sunlight and heat. This increases both the reliability of the operation as well as its service life.

2. Depending upon the configuration of your system, verify that you have some or all of the following:

   ▪ an Ethernet or WAN socket with a fixed IP address

   ▪ SIM cards from your GSM operator. One SIM card is required for each GSM channel ➡ **Notes:**

      ◆ The default LAN IP address for Hybrid-Based Gateways is **192.168.9.2**
      ◆ The default LAN IP address for PC - Based Gateways is **192.168.0.2**

1.6 Cable Connections

There are two types of configurations:

- **Standard Gateway** – Hybrid based (HBN)
- **Heavy-Duty Gateway** – PC Based

1.6.1 Standard Gateway - Hybrid Based (HBN)

Figure 3. HG7000 - HBN Connection Settings

1.6.2 Heavy-Duty Gateway – PC Based

Figure 4. HG-7000 – PC Connection Settings

➡ **Note:** The cables to the devices should be installed so that they do not cause any physical risk. Power cables should be installed separate from the signal cables.

1.7 Inserting the SIM Cards

1. Insert the GSM SIM Cards. One SIM card should be used per each cellular channel.

   The SIM port is spring loaded. Slide the SIM card into the slot and it will latch in place. To remove a SIM card, press the SIM card and it will pop out.
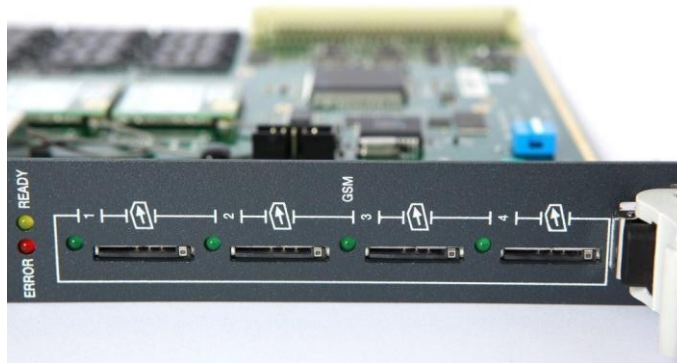
Optionally, use the CG board's multi-SIM extender: a. Pull out the CG board.
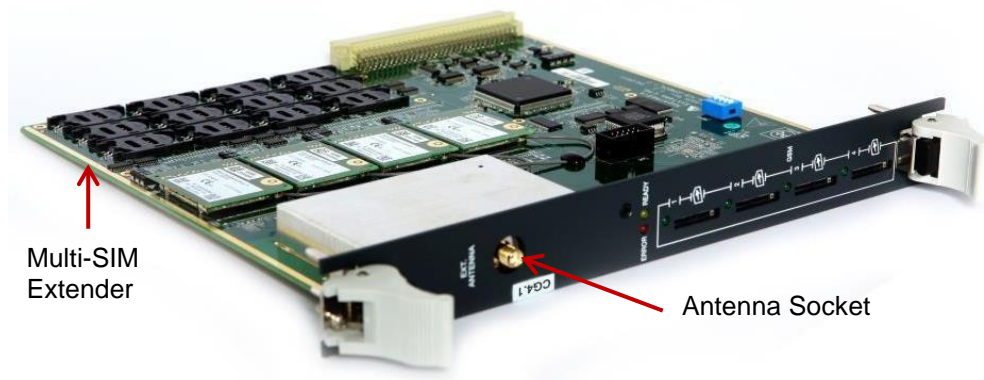
Figure 5. CG Card with 12 Multi-SIM Extender

b. Slide back and pull up the SIM socket.

⚠️ **Caution:** Do not use force on the SIM sockets.

   c.   Slide in the SIM cards.

   d.   Lock the SIM sockets.

➡️ **Note:** Some versions of the CG board have SIM drawers. Push the small yellow button for the SIM drawer to exit. Remove the SIM drawer, place the SIM card in the SIM drawer and replace the SIM drawer.

SIM Card

SIM Drawer

Yellow button for drawer
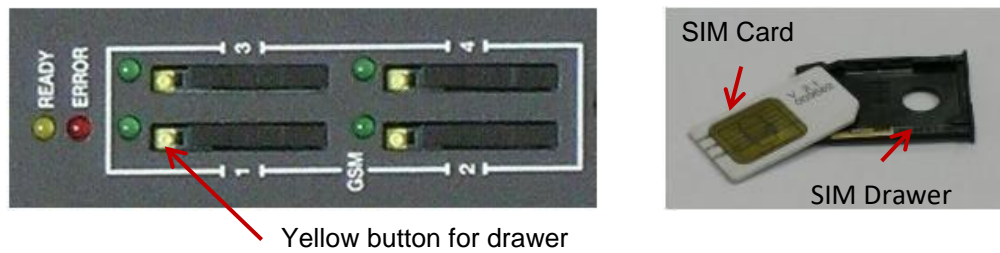
2. Install the antennas. Each cellular card requires one antenna.

⚠️ **Caution:** The provided antennas are for indoor use only, and will be irreversibly damaged if placed outdoors. RF combiners and external antennas are sold separately.

   a.   Locate the antenna socket (see Figure).

   b.   Fasten the antenna using the SMA connector. Do not use excess force.

   c.   Tether all cables securely. Tethering helps prevents breakage of connectors and damage to cellular cards.

   d.   Place the antenna indoors, where the reception level is high.

   e.   Optionally, to improve reception, place the magnetic back of the antenna on a metal plate larger than 20 × 20 cm.

1.7.1 Inserting the SD Card (Standard Gateway)

The Gateway saves Call Detail Records (CDRs) on a Secure Digital (SD) flash memory card that is supplied by Hypermedia. Insert the SD card into the SD port of the HBN card.

Figure 6. SD Card and Port

➡️ **Note:** CDRs are displaced on a FIFO basis.

1.8 Powering Up and LEDs Status

1.8.1 Powering Up

1. Turn on the unit. The power panel is located at the top right corner of the system.

Figure 7. Power Panel

➡ **Note:** Redundant power supplies are optional. When installed, if one fails, or if the system is powered up with just one power supply, an alarm will sound. To stop the alarm, press the Alarm Reset button at the top left of the panel.

2. Check the LEDs:

- For **HBN** LEDs, see Table 2
- For **PC Board** status LEDs, see Table 3
- For **MG Board** Status LEDs, see Table 4
- For **Cellular Card Green SIM** LEDs, see Table 5

1.8.2 LEDs Status

Following are explanations of LED behavior for each of the Hypermedia Gateway's cards.

Table 2. HBN LEDs

	State	Explanation
	Main ETH	
	Yellow	LAN Traffic
	Green	LAN Connection
	Media ETH	

	State	Explanation
	Yellow	LAN Traffic
	Green	LAN Connection
	Red LED - ERR	
	Blinking	Board Error
	Yellow LED - RDY	
	Off	Power is OFF
	Short Blink	Board Ready
	Fast Blink	Maintenance mode
	Green LED - RX	
	On	Internal Communication
	Yellow LED - TX	
	On	Internal Communication

Table 3. PC Board status LEDs

	State	Explanation
	LAN 1	
	Yellow	LAN Traffic
	Green	LAN Connection
	LAN 2	
	Yellow	LAN Traffic
	Green	LAN Connection
	Red LED - ERR	

	State	Explanation
	Blinking	Board Error
	Yellow LED - RDY	
	Off	Power is OFF
	Short Blink	Board Ready
	Fast Blink	Maintenance mode
	Green LED - HDD	
	On	Disk Activity
	Yellow LED - Status	
	On	Internal Communication

Table 4. MG 2.1 Board Status LEDs

	State	Explanation
	Red LED - ERR	
	Blinking	Board Error
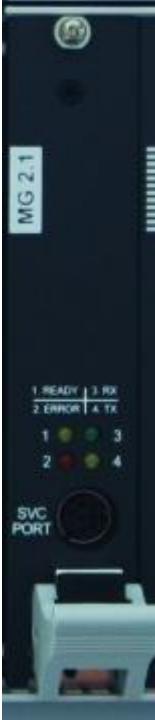
	Yellow LED - RDY	
	Off	Power is OFF
	Short Blink	Board Ready
	Fast Blink	Maintenance mode
	Green LED - RX	
	On	Internal Communication
	Yellow LD - TX	
	On	Internal Communication

Table 5. Cellular Card LEDs Status

	State	Explanation
	Red LED	
	On	Board Error
	Yellow LED	
	Short blink	Board Ready
	SIM Cards - Green LED	
	Flashing	A SIM card is not installed in this channel or the port is still being initialized.
	Off	No reception; the channel is not registered to a cellular network.

Short blinks (mostly Off)	Stand by; the channel is registered but no call is in progress.
Long blinks (mostly On)	User is either dialing out or receiving a call on this channel.
Steady On	In use. A call is in progress.

2 HMC Quick Start

Use the Hypermedia Management Console (HMC) to configure and monitor a Hypermedia Gateway from a remote location. Access to the Gateway is over TCP/IP using a standard version of Internet Explorer.

➡ **Note:** The Hypermedia Management Console is customized to match the specific order. According to the customization, some branches of the HMC may or may not appear. This section contains:

- Installation (section 2.1   )
- Setting the IP address (section 2.2)
- Start-up and Initial Connecting (section 2.3   )
- Save and Backup/Restore Configuration Settings (section 2.4)

2.1 Installation

To install the Hypermedia Management Console program:

1. Ensure that the computer matches the following minimum system requirements:

   ▪ Windows XP, Vista, Windows 7 or 8

   ▪ Internet Explorer 7 or above

2. Ensure that you have access to the installation file. It is included with the Hypermedia Gateway CD-ROM.
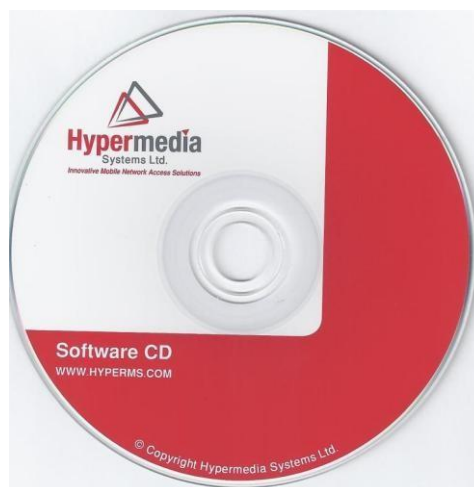
Figure 8. Hypermedia Gateway CD-ROM

The installation file name begins with the letter **HMC** and ends with the extension **.exe**. The specific name depends upon the type of installation.

3. Double-click the file **HMCxxx-xxx.exe** file. The Setup program starts.
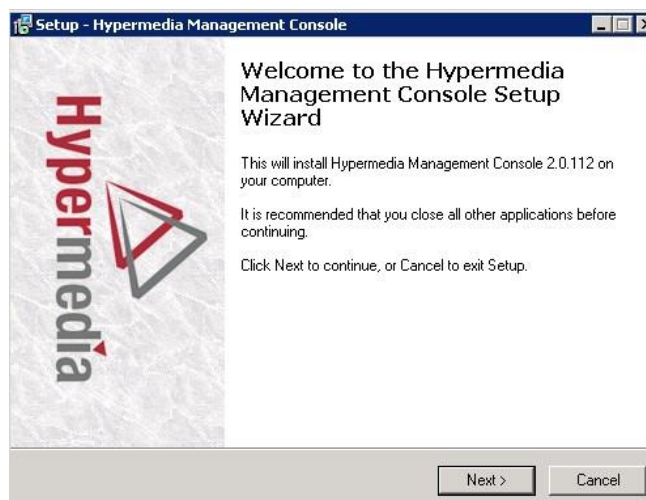
Figure 9. Setup Welcome Screen

4. Click **Next**. The License Agreement is displayed.

5. To continue, you must accept the terms of the agreement. Click **I accept the agreement** and click **Next**. The Select Destination Location window is displayed.

6. Define the location where the program files will be installed. The default location is "C:\ProgramFiles\Hypermedia". Click **Next**. The Select Start Menu Folder is displayed.

7. Define the name of the program group that will be added to the Start Menu. The default name is Hypermedia. Click **Next**. The Additional Tasks window is displayed.

8. Optionally, select the checkbox to create a Desktop shortcut. Click **Next**. The —Ready to Installǁ window is displayed.
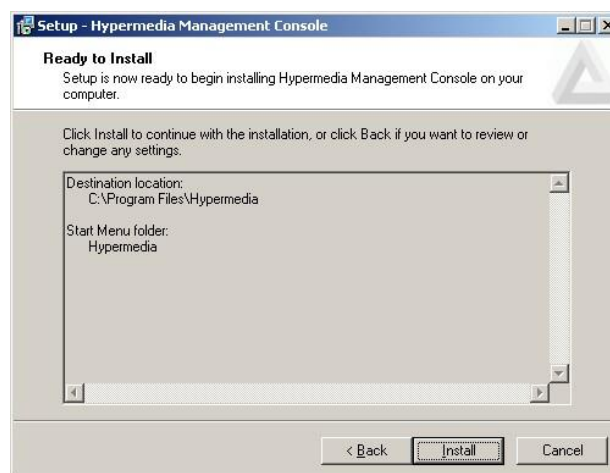
Figure 10. Setup Ready to Install Screen

9. Click **Install**. The installation process begins. A progress bar reports the progress of the installation.

   After the installation is complete, click **Finish**. The installation program creates a program group in the Start menu and, optionally, a Desktop shortcut
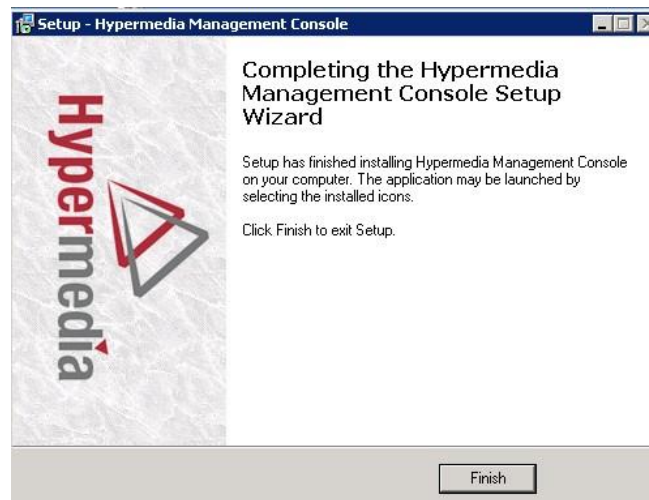
Figure 11. Setup Finish Screen

2.2 Setting the IP Address

To change or set the IP address:

1. From the Hypermedia program group, select **Server List**. The HyperGateway Servers Address List screen opens in the default browser.

2. If required, click the warning bar at the top of the screen and from the dropdown menu click **Allow Blocked Content**. Confirm your choice by clicking **Yes** on the confirmation message.

Figure 12. Hypermedia Gateway Server List

Note: To avoid recurring displays of the warning bar, browse from the Explorer menu bar to **Tools > Internet Options > Advanced** and select **Allow active content to run in files on My Computer**.

Your Gateway appears in the Server List with its default address.

3. Click ⚙ (Change Server Settings). The Login screen is displayed.

Figure 13. The Login Screen

4. Enter the password and click **Submit**. The default password is **admin**. The HGS Setup Parameters screen is displayed.
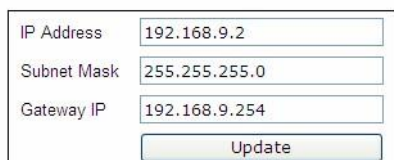
Figure 14. HGS Setup Parameters Screen

5. From the HGS Server system function line, click **Stop**. A confirmation message indicates that the service has stopped successfully.

6. On the IP Configuration line, click **Change**. The IP Address screen is displayed.

Figure 15. IP Address Screen

7. Enter the new IP Address parameters.

Note: Setting the IP address through this page will permanently affect the Gateway IP address settings once rebooted.

8. Click **Update**. Focus is returned to the HGS Setup Parameters Screen.

9. From the HGS Server line, click **Start**. A confirmation message indicates that the service started successfully.

2.3 Start-up and Initial Connecting

To run the Hypermedia Management Console:

1. Click the Windows **Start** button **> Programs > Hypermedia**. The Hypermedia program group expands.

2. Click **Hypermedia Management Console**. The program opens in the default browser.
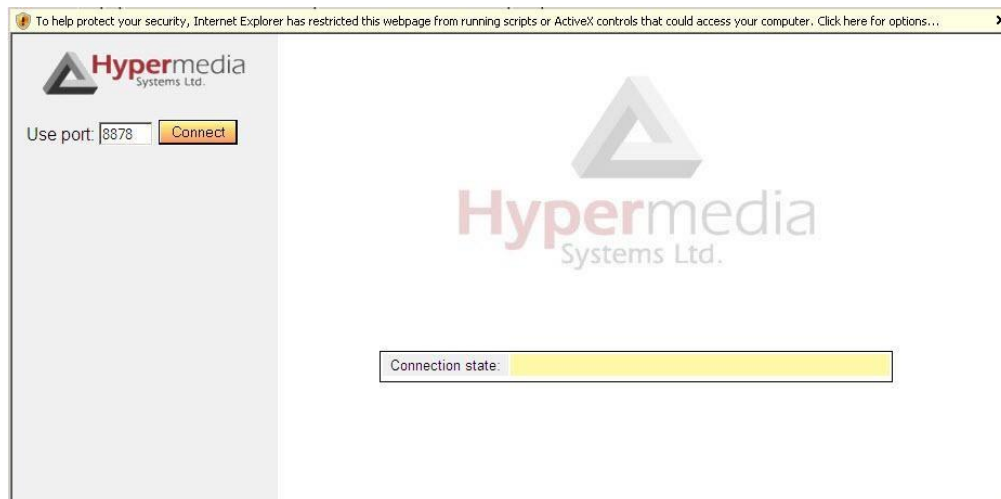
Figure 16. HMC Connection Screen

3. Click the warning bar at the top of the screen and, from the dropdown menu, click **Allow Blocked Content**. Confirm your choice by clicking **Yes** on the confirmation message.
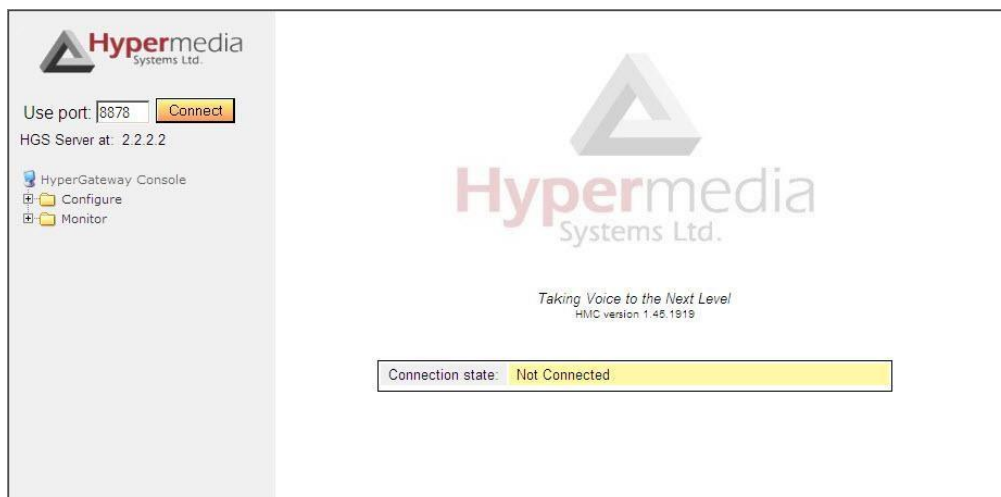
Figure 17. HMC Connection Screen

Note: To avoid recurring displays of the warning bar, browse from the Explorer menu bar to **Tools > Internet Options > Advanced** and select **Allow active content to run in files on My Computer**.
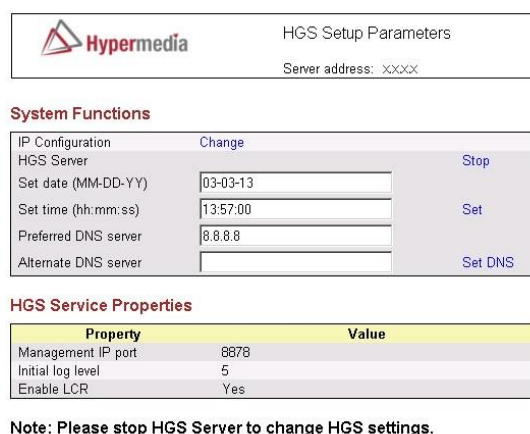
4. Enter the IP address:

a. Expand the **Configure** branch.

b. Expand the **Server Settings** branch.

c. Select **IP address**. The Server Address screen is displayed.

d. Enter the IP address and click **Apply Settings**
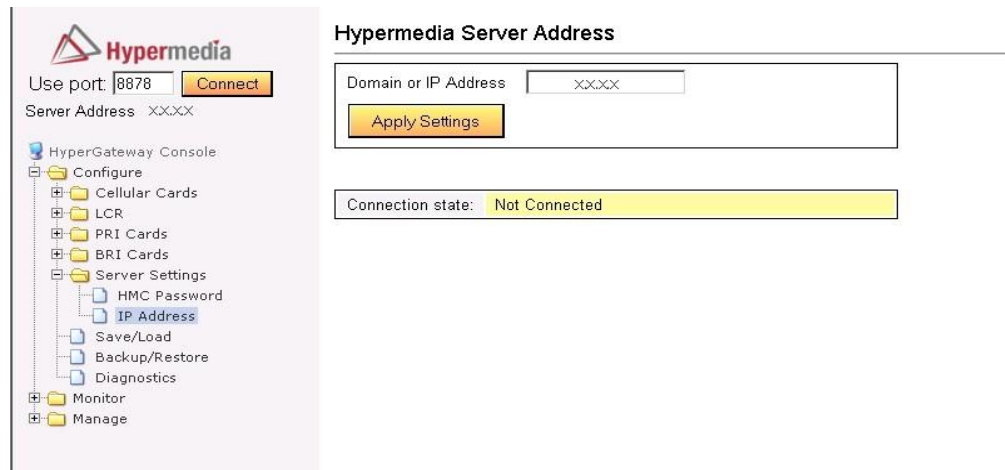
Figure 18. HMC Server Address Screen

➡ **Note:** If the Gateway is located behind a firewall, enable traffic on TCP ports 8878, 8879, 80 and 22. For details, contact the network administrator.

➡ **Note:** The above IP address setting does not affect the address of the Gateway. It only defines the IP address the HMC will attempt to connect to.

5. Either press **F5** or click the browser's **Refresh button**. The authorization screen is displayed.
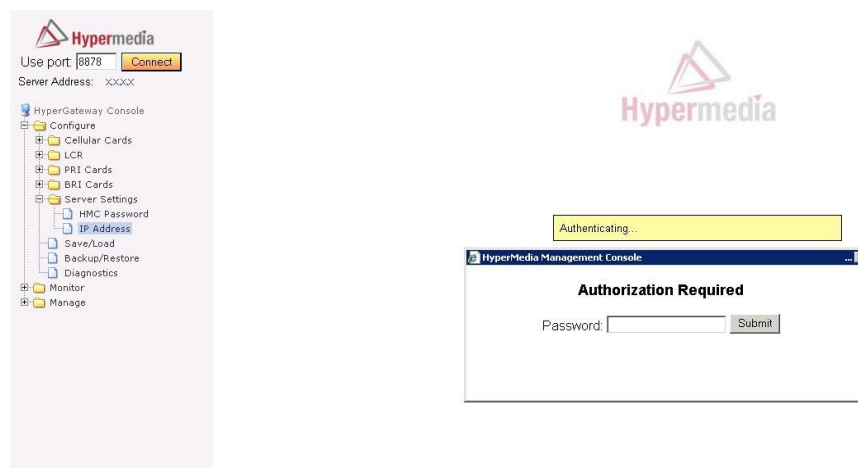
Figure 19. HMC Login Authorization Request

➡ **Note:** The default password is **admin**.

6. Enter the password and click **Submit**. A confirmation message is displayed, indicating you have successfully connected to the Hypermedia.

The Connection State screen is displayed.

HMC	2.0.137	
Model	HBS BP	
Media Card		
HGS	2.0.3747	ok
SGW	2.1.68	inactive
HyperConnect	2.0.28	inactive
HyperID	2.0.3747	inactive
NPS	2.0.96	inactive
SMSPro	2.1.244	inactive
WebSMS	1.1.217	inactive

Figure 20. HMC Connection State Display

A list of all services is displayed, including their versions and current activation/installation state.

2.4 Save and Backup/Restore Configuration Settings

2.4.1 Save All

Use the configuration branch to permanently save all the configuration settings in the HyperGateway

2.4.2 Store Settings on Cards

Use this option to permanently save all the configuration settings in the Hypermedia Gateway. This process might take up to 60 seconds.

Save All Settings

Store settings on cards
Permanently save all the configuration settings in the HyperGateway. This process might take up to 60 seconds.

[Save All Settings]

Figure 21. Save All Settings configuration branch

2.4.3 Backup/Restore

Use this option to download the entire configuration of the Gateway to your PC. The downloaded backup file can then be uploaded by performing a system restore.

Backup and Restore

Backup

Save current configuration to backup file   [Create Backup]

Last backup: Monday, February 25, 2013 11:28:11 PM   [Download Backup]

Restore

Never restored

Restore configuration from backup file
[_____ Browse...]   [Upload and Restore]

Backing up

Backing up LCR card at address LCR
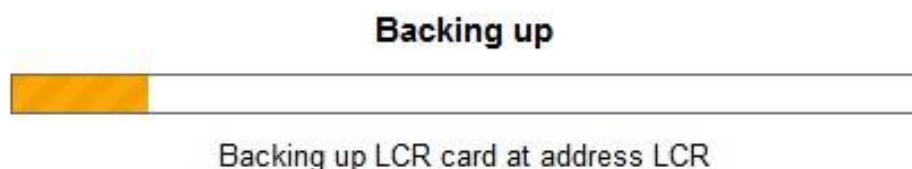
Figure 22. Backup and Restore

3 Configuring a Cellular Card

This section contains:

- Cellular Card and System Terminology (section 3.1   )
- Media Connections (section 3.2   )
- PIN Codes (section 3.3   )
- Reset (section 3.4   )
- Information Screens (section 3.5   )
- Locks (section 3.6   )
- SIM Select (section 3.7   )
- Cell Selection (section 3.8   )
- Settings (section 3.9   )
- Network Parameters (section 3.10   )
- USSD SIM Balance (section 3.11   )
- Monitoring Cellular Cards (section 3.12   )

3.1 Cellular Card and System Terminology

A cellular card has 4 modules, each of which can have 1 to 4 SIM holders. Therefore, each card can hold up to 16 SIM cards. The Hypermedia Gateway can include several cards.

The first SIM cards of each module are loaded into the spring-loaded SIM ports from the front of the Cellular Card.
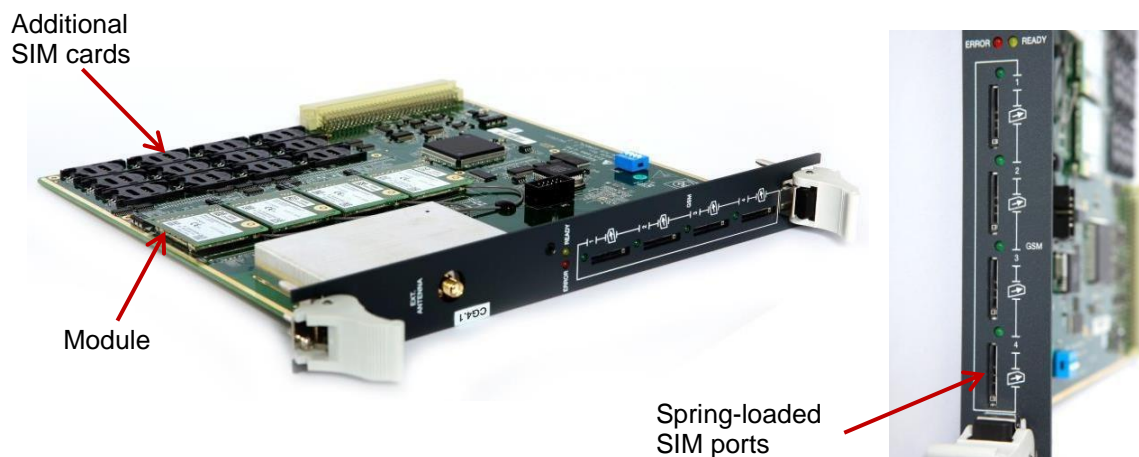
Figure23. Cellular Card SIM Ports and Holders

Some of the parameters can be applied to specific SIM cards, some to a specific module, some to the entire cellular card and some to all the cards in the system.

3.2 Media Connections

Use the Media Connection screen to configure the connections from the Cellular card channels to other cards and channels of the system, including the PRI cards (E.1) and the VoIP cards (MG). Connections can be either static or dynamic, as in the case of LCR.

For example, you can assign each cellular channel to a specific E1 channel. In this case, every time there is an incoming call from a specific E1 channel, it will be routed to the configured channel on the cellular card and vice versa.

Note: The matrix can be configured in any combination. Routing can be assigned between any cellular channel and any other channel in the system, including other cellular channels.

3.2.1 Associating/Linking Cellular Channels

To associate a cellular channel with another media channel:

1. From the Cellular Cards branch of the HMC navigation pane, , click the **Media Connections** sub-branch. The Media Matrix is displayed.

Cellular Cards Media Matrix

Select cellular card

| Slot | ◉ 3 |

Selected card at slot 3 (GSM)

Channel	Target Link (Select to change) | Unlink All
1	CG4.0(3) Channel 1
2	CG4.0(3) Channel 2
3	CG4.0(3) Channel 3
4	CG4.0(3) Channel 4

Figure 24. Cellular Media Matrix screen

2. If more than one slot is displayed, select a specific cellular card. The Media Matrix of that cellular card is displayed.

3. Click within a channel row. The row turns yellow.

4. Click **Edit**. The row becomes configurable.

Configuring a Cellular Card

Cellular Cards Media Matrix

Select cellular card

| Slot | ◉ 3 |

Selected card at slot 3 (GSM)

Channel	Target Link Edit | Unlink All
1	-
2	-
3	-
4	-

Cellular Cards Media Matrix

Select cellular card

| Slot | ◉ 3 |

Selected card at slot 3 (GSM)

| Channel	Target Link Save | Auto Link | Cancel
1	E1.0(12) ▾ Channel 1 ▾
2	-
3	-
4	-

Figure 25. Media Matrix Row when Configurable

5. From the first dropdown list, allocate the channel to a card by selecting the card.

Note: If all of the card's channels are already allocated, the message —Fully allocatedǁ appears.

6. From the second dropdown list, assign the channel to a specific channel on the target card.
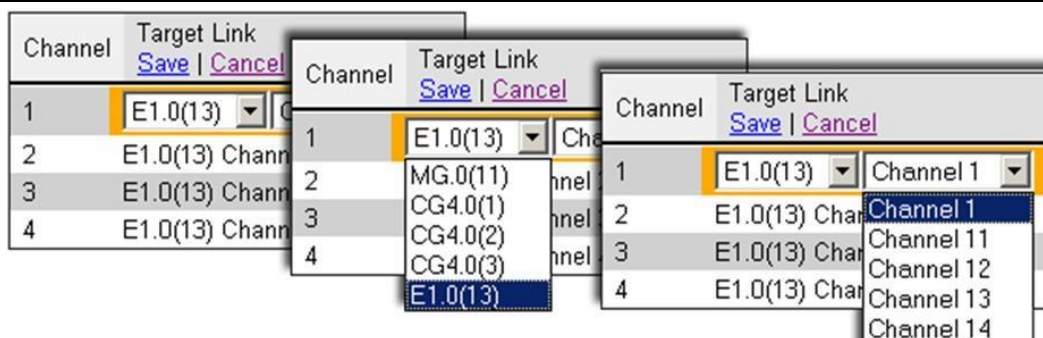
Figure 26. Assigning a Target Link

7. Click **Save**. The configuration dropdown boxes are hidden.

8. Optionally, repeat the process for additional channels and other media types.

9. Click **Apply Settings** and wait for —Configuration Saved‖ to be displayed.

3.2.2 Auto Linking

Enables associating all channels of one media card to another media card.

To create an auto-link:

1. From the Cellular Cards branch of the HMC navigation pane, click the **Media Connections** sub-branch. The Media Matrix is displayed.
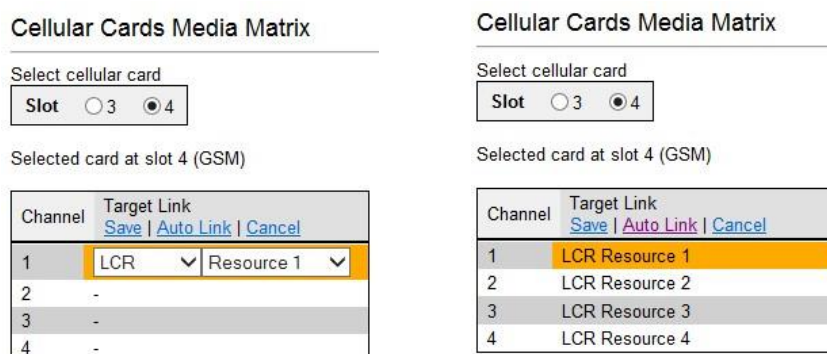
Figure 27. Auto Media connecting

2. If more than one slot is displayed, select a specific cellular card. The Media Matrix of that cellular card is displayed.

3. Click within a channel row. The row turns yellow.

4. Click **Auto Link**.

   All channels can be associated with one media card to another: card X channel 1 to card Y channel 1, card X channel 2 to card Y channel 2, etc.

3.2.3 Unlinking Cellular Allocations

To break an allocation:

5. From the HMC navigation pane Cellular Card branch, click the **Media Connections** sub-branch. The Media Matrix is displayed.

6. Click within a channel row. The row turns yellow.

Channel	Target Link Edit | Unlink | Unlink All
1	CG4.0(3) Channel 1
2	CG4.0(3) Channel 2
3	CG4.0(3) Channel 3
4	CG4.0(3) Channel 4

Figure 28. Breaking a Target Link

7. Click **Unlink**.

8. Click **Apply Settings** and wait for —Configuration Saved‖ to be displayed.

Configuring a Cellular Card

3.3 PIN Codes

Use the PIN Codes screen to configure the PIN code that the Gateway uses when a SIM card with an active PIN is inserted. For more information regarding the PIN code, consult your cellular provider.

To enter a SIM card's PIN code:

1. From the Cellular Cards branch of the HMC navigation pane, click the **PIN Codes** sub-branch. The PIN Codes screen is displayed.

Cellular Card PIN Codes

Select cellular card

Slot ⊙ 1 ○ 2

Selected card at slot 1 (GSM)

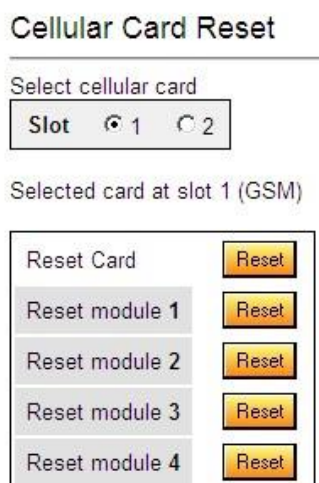| Module 1 | |
Module 2	
Module 3	
Module 4	

Figure 29. HMC Cellular PIN Codes Screen

2. If more than one slot is displayed, select a specific Cellular Card. The PIN Codes screen of that cellular card is displayed.

3. Enter the PIN code into the associated Module's field.

4. Click **Apply Settings** and wait for —Configuration Saved‖ to be displayed.

3.4 Reset

Use the Cellular Card Reset screen to reset either the entire cellular card or a specific cellular module.

To reset a cellular card or module:

1. From the Cellular Cards branch of the HMC navigation pane, click the **Reset** sub-branch. The Reset screen is displayed.

Figure 30. Cellular Card Reset screen

2. If more than one slot is displayed, select a specific Cellular Card. The Reset screen of that cellular card is displayed.

Caution: There is no confirmation message. The Reset command is sent as soon as the reset button is clicked.

3. Click **Reset**. The screen confirms that the Reset command has been sent.

Figure 31. Reset screen after sending the Reset command

3.5 Information Screens

Several HMC screens display information.

3.5.1 Module Info

Use the Module Info screen to review information about the modules of a cellular card.

1. From the Cellular Cards branch of HMC navigation pane, click the **Module Info** sub-branch. The Module Info screen is displayed.
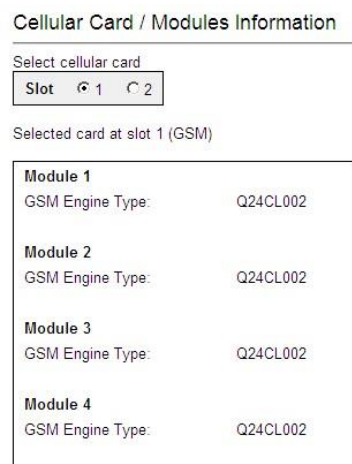
Figure 32. HMC Module Info Screen

2. If more than one slot is displayed, select a specific Cellular Card. The Module Info screen of that cellular card is displayed

3.5.2 Serial Numbers

Use the Serial Numbers screen to view the GSM Modules International Mobile Equipment Identity (IMEI) and the SIMs International Mobile Subscriber Identity (IMSI).

1. From the HMC navigation pane Cellular Cards branch, click the **Serial Numbers** sub-branch. The Serial Numbers screen is displayed.

Figure 33. HMC Serial Numbers Screen

2. If more than one slot is displayed, select a specific Cellular Card.

3.6 Locks

Use Locks to restrict access to specific GSM operators and/or a specific SIM card. When a lock is defined, the Gateway will only accept calls from an operator or a SIM card that matches the Lock number.

In addition, use Locks to prevent roaming handover in cases where the Gateway is located close to another county or a country border.

To define a Lock number:

1. Ensure the following:

   ▪ You have obtained the codes from the cellular operator.

   ▪ The cellular modules support SIM locks.

2. From the Cellular Cards branch of the HMC navigation pane, click the **Locks** sub-branch. The Locks screen is displayed.

Figure 34. HMC Cellular Locks Screen

3. If more than one slot is displayed, select a specific Cellular Card. The Locks screen of that cellular card is displayed.

4. Fill the fields of the following:

   SIM Lock

   Use SIM Locks to avoid using SIM cards other than those whose Mobile Network Code (MNC) and Mobile Country Code (MCC) values have been entered.

   Operator Lock

   Use Operator Locks to avoid registration to any network other than the one whose MNC and MCC values have been entered.

5. Click **Apply Settings** and wait for —Configuration Saved‖ to be displayed.

3.7 SIM Select

Use the SIM Select screen to manually select and activate a SIM card for current use. SIM Select should not be used when SIM Auto Manage is active. The definition can be applied just to the module, to all 4 modules on the card, or to all the cellular cards in the system (see Cellular Card and System Terminology in section 3.1   ).

To manually select SIM cards:

1. From the Cellular Cards branch of the HMC navigation pane, click the **SIM Select** sub-branch. The SIM Select screen is displayed.

Figure 35. HMC SIM Select Screen

2. If more than one slot is displayed, select a specific Cellular Card. The SIM Select screen of that cellular card is displayed.

3. Select an application option:

    Module Settings
    Applies the SIM configuration to the specific module.

    Entire Card
    Applies the SIM configuration to all the modules on the card.

Figure 36. HMC SIM Select Screen – selection for entire card

Entire System

Applies the SIM configuration to all the cards in the system.

4. Click **Apply Settings** and wait for —Configuration Saved‖ to be displayed.

3.8 Cell Selection

Use the Cell Selection screen to manually camp on a cellular site. Most often the user will select the strongest cell site. However, if the Base Transceiver Station (BTS) or tower is locked, this service cannot be applied.

Note: This feature is only available when Wavecom GSM or Telit GSM/UMTS modules are installed.

To camp on a site:

1. From the HMC navigation pane Cellular Cards branch, click the **Cell Selection** sub-branch. The Cell Selection screen is displayed.

Figure 37. HMC Cellular Cell Selection Screen

2. If more than one slot is displayed, select a specific Cellular Card. The Cell Selection screen of that cellular card is displayed.

3. From the **Select module** dropdown box, select a module. This is the module that the Camp selection will be applied to.

4. In one of the CellID boxes, click **Camp**. The screen indicates Camp Cell and new controls are displayed at the top of the screen.

Configuring a Cellular Card

Figure 38. HMC Cellular Cell Selection with Options Screen

5. Optionally, to camp all the card's modules on the same cell, click **Camp all modules on**.

3.9 Settings

Use the Settings screen to enable and disable advanced parameters. For assistance with these, contact Technical Support.

1. From the Cellular Cards branch of the HMC navigation pane, click the **Settings** sub-branch. The Cellular Card Settings screen is displayed.

Figure 39. HMC Cellular Card Settings Screen

2. If more than one slot is displayed, select a specific Cellular Card. The Cellular Card Settings screen of that cellular card is displayed.

3. Click **Apply Settings** and wait for **Configuration Saved** to be displayed.

3.10 Network Parameters

Use the Network Parameters screen to define the bandwidth used by a carrier.

1. From the Cellular Cards branch of the HMC navigation pane, click the **Network Parameters** sub-branch. The Cellular Card Network Parameters screen is displayed.

Figure 40. HMC Cellular Card Network Parameters Screen

2. If more than one slot is displayed, select a specific Cellular Card. The Network Parameters screen of that cellular card is displayed.

3. Select the matching bandwidth from the dropdown menu. For a table of bandwidths per country, see http://en.wikipedia.org/wiki/Mobile_network_code

4. From the HMC navigation pane, click the **Save/Load** branch and then click **Save All Settings**.

3.11 USSD SIM Balance

Use the USSD SIM Balance screen to check the balance remaining on a prepaid SIM card and to add value to a SIM card (recharge/top-up).

1. Ensure that your Service Provider has given you a USSD string for checking balance and a second string for adding value (recharging) the SIM card.

2. From the HMC navigation pane Cellular Cards branch, click the **USSD SIM Balance** sub-branch.

Figure 41. HMC Cellular USSD SIM Balance Screen

3. Enter the **Balance checking USSD string**.

4. Enter the **Recharging USSD string**.

5. Select or clear the **Check All** checkbox. When selected, the Hypermedia Management Console will check the balance of all the SIM cards.

6. Click ⓘ (Check Balance). The balance is displayed in the USSD Reply column.

7. Optionally, recharge the SIM card:

   a. Ensure that you have a recharge string. Often, the string is displayed on recharge cards after a removing a layer of ink that hides the string.

   b. Enter the string into the Recharge Balance field.

   c. Click the ⊙ (Recharge Balance) button.

8. Optionally, click the ⊠ (Excel) icon to save the results as an Excel file.

3.12 Monitoring Cellular Cards

To monitor the status of cellular cards, open the **Monitor > Cellular** branch of the Hypermedia Management Console. There are three views.

3.12.1 All Cells

To view information about all the cellular modules on all the cards, expand the Monitor > Cellular Cards sub-branch and select **All Cells**. The Cellular Cards Reception screen is displayed.

Cellular Card Receptions

Module	Type	Operator	RX Level	RX BER	Status
1 / 1	GSM	orange (8221)	-67 dBm	<0.2%	Idle
1 / 2	GSM	orange (8221)	-65 dBm	<0.2%	Idle
1 / 3	GSM	orange (8221)	-67 dBm	<0.2%	Idle
1 / 4	GSM		Unknown	Unavailable	Missing SIM card
2 / 1	GSM		Unknown	Unavailable	No Signal
2 / 2	GSM		Unknown	Unavailable	Missing SIM card
2 / 3	GSM		Unknown	Unavailable	Faulty/missing
2 / 4	GSM		Unknown	Unavailable	Faulty/missing

Figure 42. Cellular Cards Reception Screen The

screen displays the following information:

Module

This indicates the card and the SIM slot number.

Type

The module can support GSM, CDMA or UMTS.

Operator

This is the cellular network associated with the SIM card and the Cell ID.

RX Level

This indicates the received power level in dBm. The value can be between
−51dBm and −110 dBm.

RX BER

Bit Error Rate (BER) is a calculated figure for the signal quality received
from the base. It is an indication of the number of errors detected in the
signal received by the cellular channel, graded into quality ratings
according to the percentage of errors in the data. Typical values for BER
are between less than 0.2% and 6.4%. BER of more than 6.4 will result in
calls being disconnected as well as ―noisy‖ calls. If this occurs, find a
better location for the antenna or check the antenna connections.

Status

This displays the status of the specific SIM slot.

3.12.2 Reception

To view information about the SIM slots on a specific cellular module,
especially the reception level and the BER level:

1. Expand the Monitor > Cellular Cards sub-branch and select **Reception**.

2. Select a specific slot. The Cellular Cards Reception screen for that card is
   displayed.
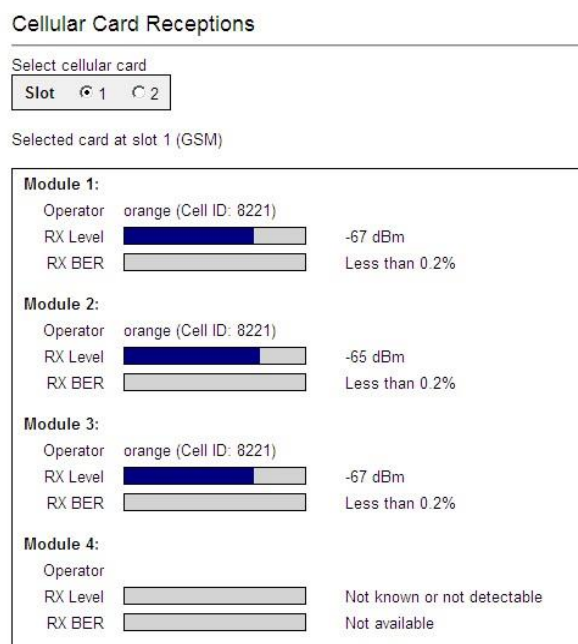
Figure 43. Specific Card's Cellular Reception Screen The

screen displays the following information:

Operator

This is the cellular network associated with the SIM card and the Cell ID.

RX Level

This indicates the received power level in dBm. The value can be between −51dBm and −110 dBm.

RX BER

Bit Error Rate (BER) is a calculated figure for the quality of the signal received from the cellular base-station (see more details in above section 3.12.1).

3.12.3 Status

To view information about the status of SIM slots on a specific cellular module:

1. Expand the Monitor > Cellular Cards sub-branch and select **Status**.

2. Select a specific slot. The Cellular Cards Status screen for that card is displayed.
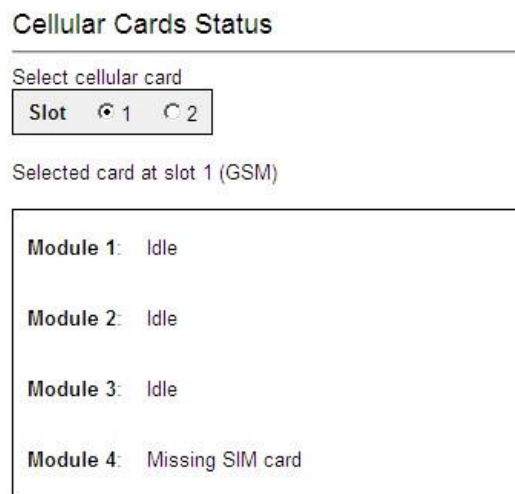
Figure 44. Cellular Cards Status Screen

3. Review the status. Common possibilities include:

- Module doesn't exist or is faulty
- Idle
- Incoming call from cellular network
- Remote side ringing
- Call connected
- Call cleared
- Dialing out through cellular network
- No Signal
- Missing SIM card

4 Configuring the SMS Server

This section contains:

- License (section 4.1   )
- Configuration (section 4.2   )
- Channel Selection (section 4.3   )
- SMS Sender (section 4.4   )
- Advanced Call Routing (ACR) (section 4.5)
- Counters (section 4.6)
- Slaves Manager (section 4.7)

4.1 License

Use the License screen to upload and apply the license of the SMS Server.

To license the SMS server:

1. Ensure you have an authorized license. Licenses are delivered via email from Hypermedia Technical Support. For assistance, contact Technical Support.

2. From the SMS Server branch of the HMC navigation pane, click the **License** sub-branch. The SMS Server License screen is displayed.

Figure 45. SMSPro License

3. Click **Browse** to locate the server license.
4. Click **Upload** to apply the license.

4.2 Configuration

Use the Configuration screen to define parameters that affect the performance of the SMS PRO Gateway.

To define parameters:

From the SMS Server branch of the HMC navigation pane, click the **Configuration** sub-branch. The Configuration screen is displayed.

Following are the configuration parameters: (scroll down to see all parameters).

Figure 46. SMS Server Configuration Screen

Server Status

Sets the status of the SMS Gateway. The actual state of the SMS Gateway is displayed below the selection box, and can have one of three values:

▪ **Running**: In this state the Gateway will process and send SMS requests.

Hypermedia Systems

- **Paused**: In this state the Gateway will not send out SMS's. Any new send requests will be queued and sent only when the 'Running' state is resumed.

- **Disconnected**: Indicates the Gateway service is down. The Mode can be set to one of three actions:

- **scheduled**: When this is set, the state of the Gateway will be determined by status commands set by the scheduler or via the SMS Gateway PRO API.

- **pause**: This puts the Gateway in the "Paused" status. Once this has been set, the only way to return to the "Running" status is to select the "run" action.

- **run**: This puts the Gateway in the "Running" status. Once this has been set, the only way to return to the "Paused" status is to select the "pause" action.

ACR

Determines whether the ACR is active or not. Can be set to either **yes** or **no**.

SMS Server Configuration

Log Level
Set the detail level of the log file. This should always be on 'error' unless technical support requires logs with a higher resolution.

debug ▼

Confirmation
Determines whether the confirmation of receipt is on by default

yes ▼

GSM 03.38 Encoding
Determines whether the GSM 03.38 Encoding is Latin or Greek

latin ▼

Collection of incoming SMS
Allows receiving incoming SMS messages on any of the available SIM cards (set by counter) by mapping each of the SIMs duringoff-peak time for a short predefined time period.

- <u>Start Time</u> : time of day (hours) on which this feature should be activated.
- <u>Timeout for first SMS</u> : the amount of time (in seconds) to wait for an incoming SMS once a SIM has been registered to the network using this feature.
- <u>Timeout for additional SMS</u> : the amount of time (in seconds) to wait for additional messages after at least one incoming message was already received

Start Time	none ▼
Timeout for first SMS	120
Timeout for additional SMS	30

Submit

Log Level

Sets the detail level of the log file. The value should always be set to 'error', unless Technical Support requires logs with a higher resolution. Options: **debug/info/warning/error**.

Confirmation (DLR)

Determines whether the receipt confirmation is on by default. Options: **yes/no**.

GSM 03.38 Encoding

Determines whether the GSM 03.38 Encoding is Latin or Greek. Options: **latin/greek**

Collection of incoming SMS

Allows receiving incoming SMS messages on any of the available SIM cards (set by counter), by mapping each of the SIMs during off-peak time for a short predefined time period.

- **Start Time**: time of day (hours) at which this feature should be activated.

- **Timeout for first SMS**: the amount of time (in seconds) to wait for an incoming SMS once a SIM has been registered to the network using this feature.

- **Timeout for additional SMS**: the amount of time (in seconds) to wait for additional messages after at least one incoming message was received.

PDU

Determines whether the PDU is active or not.

Options: **yes/no**

Queue type

- **cyclic**: a new SMS will be sent from the next available SIM card.

- **serial**: a new SMS will be sent from the first available SIM card.

Port Queue Resend on Counter Block

When a port becomes blocked from sending additional SMS but there are still messages waiting to be sent on its queue, this determines whether the

remaining messages should stall until the port is unblocked, or whether the messages should be resent to queues of non-blocked ports.
Options: **yes/no**
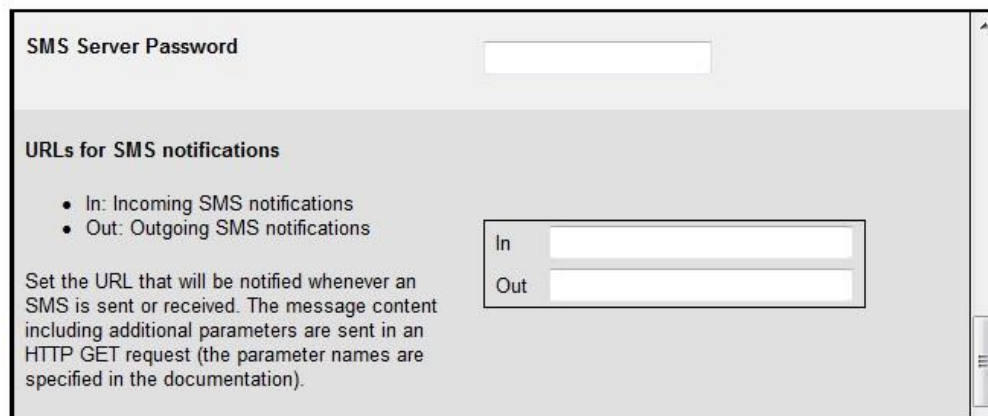
MySQL Host

Note: Only applicable on a PC based system.

Leave empty if MySQL is not used.
Using MySQL requires a separate installation of MySQL on a different PC. You should have an account that can create the database and have write access to it.

SMS Server Password
Define a password for the SMS Server if required.

URLs for SMS notifications

- **In**: Incoming SMS notifications.

- **Out**: Outgoing SMS notifications.

Set the URL that will be notified whenever an SMS is sent or received. The message content, including additional parameters, is sent in an HTTP GET request (the parameter names are specified in the Developer's API chapter).

Configuring the SMS Server

E-mail notifications from SMS Gateway

- **Server**: The SMTP server through which the e-mail notification will be sent.

Note: TLS is only supported on PC-based systems.

- **Port**: The SMTP server port (usually 25).

- **User**: User name of the mail account.

- **Password**: The password for above account.

- **From**: Who will appear as the e-mail sender (Usually same as User).

- **Incoming SMS Subject**: E-mail subject line.

- **Incoming SMS To**: E-mail address of recipient for incoming SMS.

- **Counter Event To**: E-mail address of recipient for SMS counter blocks. Each time a SIM card is blocked due to reaching a count limit, or an entire cellular module is blocked (because all its SIM cards are blocked), an e-mail describing the event will be delivered to the e-mail address defined in this field.

eMail to SMS

- **Use TLS**: Use TLS to connect to the server

Note: TLS is only supported on PC

- **Server**: The server from which the e-mails should be retrieved.

- **Port**: The incoming mail server port.

- **User**: User name of the mail account.
  Example: yyy@example.com

- **Password**: The password for above account.

- **Identification period**: When replying by SMS to an email received by SMS without explicitly specifying the target recipient code in the SMS body, the system attempts to deduce the intended e-mail recipient by

➡ the mobile number of the replier. This identification period defines how long (in hours) the system should associate this number with an intended recipient.

Note that this method is not fail safe, and in most cases it is recommended to leave this value as zero, which disables it.

- **Limit Messages**: This enables constricting the number of SMS that will be generated from a single email. Useful in disabling situations where a long email will result in sending a large number of SMS notifications.

- **Number in URL**: When sending an email to SMS, defines where to place the phone number of the target SMS recipient.
   Supposing a message is to be sent to John Doe's mobile phone whose number is 9879889403:

   - **yes**: means an SMS should be sent by sending the message to an email address of the form: "John Doe" <879889403@johndoeplace.com>>

   - **no**: means SMS will should sent by sending the message to an email address of the form: "John Doe|879889403" <jdoe@gmail.com>

- **User Authentication**: Defines whether the only authorized SMS recipients are those that appear in the user list.

No SMS counter increments for codes: In some error cases, when the SMS is not sent, it is preferable that the SMS counter will not be incremented. This parameter should contain a comma sepatated list of error codes for which the SMS counter should not be incremented.	Codes: 0022, 0026, 0029
Error codes for send delay In the 'Delay' field, enter the delay in seconds before the SIM is available for another send. In the 'Codes' field, enter a comma separated list of error codes that can trigger this delay.	Delay: 10 Codes: 0011, 0016, 001F, 0022, 0026, 0029, 002A, 0066
Error codes for send retry In the 'Retry' field, enter the number of retry attempts if send fails In the 'Codes' field, enter a comma separated list of error codes that can trigger a retry.	Retry: 2 Codes: 0011, 0016, 001F, 0022, 0026, 0029, 002A

No SMS counter increments for codes

In some error cases, when the SMS is not sent, it is preferred the SMS counter will not be incremented. This parameter should contain a comma separated list of error codes for which the SMS counter should not be incremented.

Error codes for send delay

In the 'Delay' field, enter the delay period (in seconds) before the SIM is available for another send.

In the 'Codes' field, enter a comma separated list of error codes that can trigger this delay.

Error codes for send retry

In the 'Retry' field, enter the number of retry attempts if send fails.

In the 'Codes' field, enter a comma separated list of error codes that can trigger a retry.

SMPP

- **Receive Default**: SMSC Receive Default Alphabet (SMPP to GSM).

- **Transmit Default**: SMSC Transmit Default Alphabet (GSM to SMPP).

- **destination_addr**: SMPP field value interpretation for incoming SMS (GSM to SMPP).

  SIM-Addr: Populate with SIM port address (e.g 21#1).

  Static: Use a static destination number with the value 123456789.

<u>Orig-User</u>: According to Binding port group and Message Tagging rules.

- **User Data**: For incoming SMS send the User Data in (GSM to SMPP): <u>message_payload</u>: Enabling data larger than 254 octets.

  <u>short_message</u>: Requiring all messages be shorter than 255 octets.

- **Log Level**

  Only use values other than Error when in a session with Technical Support.

Binding port group to sender

Groups of ports may be bound to the identity of the message sender (client or username). Affects the port group selection method on outbound SMS, as well as message routing to a specific client/user on inbound SMS.

- **client_id**: Port groups will be selected according to the ID of the sending client. Be sure to define the group name for "Route to Group" on the Channel Selection page exactly the same as the client ID.

- **user_name**: Port groups will be selected according to the ClientID:UserName pair. Be sure to define the group name for "Route to Group" on the Channel Selection page to match the predefined client ID and user name, in a "ClientID:UserName" format.

- **no**: Feature is disabled. Either use ACR groups or no groups at all.

Note: When using this feature, proper Client IDs must be defined on the User List page.

Configuring the SMS Server

> **Message Tagging**
> Routing of inbound messages to a specific user
> is possible in case these are replies to messages
> previously sent by that user, according to various
> criterias.
>
> - **Action:**
>   <u>attach_user</u>: Inbound messages will be
>   routed to the original sending user should
>   these be uniquely identified according to
>   the message sender's phone number.
>   <u>attach_user_num</u>: A configurable message
>   header will be added to each outbound
>   message instructing the recipient to reply
>   with a specific header.
>   <u>no</u>: Feature disabled.
>
> - **Message header** - Text to be added to
>   each outbound message (automatically
>   followed by a unique numeric value and a
>   star sign) when "attach_user_num" is
>   used.
> - **Identification period** - The duration (in
>   hours) during which the system should
>   associate a phone number with a sending
>   user for inbound message routing
>   purposes.
>   *Note that this feature is not fail safe and in
>   most cases it is recommended to leave it
>   disabled (value as zero).*
> - **Outbound SMS validity** - The duration (in
>   days) during which outbound messages
>   are stored for statistical calculation
>   purposes.
>
> **Note:** This feature is not functional when binding
> port groups to user_name.
>
> | | |
> |---|---|
> | Out SMS action | no |
> | Add Title | |
> | Identification period | 168 |
> | Out sms max valid days | 7 |

Message Tagging

Routing of inbound messages to a specific user is possible in case there are replies to messages previously sent by that user, according to various criterions.

- **Action**:

  <u>attach_user</u>: Inbound messages will be routed to the original sending user, should these be uniquely identified according to the message sender's phone number.

  <u>attach_user_num</u>: A configurable message header will be added to each outbound message, instructing the recipient to reply with a specific header.

- **no**: Feature is disabled.

- **Message header**: Text to be added to each outbound message (automatically followed by a unique numeric value and a star sign) when "attach_user_num" is used.

- **Identification period**: The duration (in hours) during which the system should associate a phone number with a sending user for inbound message routing purposes.

➡ **Note** that this feature is not fail safe, and in most cases it is recommended to leave it disabled (value set to zero).

- ▪ **Outbound SMS validity**: The duration (in days) during which outbound messages are stored for statistical calculation purposes.

➡ **Note:** This feature is not yet functional when binding port groups to **user_name.**

SIM reply timeout (in seconds)

Number of seconds to wait for a reply from the SIM before failing.

Card ready delay (in seconds)

Number of seconds to wait before sending another SMS through the same cellular card. Should usually remain zero for maximum throughput.

4.3 Channel Selection

Use the Channel Selection screen to select which modules will process SMS messages, and for routing messages through specific channels.

1. From the HMC navigation pane SMS Server branch, click the **Configuration** sub-branch. The Configuration screen is displayed.

Figure 47. SMS Server Channel Selection

2. Select the checkbox to enable a module. The Apply Settings button is displayed.

Figure 48. Route to Group Screen

3. Click **Apply Settings**. The Route to Group option is enabled.

4. Optionally, use ACR rules to define the channels the SMS messages will be routed to (see section 4.5.1).

5. Select a **Group**. There are two options:

   ▪ Click **New** to create a new Group, and enter the Group name in the field.

   ▪ Click **Select** to select an existing Group, and select a Group from the dropdown list.

6. Click **Apply Settings**.

4.4 SMS Sender

Use the SMS Sender screen to make online SMS tests with any of the SIMs preconfigured for use with the SMS Server.

The ―Outgoing Message‖ section allows sending a message through any of the predefined SIMs to any phone number. Enter the required text message and click **Send SMS**.

The ―Incoming Text Messages Log‖ section displays all inbound SMS messages and allows the following filters:

1. ―From Phone Number‖ - Displaying only text messages originated from the phone number to which a test message was previously sent (―Phone number‖ in the upper section). Select the ―Destination Only‖ option to do so. Otherwise select ―All‖.

2. ―To SIM‖ - Displaying only text messages received through the SIM on which a test message was previously sent (―SIM‖ in the upper section). Select the ―Selected‖ option to do so. Otherwise select ―All‖.

Inbound messages will appear in the window below these options. Click **Clear Log** to clear the contents of that window.

Figure 49. SMS Sender Screen

4.5 Advanced Call Routing (ACR)

Use the ACR to define special actions to be performed on a Number List. For example, white lists and black lists. The ACR enhances the SMS server's capabilities such that rules may be applied for outbound SMS messages in a similar manner to outbound calls on voice-enabled systems.

> **Note:** A white list includes the phone numbers that are authorized as dialed destinations, whereas a black list includes the phone numbers that are **prevented from being dialed.**

To enable the ACR:

1. Define the ACR rules.

2. Prepare and upload the Number List (optional).

3. Arrange the rules according to their priority. The list of rules is scanned and applied from top to bottom.

4. Set a default action when there was not match to the rules above it, or when no rule provided a group selection.

4.5.1 ACR Rules

To create an ACR Rule:

1. Ensure that an up-to-date **ACR Number Lists.csv** file has been uploaded to the Gateway.

2. From the SMS Pro Server branch of the HMC navigation pane, click the **ACR Rules** sub-branch. The ACR Rules screen is displayed.

ACR - Advanced Call Routing - Rules

Prioity	Name	Description	Edit	Delete
	Default	Allow call	block	

Add new rule

Figure 50. ACR Rules Screen

3. Click **Add new rule**. The Add New Rule screen is displayed.

Configuring the SMS Server

Add New Rule

Details:	
Rule Name	

Check:	
Destination	No check ▼

Actions:	
Block	☐
Route to group	-none- ▼

Save Cancel

Figure 51. Add New Rule Screen

4. In the Rule Name field, type the rule name.

5. In the Check field, from the Destination dropdown menu, define the rule indication.

   If an indication is selected, a dialog box similar to the following is displayed:

Check if destination begins with	
⦿ Number	
⦿ Number from	None ▼

save clear

Figure 52. Sample Check Dialog Box (source)

No Check

The rule does not check the Destination number.

Begins With

The rule checks if the Destination number begins with specific digits or with a tag that appears on the list.

Ends With

The rule checks if the Destination number ends with specific digits or with a tag that appears on the list.

In Range

The rule checks if the Destination number is within a specific range.

Identical to

The rule checks if the Destination number is exactly the specific digits or tag that appears on the list.

Operator is

To be used in conjunction with the Local Number Portability (LNP) application which looks up the destination number in a pre-loaded database of numbers and the cellular operator these were ported to.

6. Complete filling the dialog box and click **Save**.

7. In the Actions area, define what the ACR does when a number matching the indications defined in the Check area is identified.

   No Actions are Defined

   If no actions are defined, the text message is allowed as is.

   Block

   Text messages matching the indications are blocked.

   Route to Group

   Text messages matching the indications are routed through the defined Channel Group.

8. Click **Save**. The new rule is added to the ACR Rules screen.

9. Prioritize the rule. Use the arrows in the Priority column to increase or decrease a rules priority.
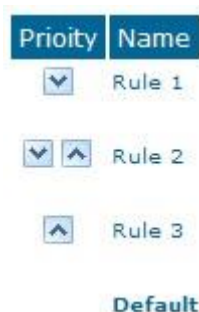
Figure 53. Rule Prioritization Arrows

4.5.2 Modifying the ACR Number List

To modify the ACR Number List:

1. From the HMC navigation pane SMS Server branch, click the **ACR Numbers Lists** sub-branch. The ACR Number Lists screen is displayed.

Figure 54. ACR Number Lists Screen

2. Click **Export**. The standard Windows browse dialog box is displayed.

3. Save the **.csv** file.

4. Open the file in a text-editor, such as Notepad.

➡ **Note:** The file format must be preserved, noting the words **tag,number** must appear as the first row of the list.

5. Modify the file.

6. Save and close the file.

7. On the ACR Number Lists Screen, click **Browse**. The standard Windows browse dialog box is displayed.

8. Locate the **.csv** file containing the lists, and click **Open**. The path to the .csv file is displayed on the Number Lists Screen.

9. Select one of the following:

   ▪ **Overwrite**: the old .csv file is replaced by the new file.

   ▪ **Append**: the entries on the new .csv file are added to the old .csv file.

10. Click **Import**. The report of total lists and total numbers is updated.

4.5.3 Creating a New ACR Number List File

To create a number list:

1. Create a file in a text-editor, such as Notepad, with the extension **.csv**.

2. Enter the words **tag,number** as the first row of the list.

➡ **Note:** In following step 3, the term —list‖ indicates all entries that share the same tag.

3. Add a tag and number, with a comma between them, to each entry. Ensure a comma separates the tag from the number.

   Following is an example of five lists:

   tag,number XYZ,0774445004

   XYZ,0509080704

   XYZ,0523030303

   ABC,0509380137

   ABC,0509380136

   CLCOM,052 PHONE,054

   CELLC,050

⚠ **Caution:** A comma must separate the tag and the number or the list will not register properly.

4. From the SMS Server branch of the HMC navigation pane, click the **ACR Numbers Lists** sub-branch. The ACR Number Lists screen is displayed.

Total lists on database:9
Total Numbers in all lists:12

Choose a CSV file to upload:

Browse...

○ Overwrite
● Append

Import

Export

Upload Result:
The file 2008-12-09.csv has been uploaded
File total rows=12

Figure 55. ACR Number Lists Screen

5. Click **Browse**. The standard Windows browse dialog box is displayed.

6. Locate the **.csv** file containing the lists, and click **Open**. The path to the .csv file is displayed on the Number Lists Screen.

7. Select one of the following:

   ▪ **Overwrite**: The old .csv file is replaced by the new file.

   ▪ **Append**: The entries on the new .csv file are added to the old .csv file.

8. Click **Import**. The report of total lists and total numbers is updated.

4.6 Counters

Use SMS Counters to allocate the use of SIM cards.

4.6.1 Enabling Counters

1. Ensure that on the Channel Selection screen the module is **SMS enabled** (see —Channel Selectionǁ in section 4.3).

2. From the SMS Server branch of the HMC navigation pane, click the **Counters** sub-branch. The SMS Counters screen is displayed.

3. Identify the port of the card that is to be enabled:

   ▪ **Card**: Identifies the slot the card occupies.

   ▪ **Port**: Matches the module within the card.

4. Select the checkbox in the **Enable** column.

   Note: The **Active** column (read only) indicates if counting is, or has been, active on a port.

5. Select the **Enable** checkbox of the SIM cards that will participate in counting.

6. Set the following parameters:

   ▪ **Switch Number**: Enter the number of SMSs sent by a SIM card after which the module will switch to send by the next SIM card. This number has to be at least one (1).

   ▪ **Blocked Number**: Enter the number of SMSs a SIM card can send before the Gateway blocks the SIM card. If set to zero (0), the SIM cards are never blocked.

   ▪ **Daily Quota**: Enter the allowed number of SMSs that can be sent by a SIM card per day.

7. Click **Update Configuration**. Status is updated and is indicated by color.

Card	Port	All	Enable	Active	Delete	Switch Number	Blocked Number	Day Quota	SIM-1	SIM-2	SIM-3	SIM-4
ALL	ALL	☐ Enable ☐ Reset	☐		☐	0	0	0	☐ Enable ☐ Reset	☐ Enable ☐ Reset	☐ Enable ☐ Reset	☐ Enable ☐ Reset
Slot - 1 (21)	1	☐ Enable ☐ Reset	☑	☑	☐	20	500	100	☑ Enable ☐ Reset 3 3	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0
Slot - 1 (21)	2	☐ Enable ☐ Reset	☑	☑	☐	20	500	100	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0
Slot - 1 (21)	3	☐ Enable ☐ Reset	☑	☑	☐	20	300	100	☑ Enable ☐ Reset 2 2	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0
Slot - 1 (21)	4	☐ Enable ☐ Reset	☑	☑	☐	20	300	100	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0	☑ Enable ☐ Reset 0 0

Figure 56. Counters and Colors

- ▪ **Yellow border**: Indicates the module's selected SIM.

- ▪ **Green**: The SIM is active and there is reception.

- ▪ **Yellow**: The SIM is not active. The SIM is present, but is not enabled.

- ▪ **Pink**: SIM is blocked by the cellular card. Could also be a reception issue, or no SIM.

- ▪ **Red**: The SIM card is blocked.

8. Optionally, set the **Counter Event To** in the configuration screens (see —Email Notifications from SMS Gateway‖ is section 4.2).

9. Optionally, set the Scheduler's automatic **Reset SIM Counter** function (see —Reset SIM Counter‖ is section 5.1.3   ).

4.6.2 Disabling Counters

To disable Counters for a specific module:

1. Ensure that on the Channel Selection screen the module is **SMS disabled** (see —Channel Selection‖ in section 4.3   ).

2. Select the **Delete** checkbox.

3. Click **Update Configuration**. The row is deleted from the Counters screen.

4.7 Slaves Manager

In a network of multiple SMS PRO Gateways, one Gateway can be defined as the Master. Slave Gateways are entered on the Master Gateway's Slave Manager page. It is neither required nor possible to define the Master Gateway from the Slave Gateway.

When a Master/Slave network is configured, the Slave Gateway's SIM cards are displayed on the Master Gateway. For example, it is possible to configure counters on the Slave Gateway from the Master Gateway.

4.7.1 Adding a Slave Gateway to a Master Gateway

To add a Slave Gateway to the Master Gateway:
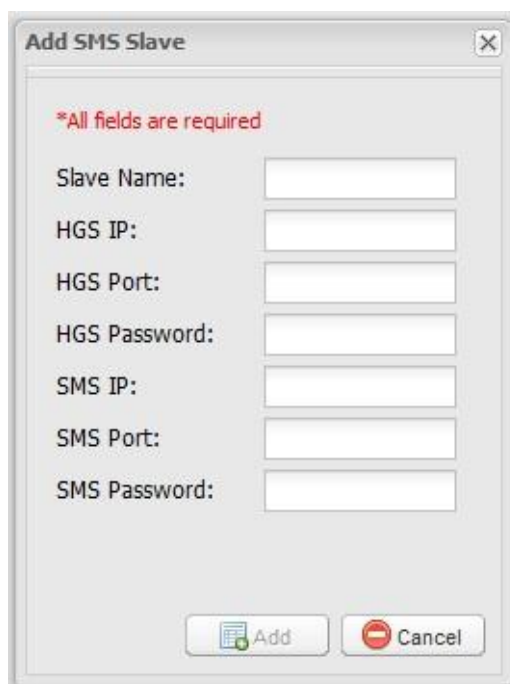
1. From the Master Gateway's HMC navigation pane SMS Server branch, click the **Slaves Manager** sub-branch. The Slaves Manager screen is displayed.

Figure 57. Slaves Manager Screen

2. Click **Add Slave**. The Add SMS Slave dialog box is displayed.

Figure 58. Add SMS Slave Screen

3. Fill the Slave parameters:

Slave Name

Enter a name that assures proper identification of the Slave.

HGS IP

This is the IP address to access the HyperGateway System application. It is usually the same as the IP address used to access the SMS application.

HGS Port

The default port is **8878**.

HGS Password

Enter the password that will enable access to the HyperGateway Server (same one used by HMC to log in directly to the Slave system).

SMS IP

This is the IP address to access the SMS application. It is usually the same as the IP address used to access the HyperGateway Server.

SMS Port

The default port is **63333**.

SMS Password

Enter the password that will enable access to the SMS application, as configured on the Slave system.

4. Click **Add**. Focus returns to the Slave Manager screen and the new Slave is displayed in the list.

4.7.2 Configuring a Slave to have its SIM Cards used by the Master

Once a Slave Gateway has been successfully added to the master (see above), in order to configure that Slave Gateway to have its SIM cards used by the Master Gateway:

1. From the SMS Server branch of the Slave Gateway's HMC navigation pane, click the **Channel Selection** sub-branch. The Channel Selection screen is displayed.

2. Follow the procedure described in —Channel Selection‖ (see section 4.3). Ensure the following:

- The module is enabled

- The module is assigned to a Group

5 Scheduler

Use the Task Scheduler to configure the Gateway to repeat commands at scheduled intervals. Several commands are preconfigured. In addition, it is possible to manually configure a command.
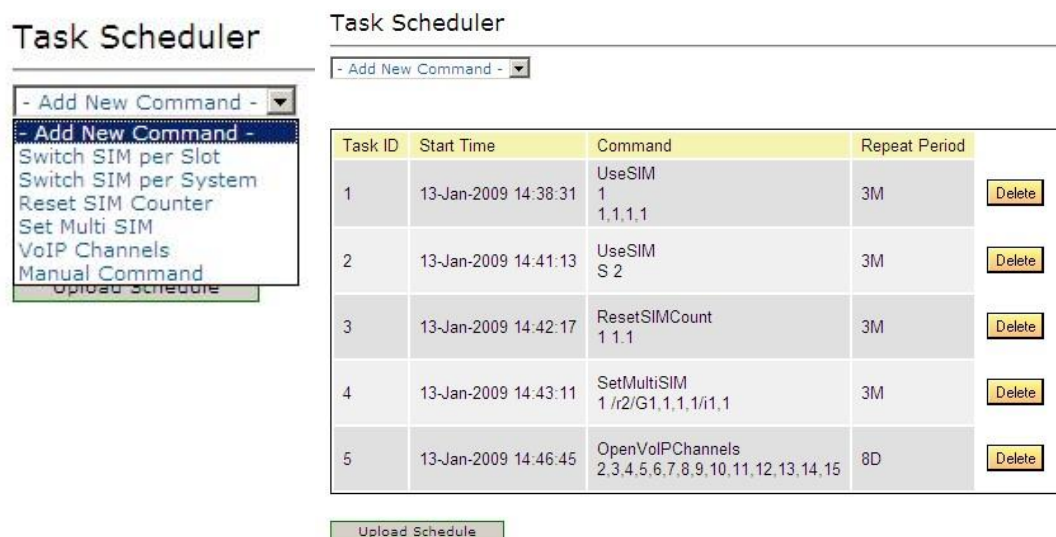
Figure 59. Dropdown Menu of Tasks and Table of Scheduled Tasks

5.1 Scheduler Commands

5.1.1 Switch SIM per Slot

Use the Switch SIM per Slot task to configure a GSM slot to use specific SIM cards for a defined period of time.

1. From the HMC navigation pane, expand the **Manage** branch.

2. Click the **Scheduler** sub-branch. The Task Scheduler screen is displayed.

3. From the **Add New Command** dropdown menu, select **Switch SIM per Slot**. The Task Scheduler automatically advances to the next screen.

Figure 60. Task Scheduler Switch SIM per Slot Screen

4. Configure the task parameters:

   Slot

   Select or clear the checkboxes. Each checkbox represents the GSM card located in the numbered slot counting from the left.

   SIM

   From each module's dropdown menu, select the SIM card that that module will use. Select As Is if the Gateway does not change the SIM activity.

➡ **Note:** Use the All dropdown menu to assign the same SIM card to all four modules.

5. Click **Next**. The Set Command screen, with the command syntax, is displayed.

Figure 61. Task Scheduler Set Command Screen

⚠ **Caution:** Clicking **menu** deletes the new task. The table of schedules tasks is redisplayed.

6. Configure the task's schedule:

   a. Click 🗓 (calendar icon). A calendar opens in a new browser tab.

➡️ **Note:** First, set the time. As soon as you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   b. Enter the time that the command will start.

   c. Enter the date that the command will start. When you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   d. From the Repeat drop-down menu, select either **Yes** or **No**.

   e. If the task is configured to repeat, select a **Repeat Period**. The Repeat Period can be either months, days, hours, or minutes.

7. Click **Set Command**. The new Task is displayed in the Task Scheduler screen.

8. Click **Upload Schedule**. The Server activates the schedule according to the defined dates and times.

5.1.2 Switch SIM per System

Use the Switch SIM per System task to configure a Gateway to use one specific SIM card for a defined period of time.

1. From the HMC navigation pane, expand the **Manage** branch.

2. Click the Scheduler sub-branch. The Task Scheduler screen is displayed.

3. From the **Add New Command** dropdown menu, select **Switch SIM per System**. The Task Scheduler automatically advances to the next screen.
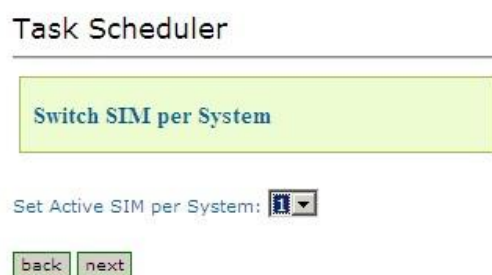
Figure 62. Task Scheduler Switch SIM per System Screen

4. From the Set Active SIM per System dropdown menu, select the SIM card that the entire system will use.

5. Click **Next**. The Set Command screen, with the command syntax, is displayed.

Figure 63. Task Scheduler Set Command Screen

⚠️ **Caution:** Clicking **menu** deletes the new task. The table of schedules tasks is redisplayed.

6. Configure the task's schedule

   a. Click (calendar icon). A calendar opens in a new browser tab.

➡️ **Note:** First, set the time. As soon as you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   b. Enter the time that the command will start.

   c. Enter the date that the command will start. When you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   d. From the Repeat drop-down menu, select either Yes or No.

   e. If the task is configured to repeat, select a **Repeat Period**. The Repeat Period can be either months, days, hours, or minutes.

7. Click **Set Command**. The new Task is displayed in the Task Scheduler screen.

8. Click **Upload Schedule**. The Server activates the schedule according to the defined dates and times.

5.1.3 Reset SIM Counter

Use the Reset SIM Counter task to configure a GSM slot's module to restart the recording of time in use.

1. From the HMC navigation pane, expand the **Manage** branch.

2. Click the **Scheduler** sub-branch. The Task Scheduler screen is displayed.

3. From the **Add New Command** dropdown menu, select **Reset SIM Counter**. The Task Scheduler automatically advances to the next screen.

Figure 64. Task Scheduler Reset SIM Counter Screen

4. Configure the task parameters

Slot

Select or clear the checkboxes. Each checkbox represents the GSM card located in the numbered slot counting from the left.

Module

From the Module column, select the module upon which the task will be performed. Only one Module can be selected.

SIM

From the module's SIM dropdown menu, select the SIM card for which the count will be reset.

➡ **Note:** Select All to reset the count on all of the module's SIM cards.

5. Click **Next**. The Set Command screen, with the command syntax, is displayed.

Figure 65. Task Scheduler Set Command Screen

⚠ **Caution:** Clicking menu deletes the new task. The table of schedules tasks is redisplayed.

6. Configure the task's schedule:

   a. Click (calendar icon). A calendar opens in a new browser tab.

➡ **Note:** First, set the time. As soon as you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   b. Enter the time that the command will start.

   c. Enter the date that the command will start. When you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   d. From the Repeat drop-down menu, select either Yes or No.

   e. If the task is configured to repeat, select a **Repeat Period**. The Repeat Period can be either months, days, hours, or minutes.

7. Click **Set Command**. The new Task is displayed in the Task Scheduler screen.

8. Click **Upload Schedule**. The Server activates the schedule according to the defined dates and times.

5.1.4 Set Multi SIM

Use the Set Multi SIM task to create cycles that define when each SIM card is used and after how much time a SIM card is removed from usage.

1. From the HMC navigation pane, expand the **Manage** branch.

2. Click the **Scheduler** sub-branch. The Task Scheduler screen is displayed.

3. From the **Add New Command** dropdown menu, select Set **Multi SIM**. The Task Scheduler automatically advances to the next screen.

Task Scheduler

Set Multi SIM

Slot   ☐ 1   ☐ 2

Module	○ 1 ○ 2 ○ 3 ○ 4
SIM	☐ 1 ☐ 2 ☐ 3 ☐ 4
Switch Period	
Lock Period	

back   next

Figure 66. Task Scheduler Set Multi SIM Screen

4. Configure the task parameters:

Slot

Select or clear the checkboxes. Each checkbox represents the cellular card located in the numbered slot counting from the left.

Module

From the Module row, select the module number on the cellular card upon which the task will be performed. Only one Module can be selected.

SIM

From the SIM row, select the checkbox to include the SIM card in the cycle.

Switch Period

Enter an amount of time measured in minutes that each SIM card is active.

When the period of time expires, the next SIM card become active.

Lock Period

Enter an amount of time measured in minutes after which the SIM cards can no longer be used to place calls.

5. Click **Next**. The Set Command screen, with the command syntax, is displayed.

Figure 67. Task Scheduler Set Command Screen

Caution: Clicking menu deletes the new task. The table of schedules tasks is redisplayed.

6. Configure the task's schedule:

   a. Click _____ (calendar icon). A calendar opens in a new browser tab.

Note: First, set the time. As soon as you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   b. Enter the time that the command will start.

   c. Enter the date that the command will start. When you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   d. From the Repeat drop-down menu, select either Yes or No.

   e. If the task is configured to repeat, select a **Repeat Period**. The Repeat Period can be either months, days, hours, or minutes.

7. Click **Set Command**. The new Task is displayed in the Task Scheduler screen.

8. Click **Upload Schedule**. The Server activates the schedule according to the defined dates and times.

5.1.5 Manual Command

Use the Manual Command task to customize a task and its schedule.

1. From the HMC navigation pane, expand the **Manage** branch.

2. Click the **Scheduler** sub-branch. The Task Scheduler screen is displayed.

3. From the **Add New Command** dropdown menu, select **Manual Command**. The Task Scheduler automatically advances to the next screen.

Figure 68. Task Scheduler Manual Command Screen

Caution: Clicking menu deletes the new task. The table of schedules tasks is redisplayed.

4. Configure the task and its schedule:

   a. Click ▦ (calendar icon). A calendar opens in a new browser tab.

   Note: First, set the time. As soon as you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   b. Enter the time that the command will start.

   c. Enter the date that the command will start. When you click the date, the browser tab closes and the date and time are entered into the Start Time field.

   d. Enter the command. For help with command syntax, contact Hypermedia technical support.

   e. From the Repeat drop-down menu, select either Yes or No.

   f. If the task is configured to repeat, select a **Repeat Period**. The Repeat Period can be either months, days, hours, or minutes.

5. Click **Set Command**. The new Task is displayed in the Task Scheduler screen.

6. Click **Upload Schedule**. The Server activates the schedule according to the defined dates and times.

6 Developer's API

This section defines the API for the Hypermedia SMS PRO Gateway. The API is designed to enable development of third party applications that wish to utilize the Hypermedia SMS PRO Gateway.

Use the developer's API to control the SMS server and send and receive SMS messages using commands over a TCP connection. Typically, this is used to send alarms, warnings, alerts, messages and any other system information that must be delivered quickly to specific individuals.

The SMS Pro Gateway also supports seamless integration with SMPP (Short Message Peer-to-Peer protocol).

6.1 Overview

Following are several points of general importance:

- Development Platforms

  The API is based on a text based protocol over a TCP connection. It is, therefore, platform independent and only requires that the application have access to TCP/IP sockets.

- Configuration

  See the —[Configuration]‖ section for the SMS PRO Gateway configuration screens that are referred to in various parts of this chapter.

- The Protocol

  A TCP connection is used to send requests and receive events from the SMS PRO Gate- way. The default TCP port that is used to connect to the SMS PRO Gateway is 63333.

  The requests, replies, and events are formatted using JSON notation. (More information on JSON can be found at http://www.json.org.) This simplifies use of the SMS PRO Gateway API from any programming language.

- Termination of Lines

  Every line sent to the server should be terminated with a CR LF. All replies and events received from the SMS PRO Gateway are also terminated by a CR LF pair.

6.2 Logging In

To log in to the SMS PRO Gateway:

1. Create a TCP connection to the gateway listening port (default is 63333).
2. Send the following line with the replacement values described in Table 6:
   ```
   {"method":"authentication","server_password":"admin","client_id":"id1"}
   ```

Table 6: Login Message Fields

Field Name	Field Meaning
server_password	Replace the value for the server_password field with the password assigned to the gateway via the SMS server's configuration page of the Hypermedia Management Console.
client_id	Set the client_id field value to an ID that will identify your session. This ID enables you to associate requests with your connection and appears in the CDR records for messages sent during your session.

3. Ensure that the line ends with CR LF.

6.2.1.1 Results

If the supplied password is incorrect, no reply is returned (for security reasons) and—if no correct password is supplied—the connection will be disconnected after a few seconds.

If a correct password is supplied, the SMS PRO gateway will reply with:

```
{"server_password": "admin", "reply": "ok", "client_id":
"id1", "method_reply": "authentication"}
```

At this point you can send valid JSON requests to the SMS PRO Gateway.

Note the following**:**

- If no password is set on the Gateway, no authorization is required and the Gateway is ready to receive requests as soon as the TCP connection is established.

- If another client logs in with the same ID as an existing client, then the new client will cause the disconnection of the old client. A message is sent to each client indicating the disconnection. Therefore, it is recommended that each new client be assigned a unique ID. Note that if no ID is given, a unique ID will be generated for the client by the Gateway.

- For each JSON line sent to the server, any unrecognized fields are returned in the reply with their values.

6.3 SIM Configuration

This section describes available SIM configuration methods.

6.3.1 Getting the Active SIM Configuration

The SIM configuration can indicate a single, local connection between one HGS system and the SMS PRO Gateway to which it is connected. In addition, the SMS PRO Gateway can also connect to multiple HGS systems.

6.3.1.1 Local Connection

To check the configuration status of the SIM ports on all the GSM cards, issue the following command:

```
{"method":"get_sim_config"}
```

The SMS PRO gateway will respond with a JSON reply which contains all the active SIM ports and the routing groups to which they belong. This is illustrated next:

```
{"sim_config": {

      "21#1": {"group": "orange",  "port": "1", "card": "21"},
      "21#2": {"group": "mobile1","port": "2", "card": "21"},
      "21#3": {"group": "orange",  "port": "3", "card": "21"},
      "21#4": {"group": null,      "port": "4", "card": "21"}

    },

"method_reply": "get_sim_config"

}
```

In the above example, four active SIM cards are returned (21#1, 21#2, 21#3, 21#4) where 21#1 means the first SIM port in GSM card at address 21 (hex). This is the far-left slot; the cellular card to its right is at address 22, etc. Also, —orangell is the name of the routing group associated with this SIM. Thus, the reply indicates that:

- There are four active SIM cards in the device
- All of them are in the same GSM card
- The first three SIM cards are associated with specific routing groups ▪ The fourth SIM is not associated with any group.

6.3.1.2 Master/Slave Multiple Connections

The SMS PRO Gateway can connect to multiple HGS systems. This is useful in situations where either a larger SMS capacity is required or where there is an advantage to geographically separating the SIM cards. In these cases, one SMS PRO gateway is the master and controls the other HGS systems. For more information on this, see the —[Slave Managers](#)‖ section.

In the case of a Master/Slave configuration, the Master SMS PRO Gateway's reply to the `get_sim_config` method will return the following:

```
{"sim_config": { "slave_2@21#2": { "sys_name" : "slave_2", "group"
                                    : "4541",
                                    "port" : "2",
                                    "card" : "slave_2@21"

                                  },
                "slave_2@21#3": { "sys_name" : "slave_2",
                                  "group" : "orange", "port" :
                                  "3",
                                  "card" : "slave_2@21"

                                },
                "21#1": { "sys_name" : "master_sys",
                          "group" : null,
                          "port" : "1",
                          "card" : "21"

                        }
              },

"method_reply": "get_sim_config"}
```

In the above example, three active SIM cards are returned (slave_2@21#2, slave_2@21#3 and 21#1). 21#1 means the same as in the previous example, that is, the first SIM port in the GSM card at address 21.

➡ **Note** that in this case, it belongs to the Master SMS PRO Gateway.

The identification of SIM cards that are located on other HGS devices are preceded by **"name@"**. For example, slave_2@21#2 means —the second SIM port in the GSM card at address 21 on a remote HGS device named slave_2‖. The meaning of the group and port parameters remain the same as in the previous example.

The `sys_name` parameter is the unique name of the SMS PRO Gateway on which the SIM is located. On the master SMS PRO Gateway, this will always be `master_sys`. The name assignment of a slave system (slave_2 in the above example) is done using the HMC user interface of the master SMS PRO gateway. This enables assigning an IP of a slave SMS PRO Gateway with a unique system name.

6.3.2 Setting the Active SIM Configuration

Using the `set_sim_config` method it is possible to add or remove SIM cards to the pool of available SIMs and also assign groups to SIM ports. Following are several examples:

6.3.2.1 Example 1:

Add the first SIM in the second GSM card (from the left) to the pool of SIM slots available for sending SMSs:

```
{"method":"set_sim_config",

 "groups":{"22#1": {"port": "1", "card": "22","activ":true} }}
```

The gateway will respond with:

```
{"reply": "ok",

 "groups": {"22#1": {"activ": true, "port": "1", "card": "22"}},

"method_reply": "set_sim_config"}
```

Similarly, sending the above command with the `activ` property set to `false` would remove the SIM from the pool of SIM cards for sending SMSs.

6.3.2.2 Example 2:

Add two SIM ports from the far-left GSM card to the active SIM pool and associate these SIM slots with the groups ―orange‖ and ―TMobile‖ respectively.

```
{"method":"set_sim_config",

 "groups":{"21#2":
```

```
            {"group":"bbb", "port":"2", "card":"21","activ":true},

        "21#3":

            {"group":"ccc", "port":"3", "card":"21","activ":true} }

    }
```

The gateway will respond with:

```
{"reply": "ok",

 "groups":

  {"21#2":

   {"activ": true, "group": "orange", "port": "2", "card": "21"},

"21#3":

   {"activ": true, "group": "TMobile", "port": "3", "card": "21"}},

 "method_reply": "set_sim_config"}
```

The `set_sim_config` method should be used on both master and slave SMS PRO Gateways to set their active SIM cards and assign groups to these cards. On slave systems, the `get_sim_config` method will return the configuration that was set and on a master system it will return the configuration of the master system and all the slave systems, as seen in the Master SMS Gateway PRO's reply example in ―Local Connection‖.

6.3.3 Changing the Routing Group of an Active SIM

It is possible to set or change the routing group an active SIM belongs to by issuing the `set_group` command. For example:

```
{"method":"set_group", "group":"Vodaphone","sim_add":"21#4"}
```

The above command will associate the fourth SIM channel in the far-left cellular card (address 21) with a routing group called ―Vodaphone‖.

Note regarding groups:

If a SIM channel is not associated with a group, it *can* be used by the server to send an SMS that belongs to any group. This means that an SMS targeted for a certain group might also be sent via a SIM channel that is not associated with any group. If an SMS being sent has no group parameter, it will only be sent via SIM channels that are not associated with any group *or*

SIM channels that are associated with a special group named `sms_gen`. Thus, if you wish that an SMS be sent **only** through SIM channels that are associated with the SMS group parameter (and not through SIM channels that have not been assigned a group name) the recommended method is to assign the group name `sms_gen` to all the SIM channels that have no group assigned to them.

6.3.4 Receiving Notification of Configuration Changes

To receive notification each time the active SIM configuration changes, issue the following command:

```
{"method":"register_for_config_change"} And
```

the gateway will respond with:

```
{"reply": "ok", "method_reply":
"register_for_config_change"}
```

Once this is done, each time a SIM is added or removed from the SIM pool, the SMS PRO Gateway will send the following notification:

```
{"notification": "config_change"}
```

At this point, the SMS PRO Gateway should be queried again for the new status of active SIMs using the `get_sim_config` command.

6.4 Sending an SMS

All the following examples send the SMS —hello‖ to the number 6453298.

```
{"number":"6453298", "msg":"hello", "unicode":"5"}

{"number":"6453298", "msg":"hello", "unicode":"5",
"msg_id":3432}

{"number":"6453298", "msg":"6B656C6C6F", "unicode":"0",
"msg_id":3432}
```

The example shown below sends —привет‖, which is the Russian equivalent of —hello‖, to the same number. The JSON representation of —привет‖ is "\u043f\u0440\u0438\u0432\u0435\u0442".

This can be obtained in multiple ways, depending on programming language used. In PYTHON for example, the conversion to JSON representation of the entire API message may done using:

```
json.dumps({"number":"0544331124", "msg":"привет",
"unicode":"5","msg_id":3433})
```

This will return:

```
{"number":"0544331124",
"msg":"\u043f\u0440\u0438\u0432\u0435\u0442",
"unicode":"5","msg_id":3433}
```
which may then be sent to

the gateway to trigger sending the SMS.

The following table displays and defines the fields given in the above example.

Table 7: Fields for Sending an SMS

Field Name	Field Meaning
number	Mandatory. The destination number to which the SMS should be sent.

Field Name	Field Meaning

msg	Mandatory. The message itself, in one of several encoding methods, depending on the value of the `unicode` parameter (below).
unicode	Mandatory. Defines the message format. Can be one of the following values: 0 - `msg` is a hexadecimal representation of a GSM03.38encoded string (can represent up to 160 characters per SMS). 1 - `msg` is a hexadecimal representation of a UCS-2 Unicode string (can represent up to 70 UCS-2 characters per SMS). 3 - `msg` is a JSON string, to be sent to the cellular network using UCS-2 encoding (can contain up to 70 characters per SMS). 4 - `msg` is a JSON string, to be sent to the cellular network using GSM03.38 encoding (can contain up to 160 characters per SMS). 5 - `msg` is a JSON string. The gateway attempts to convert the string to the more compact GSM 03.38 format. However, upon failure to do so, the gateway will attempt to send it in UCS-2. 9 - `msg` is a hexadecimal representation of a string encoded according to the additional parameter `encode_hex`. The gateway attempts to convert the string to the more compact GSM 03.38 format. However, upon failure to do so, the gateway will attempt to send it in UCS-2. 20 - `msg` is a hexadecimal pre-encoded PDU message, to be sent transparently by the gateway to the cellular network. An additional `pdu_len` parameter is required in this mode. 21 - `msg` is a hexadecimal 8-bit message, to be sent transparently as —8-Bit Binary‖ to the cellular network.
msg_id	The ID of this request. Responses related to this message will contain this ID so that the context can be understood by the application. The ID also appears in the SMS CDR. If this field is omitted, the corresponding field in the CDR has a value of —Unknown‖.

encode_hex	Valid only for Unicode = 9 and explained above. The default value of this parameter is —latin-1‖. Additional values are —ascii‖, —utf-16-be‖, —utf-8‖. More platformdependent values may exist.
Field Name	**Field Meaning**
pdu_len	Valid only for Unicode = 20 (see above). Length of the PDU to be sent in bytes (excluding the SMSC address octets).

➡ **Note:** GSM03.38 encoding as used above refers to the default GSM 7-bit alphabet.

Table 8 lists optional fields which can be added to a request.

Table 8: Optional Fields when Sending an SMS

Field Name	Field Meaning
group	A string that defines the SIM group that this message should be sent to. This in effect constrains the set of SIM ports that the SMS can be sent through.
priority	The priority to be given to this message. The priority value is an integer that equals 1 or higher. The lower the number, the higher the priority, meaning that messages whose priority value is lower will be sent before messages with a higher value. *Important note regarding priorities and groups:* The priority is designed to get an SMS out as fast as possible using any available resource. If an SMS is sent to a certain SIM group with a priority, it will go through SIM channels of that group *unless there are messages already queued on that group and other free SIM channels exist in the system*. This means that if there are free SIM channels that belong to another group (that might belong to a different carrier with different pricing), the SMS could be sent via those cards. Since the priority algorithm prefers time to deliver over economy, take great care when sending an SMS with a priority if there are multiple groups in the system.
Field Name	**Field Meaning**

queue_type	There are two queue types used by the SMS PRO Gateway: the regular queue and the master queue. The master queue is meant for circumventing the regular queue if there are urgent SMS requests or bulks to be sent. The SMS PRO Gateway first handles messages in the master queue and only after that queue is emptied does the gateway handle messages in the regular queue. Note that both queues are identical in terms of their attributes (groups and priorities), only that the master queue is handled first if any messages exist in it. If this parameter does not exist in the message, it will be sent to the regular queue. If it does then its value must be —master‖.

send_to_sim	It is possible to bypass the group and priority logic of the SMS PRO Gateway by requesting an SMS to be sent to a specific SIM channel. Below is an example for the syntax of doing this:
	
	`{"number": "4333222","msg":"6B656C6C6F",`
	
	`"unicode":"0","send_to_sim":"22#3"}`
	
	In this example, 22#3 means the third SIM in the second cellular card. This is useful if an application requires its own business logic for using the SIM channels. Note that a separate queue with the highest priority is used when sending to a SIM directly so the message will be sent before any other messages that might have already been queued to the gateway using the gateway's queuing logic (group/priority)

confirmation	If —confirmation‖ is set to —yes‖, then a notification will be sent when the remote party received the SMS. Usage example:
	
	`{"number":"353634643","msg":"6B656C6C6F","unicode":`
	
	`"0","confirmation":"yes"}`
	
	Note that setting the confirmation field overrides the default setting in the SMS configuration screen in the HMC.

The reply for the above message (with only the mandatory fields) would be:

```
{"client_id": "id1", "msg_id": 3433, "number": "6453298",
"retry_num": 0, "unicode": "1", "msg":
"043F04400438043204350442", "reply": "proceeding"}
```

Table 9 displays and defines the reply fields.

Table 9: Reply Fields for Send SMS Request

Field Name	Field Meaning
client_id	The ID of the client who issued the request.
msg_id	The ID of the request.
unicode	The encoding type that was actually used (will be different than the requested value for some of the values).

reply	The status of the message. Possible values are: —**proceeding**‖: The SMS has been queued for sending. —**error**‖: There was an error sending the SMS. In this case, another field named `"error_code"` is used. This field contains the error code for this reply. A detailed list of error codes is available in table Table 14, —Error Codes". Special attention should be given to the error code E8 (232). This indicates that the message queue for the SMS PRO gateway is full and no more messages can be accepted for delivery. In this case, the sending application should wait until the queues are emptied by the server. The amount of time depends on the number of active SIM cards that can deliver the messages. It should be taken into account that the average throughput of four SIM cards (capacity of one cellular card) is about one outgoing SMS per second, though this can vary with different operators or network conditions. —**ok**‖: The SMS was sent successfully. —**confirmation**‖: A confirmation that the SMS has been received by the remote party. In this case another field will exist in the reply named —**confirmation_val**‖ and its value will be the confirmation code received from the network. A detailed list of confirmation codes is available in Table 15, —Confirmation Codes‖. If the reply was either —ok‖ or —error‖, a field named —retry_num‖ will contain the number of attempts made until this result was achieved.
number	The requested destination number.
Field Name	**Field Meaning**
msg	The requested message to be sent.

Table 9b: Additional fields in the reply message

Field Name	Field Meaning
retry_num	The number of retries made prior to successful sending of the message
pdu_num_of_sms	Number of concatenated SMS's used to send the requested message.
card_add	Address of the cellular card through which the message was sent (―21‖ being the far-left slot)
port_num	Number of the cellular port on the card at ―card_add‖ used to deliver the message.
active_sim	The SIM that was used to deliver the message (out of up to 10 SIMs used on a single cellular port, depending on the system configuration).
ccid	The ICCID value of the SIM card through which the message was sent (usually written on the back of the SIM card).

Notes:

1.   The SIM channel through which the SMS will be sent depends on whether a linear or cyclic queue type was set in the SMS PRO Gateway configuration screen.

2.   Additional parameters might exist in the reply message, depending on the gateway's software version and configuration.

Additional SMS Sending Examples

Unicode mode 9:

Using the cp1252 encoding:

```
{"number":"0544331124","msg":"3132330A414243","unicode":"9",
"encode_hex":"cp1252"}
```

Using UTF-16-BE:

```
{"number":"0544331124","msg":"043f04400438043204350442",
"unicode":"9","encode_hex":"utf-16-be"}
```

Unicode mode 5, including all reply messages:

Sending an SMS:

```
{"number":"0544331124",
"msg":"\u043f\u0440\u0438\u0432\u0435\u0442",
"unicode":"5","msg_id":3433} An
```

immediate —proceeding‖ reply:

```
{"client_id": "192.168.123.2042013-12-30 07:31:18.695932",
 "msg_id": 3433, "number": "0544331124", "retry_num": 0,
 "pdu_mode": "yes", "pdu_num_of_sms": 1, "unicode": "1",
"msg": "043F04400438043204350442", "reply": "proceeding"}
```

An —SMS sent‖ reply:

```
{"unicode": "1", "sms_reference_list": [4179], "sim_data":
"3,73,100,100,100,7,50", "config_confirmation": "yes",
"msg_id": 3433, "port_num": "4", "number": "0544331124",
"retry_num": "0", "pdu_mode": "yes", "active_sim": 3,
"pdu_num_of_sms": 1, "sending_time": "00:00:02",
"client_id": "192.168.123.2042013-12-30 07:31:18.695932",
"msg": "043F04400438043204350442", "reply": "ok",
"card_add": "21", "pdu_cnt": 1, "pdu_seq": 1, "ccid":
"89972080091094690670"}
```

And finally, a —delivery receipt‖ reply (if configured to receive one):

```
{"confirmation_final": "yes", "client_id":
"192.168.123.2042013-12-30 07:31:18.695932",
"sms_reference_list": [4179], "sim_data":
"3,73,100,100,100,7,50", "config_confirmation": "yes",
"msg_id": 3433, "port_num": "4", "number": "0544331124",
"retry_num": "0", "pdu_mode": "yes", "active_sim": 3,
"pdu_num_of_sms": 1, "pdu_seq": 1, "unicode": "1", "msg":
"043F04400438043204350442", "reply": "confirmation",
"card_add": "21", "confirmation_val": "0", "pdu_cnt": 1,
"ccid": "89972080091094690670"}
```

Unicode mode 20 (transparent PDU):

```
{"pdu_len":29,"unicode":"20","msg":"0031000A8150320434330000
FF12C83CBC2C6F96C9E930084AAC82CA7838","send_to_sim":"21#1"}
```

(A "number" field may also be inserted above only for CDR logging purposes)

The immediate —proceeding‖ reply:

{"client_id": "127.0.0.12012-01-18 14:58:04.207737",
"pdu_len": 29, "send_to_sim": "21#1", "retry_num": 0,
"number": "PDU", "unicode": "20", "msg":
"0031000A8150320434330000FF12C83CBC2C6F96C9E930084AAC82CA783
8", "reply": "proceeding"}

And the —SMS sent‖ reply:

{"unicode": "20", "pdu_len": 29, "sms_reference_list":
[1172], "sim_data": "1,61,100,100,100",
"config_confirmation": "yes", "port_num": "1",
"send_to_sim": "21#1", "retry_num": 0, "number": "PDU",
"client_id": "127.0.0.12012-01-18 14:58:04.207737", "msg":
"0031000A8150320434330000FF12C83CBC2C6F96C9E930084AAC82CA783
8", "reply": "ok", "card_add": "21", "sending_time":
"00:00:03"}

Unicode mode 21 (8-bit binary):

{"number":"+972544331124","msg":"47736D","unicode":"21","pdu
_dest_port":"8091"}

The immediate —proceeding‖ reply:

{"client_id": "192.168.123.2042013-12-30 07:31:18.695932",
"number": "+972544331124", "retry_num": 0, "pdu_mode":
"yes", "pdu_num_of_sms": 1, "unicode": "21","msg": "47736D",
"reply": "proceeding", "pdu_dest_port": "8091"}

The —SMS sent‖ reply:

{"unicode": "21", "sms_reference_list": [4183], "sim_data":
"3,75,100,100,100,9,50", "config_confirmation": "yes",
"ccid": "89972080091094690670", "port_num":"4", "number":
"+972544331124", "retry_num": "0", "pdu_mode": "yes",
"active_sim": 3, "pdu_num_of_sms": 1, "sending_time":

```
"00:00:02", "client_id": "192.168.123.2042013-12-30
07:31:18.695932", "msg": "47736D", "reply": "ok",
"card_add": "21", "pdu_cnt": 1, "pdu_seq": 1,
"pdu_dest_port": "8091"}
```

And finally, a delivery receipt reply:

```
{"confirmation_final": "yes", "ccid":
"89972080091094690670", "sms_reference_list": [4183],
"sim_data": "3,75,100,100,100,9,50", "config_confirmation":
"yes","port_num": "4", "number": "+972544331124",
"retry_num": "0", "pdu_mode": "yes", "active_sim": 3, "msg":
"47736D", "pdu_num_of_sms": 1, "pdu_seq": 1, "unicode":
"21", "client_id": "192.168.123.2042013-12-30
07:31:18.695932", "reply": "confirmation", "card_add": "21",
"confirmation_val": "0", "pdu_cnt": 1, "pdu_dest_port":
"8091"}
```

6.5 Sending Bulk SMS

To send a large number of SMS with the same message to various destinations, use bulk mode. The following is a sample method for sending SMS in bulk mode:

```
{"method":"start_bulk", "bulk_id": 453, "msg": "6B656C6C6F",
"unicode": "0" "queue_type":"master"}
```

Table 10: Bulk SMS Message Fields

Field Name	Field Meaning
"method":"start_bulk"	Indicates that a new SMS bulk session is requested.
"bulk_id":453	Associates the ID 453 with this bulk. This ID can later be used for additional operations on this bulk.
"msg":"6B656C6C6F"	Associates the message "6B656C6C6F" (hello) with this bulk.

From this point on, when a message is sent to the SMS PRO Gateway with a bulk ID but without a message, the message associated with the bulk ID will be sent in the SMS to the destination number. A message that is part of a bulk will look like this:

```
{"number":"6458965", "bulk_id":453, "msg_id":3212}
```

The above will send the message ―hello‖ to the number 6458965.

Note also the optional ―msg_id‖ field. This should be a unique id. It is useful when a confirmation request is added since this message ID is returned in the confirmation and written to the CDR.

6.5.1 Changing the Priority of Bulk Messages Already Sent

To change the priority of messages already sent to the server, use the method below. This sample changes the priority of bulk ID 453 to priority 4:

```
{"method":"change_priority", "bulk_id":453, "priority":4}
```

6.5.2 Deleting an Entire Bulk

To remove all instances of a bulk message from the server, use the method below. This sample will remove bulk ID 453 from the server. Any existing messages belonging to this bulk that have not been already sent will be deleted.

```
{"method":"delete_bulk", "bulk_id":453}
```

6.5.3 Moving a Bulk or SMS Queued to the Master Queue

The following will move all the messages queued on bulk ID 453 to the master queue (see ―Queue Type‖ in Table 8). If the master queue was empty, then all previous processing of the regular queue will pause and processing of this bulk will begin immediately.

```
{"method":"move_to_master" , "bulk_id":453}
```

6.5.4 Removing a Bulk from the Master Queue

Use the following method to remove a bulk from the master queue and return it to the regular queue:

```
{"method":"remove_from_master", "type":"bulk", "id":4343}
```

6.5.5 Closing a Bulk Session

Following this operation, no more messages can be sent with the ID of this bulk. There are two methods for closing a bulk:

- `"end_bulk"` - this will close a bulk session, but will not delete the bulk until all the pending messages in the bulk have been sent by the gateway. Example:

```
{"method":"end_bulk", "bulk_id":453}
```

- `"stop_bulk"` – this will immediately delete a bulk session, including all pending messages for this bulk. Example:

```
{"method":"stop_bulk", "bulk_id":453}
```

6.6 SMS Event Notifications

It is possible to receive notifications whenever an SMS is sent from the gateway or received by the gateway. When registering for incoming or outgoing SMS notifications, any such event will be sent to the client and will include the full details of the SMS.

The following table shows the commands for registering and unregistering for SMS events:

Table 11: Registering and Unregistering SMS Event Notifications

Command (and gateway's reply)	Effect

`{"method":"register_for_incoming_sms"}`
 	
`{"reply": "ok", "method_reply": "register_for_incoming_sms"}`
	Start receiving CDR notifications for incoming SMS.

`{"method":"register_for_outgoing_sms"}`
 	
`{"reply": "ok", "method_reply":" register_for_outgoing_sms"}`
	Start receiving CDR notifications for outgoing SMS.

`{"method":"unregister_for_incoming_sms"}`
 	
`{"reply": "ok", "method_reply": "unregister_for_incoming_sms"}`
	Incoming SMS CDR notifications will no longer be received.

```{"method":"unregister_for_outgoing_sms"}```
 	
```{"reply": "ok", "method_reply":```
```"unregister_for_outgoing_sms"}```
	Outgoing SMS CDR notifications will no longer be received.

Below is an example of an incoming SMS event notification

```
{"direction": "in", "notification": "cdr", "port_num": "2",
"number": "+972547893166", "datetime": "2009-09-21
15:07:04", "card_add": "21", "message": "GOOD"}
```

The incoming SMS in the next example contains also Unicode characters

```
{"direction": "in", "notification": "cdr", "port_num": "2",
"number": "+972547893166", "datetime": "2009-09-21
15:23:29", "card_add": "21", "message": "Hypermedia
\u05d9\u05d5\u05e4\u05d9"}
```

The following is an example of a notification of an outgoing SMS event (as a result of registering for outgoing SMS notifications):

```
{"direction": "out", "notification": "cdr", "msg_id":
"Unknown", "port_num":"2", "number": "0521111111",
"retry_num": 0, "datetime": "2009-09-17
17:40:21", "result": "Err-0015", "client_id": "232",
"card_add": "21", "message": "GOOD", "sending_time":
"00:00:03"}
```

The following table shows the fields that exist in SMS notification messages and their meaning:

Table 12: SMS Event Notification Fields

Field	Applies to	Meaning
direction	Both incoming and outgoing	Direction of traffic: `"in"` for notification of an incoming SMS, `"out"` for a notification of an outgoing SMS
notification	Both incoming and outgoing	Notification type. For SMS CDR, event notifications will always be of type `"cdr"`.

Developer's API

msg_id	Outgoing only	The message ID that was set for the SMS send request. If no ID was set, the value will be "Unknown".
port_num	Both incoming and outgoing	Which SIM channel number (1 to 4) was used to receive or send the message
number	Both incoming and outgoing	For incoming messages: The CLI of the sender of the SMS (number from which the SMS was sent). For outgoing messages: The DDI of the SMS (the number to which the SMS was sent).

Field	Applies to	Meaning
datetime	Both incoming and outgoing	For incoming messages: The date and time when the SMS was received by the gateway. For outgoing messages: The date and time the message was sent.
result	Outgoing only	"ok" if no errors. The string "Err-" followed by the zero padded error code (a detailed list of error codes is available in Table 14). The string "Confirmation_val-" followed by the confirmation code (see Table 15, —Confirmation Codes‖).
client_id	Outgoing only	The ID of the client who initiated the SMS sending.
card_add	Both incoming and outgoing	The internal address of the slot (in hex). 21 represents the first slot from the left, 22 the second, etc. In a cascaded configuration (two physically connected devices), the first slot from the left of the first device is at address 21 and the first slot from the left of the second device is at address 31.

message	Both incoming and outgoing	The SMS content. If it contains Unicode characters then each of those characters will be represented by the prefix —\u‖ followed by four hexadecimal digits.
retry_num	Outgoing only	The number of attempts that were required to send the message.

6.7 HTTP Notifications

It is possible to receive incoming or outgoing SMS notifications via HTTP. The following two PHP scripts show the HTTP GET parameters that are sent to the URLs for incoming and outgoing SMS respectively (see —URLs for SMS notifications‖).

Note that the variable names are identical in syntax and meaning to the field names in the SMS event notifications (see —SMS Event Notifications‖).

6.7.1 HTTP GET variables for Incoming SMS

```php
<?php
 print "datetime-" . $_GET["datetime" ] . " | ";
 print "number-"   . $_GET["number" ]   . " | ";
 print "message-"  . $_GET["message" ]  . " | ";
 print "card_add-" . $_GET["card_add" ] . " | ";
 print "port_num-" . $_GET["port_num" ] . " | ";
?>
```

6.7.2 HTTP GET variables for Outgoing SMS

```php
<?php
 print "datetime-"     . $_GET["datetime" ]  . " | ";
 print "number-"       . $_GET["number" ]    . " | ";
 print "message-"      . $_GET["message" ]   . " | ";
 print "card_add-"     . $_GET["card_add" ]  . " | ";
 print "port_num-"     . $_GET["port_num" ]  . " | ";
 print "result-"       . $_GET["result" ]    . " | ";
 print "retry_num-"    . $_GET["retry_num" ] . " | ";
 print "msg_id-"       . $_GET["msg_id" ]    . " | ";
 print "client_id-"    . $_GET["client_id" ] . " | ";
 print "sending_time-" . $_GET["sending_time" ];
?>
```

6.8 Queue Related Operations

The following methods address aspects of the queue.

6.8.1 Retrieve Queue Status and Size

To get the status of the queues in the gateway, issue the following method:

```
{"method":"get_q_size"}
```

The following is an example of a queue status reply.

➡ **Note** that the reply is a single line – it has been indented here for clarity.

```
{"que_size":

    { "priority_3": 1,

      "priority_no":

        {"Orange": 2, "Verizon": 0, "Cellcom": 2, "total_len": 4},

      "priority_1": 1 },

 "method_reply": "get_q_size"}
```

The reply shows the number of queued messages per each priority. Messages that were sent with no priority (the default) appear under the `"priority_no"` field. Note that only `"priority_no"` elaborates how many messages are queued for each group as well as the `"total_len"` field which holds the sum of messages queued without priority.

The group details do not exist for other priorities since, as explained (see the ―priority‖ field on Table 96), there is no guarantee that a prioritized message will use the group that it was sent to. The priority is a best effort mechanism that uses the specified group only if it has free SIM channels or if no other SIMs are available.

If the current queue is the master queue then the following additional pair `"queue_type":"master"` will also appear in the JSON reply.

6.8.2 Deleting Queues

To remove all pending messages from the master queue, use the following method:

```
{ "method":"delete_queue","queue_type":"master" }
```

To remove all pending messages from the regular queue, use the following method:

```
{"method":"delete_queue"}
```

WARNING: All messages kept in the queue will be lost.

6.9 Pausing and Continuing the Gateway Operation

To cause the Gateway to stop sending messages, regardless of which queue they were added to, use the following method:

```
{ "method":"pause_server" }
```

The gateway will continue to accept requests to send out messages, but the messages will just accumulate on the queue.

To cause a Gateway that was paused using the `pause_server` method to resume sending messages pending in its queue, use the following method.

```
{ "method":"run_server" }
```

Important Note: Both the `pause_server` and the `run_server` commands will work only if the SMS Gateway PRO's status is set to —**Scheduled"** in the configuration page.

6.10 HTTP API

From version 2.0, the SMS PRO Gateway supports an HTTP API. This API is based on the JSON API described in previous sections. The parameters used are the same parameters as the JSON API, but instead of being encoded in JSON syntax, they are encoded as an HTTP GET or POST request.

The set of available HTTP commands is the same as the set of flat JSON commands, that is, all the JSON requests that do not have an inner hierarchy.

Unlike the JSON API, The HTTP API is not session-based and therefore does not require registration and/or logging in. Instead, each command sent requires an additional `server_password` parameter which specifies the password of the SMS PRO Gateway. This password is the same as the password needed for the JSON authentication command described in the —[Logging In](#)‖ section.

6.10.1 Sending an SMS Using HTTP

The following example shows how to send an SMS.

When using the HTTP API, the URL must be sent in Unicode UTF-8. The SMS PRO Gateway expects this format and converts it to the format in which the SMS will be sent (either UCS-2 or GSM 03.38).

The example sends a —Hello‖ message to a mobile phone whose number is 6453298 using HTTP via an SMS PRO Gateway located at IP address 192.168.0.2:

```
http://192.168.0.2/cb/sms_http.php?
server_password=admin&msg=Hello&number=6453298
```

Notes:

- To send the message via a specific SIM card, add `&send_to_sim=21#1` after the number. The parameters indicate the card number (21) and the SIM number (1) on that card.

- The HTTP parameters above correspond to the JSON command to send an SMS as shown in the first example in the —[Sending an SMS](#)‖ section, that is:

  {"**number**":"6453298", "**msg**":"hello"}

- If the unicode field (see Table 7, —Fields for Sending an SMS‖) is omitted—as in the above example—the SMS Gateway PRO will use a default value of 5, i.e. attempt to convert the message to GSM 03.38, and upon failure to do so will send the message using UCS-2.

Developer's API

- The **server_password** value is the same as that of the server_password value that would have been set to log-in via the JSON authentication command (see the —[Logging In](#)‖ section).

6.10.2 HTTP API Responses

Table 13 lists the possible responses to an HTTP SMS request:

Table 13: Replies for an HTTP SMS Request

Reply	Explanation
ERROR: *<description>*	Returned if an error is encountered, where *<description>* is a textual description of the nature of the error.
PROCEEDING	Returned when the command was successfully delivered to the SMS PRO Gateway and is in the process of being handled. For example, this is returned upon a successful submission of a send SMS request.
METHOD_REPLY *<JSON content>*	Returned when the command requests information that has a hierarchal structure, for example, the `get_sim_config` command. In this case, *<JSON content>* would contain the same reply which would have been returned had the command been issued using the JSON API.

6.11 CDR Support

Following are the methods for obtaining SMS CDR-related information.

6.11.1 CDR Files

The SMS PRO gateway writes SMS CDR in two files – one contains the records of incoming messages and the other stores records of outgoing messages.

These files can be viewed and downloaded from the HMC on the SMS CDR page, as shown below:

SMS CDR Files

File Name (click to download)	Last Modified	Size	Actions
SMS_IN_20131021.log.zip	21/10/2013 20:08	319 bytes	delete
SMS_IN_20131022.log.zip	22/10/2013 21:48	342 bytes	delete
SMS_IN_20131105.log.zip	05/11/2013 18:40	329 bytes	delete
SMS_IN_20131117.log.zip	17/11/2013 17:59	319 bytes	delete
SMS_IN_20131124.log.zip	24/11/2013 12:17	303 bytes	delete
SMS_IN_20131208.log.zip	08/12/2013 15:16	320 bytes	delete
SMS_IN_20131223.log.zip	23/12/2013 18:21	321 bytes	delete
SMS_IN_20131224.log.zip	24/12/2013 19:07	324 bytes	delete
SMS_OUT_20100914.log.zip	14/09/2010 14:08	255 bytes	delete
SMS_OUT_20100915.log.zip	15/09/2010 11:03	252 bytes	delete
SMS_OUT_20100930.log.zip	30/09/2010 17:36	259 bytes	delete
SMS_OUT_20101003.log.zip	03/10/2010 18:47	481 bytes	delete
SMS_OUT_20101020.log.zip	20/10/2010 15:42	248 bytes	delete

The format of a call record line for an incoming SMS is as follows:

```
2009-08-19 18:11:37|24|1|+972111111111|Thanks|OK
```

The table below shows the meaning of the above fields

Field	Meaning
2009-08-19 18:11:37	Date and Time when message arrived
24	Address of cellular card message arrived on (in this case card 24, which means the fourth card from the left).
1	Module number on above card which received the message (in this case module 1).
+4423143012	The mobile phone number of the sender of the SMS

Thanks	The message body
OK	Status code. Possible values are *OK*, *Err*, *Confirmation*

The format of a call record for an outgoing SMS is as follows:

```
2009-08-19 18:11:37|24|1|+972111111111|Thanks|OK|0|
Unknown|192.168.123.82009-08-19 18:11:32.050555|00:00:04
```

6.11.2 CDR MySQL Support

The PC-based version of the HG7000 line of products also supports using an external MySQL database to store incoming and outgoing SMS events. The MySQL connection details should be entered in the relevant fields on the SMS Server Configuration page (see MySQL Host).

➡ Note: In order to support storing messages of a non-PC-based HG7000 gateway on a MySQL database, an external application or script can register to receive SMS event notifications and write the event data to the MySQL (or any other) database.

Two MySQL tables are created by the SMS PRO gateway for the SMS records – one for incoming messages and another for outgoing messages. The schema of the tables is as follows:

```
CREATE TABLE outgoing_sms( date_ DATE , time_ TIME ,
number TEXT(30) , msg TEXT(200) , card_add INT ,
port_num INT , result TEXT , retry_times INT ,  msg_id
TEXT , client_id TEXT(50) ,sending_time TIME)

CREATE TABLE incoming_sms( date_ DATE , time_ TIME ,
number TEXT(30) , msg TEXT(200) , card_add INT ,  port_num
INT)
```

The result field contains the result of the outgoing SMS. If an error occurs the field will contain the string "Err-" followed by the error code (detailed in Table 14). If an SMS receipt is requested, the field will contain the string "Confirmation_val-" followed by the SMS confirmation return code (detailed in Table 15).

6.12 Error and Confirmation Codes

The following two tables list the error and confirmation codes that can be returned within SMS replies or notifications.

Table 14: Error Codes

Code (Dec)	Code (Hex)	Meaning
8	008	Operator determined barring. This cause indicates that the MS has tried to send a mobile originating short message when the MS's network operator or service provider has forbidden such transactions.
10	00A	Call barred. This cause indicates that the outgoing call barred service applies to the short message service for the called destination.
21	015	Short message transfer rejected. This cause indicates that the equipment sending this cause does not wish to accept this short message, although it could have accepted the short message since the equipment sending this cause is neither busy nor incompatible.
27	01B	Destination out of service. This cause indicates that the destination indicated by the Mobile Station cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signaling message was unable to be delivered to the remote user; e.g., a physical layer or data link layer failure at the remote user, user equipment offline, etc.
28	01C	Unidentified subscriber. This cause indicates that the subscriber is not registered in the PLMN (i.e. IMSI not known).

29	01D	Facility rejected. This cause indicates that the facility requested by the Mobile Station is not supported by the PLMN.
30	01E	Unknown subscriber. This cause indicates that the subscriber is not registered in the HLR (i.e. IMSI or directory number is not allocated to a subscriber).
31	01F	Normal unspecified. The GSM engine refused to send the message but no reason was stated. Note that this can also be the result of a message that was

Code (Dec)	Code (Hex)	Meaning
		recently sent to the card, before a reply was received for the previous message.
34	022	Module Error. Module has either no SIM or no reception, is faulty or is still handling the sending of a previous message.
38	026	Network out of order. This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time; e.g., immediately reattempting the short message transfer is not likely to be successful.
41	029	Temporary failure. This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time; e.g., the Mobile Station may wish to try another short message transfer attempt almost immediately.
42	02A	Congestion. This cause indicates that the short message service cannot be serviced because of high traffic.
47	02F	Resources unavailable, unspecified. This cause is used to report a resource unavailable event only when no other cause applies.
50	032	Requested facility not subscribed. This cause indicates that the requested short message service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting networks.

69	045	Requested facility not implemented. This cause indicates that the network is unable to provide the requested short message service.
81	051	Invalid short message transfer reference value. This cause indicates that the equipment sending this cause has received a message with a short message reference which is not currently in use on the MS-network interface.
95	05F	Invalid message, unspecified. This cause is used to report an invalid message event only when no other cause in the invalid message class applies.
96	060	Invalid mandatory information. This cause indicates that the equipment sending this cause has received a message where a mandatory information element is missing and/or has a content error (the two cases are indistinguishable).

Code (Dec)	Code (Hex)	Meaning
97	061	Message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.
98	062	Message not compatible with short message protocol state. This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the short message transfer state.
99	063	Information element non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

102	066	Timer expired. Sending failed due to a timeout, and during this time the GSM network didn't return any specific error code.
111	06F	Protocol error, unspecified. This cause is used to report a protocol error event only when no other cause applies.
127	07F	Interworking, unspecified. This cause indicates that there has been interworking with a network which does not provide causes for actions it takes; thus, the precise cause for a message which is being sent cannot be ascertained.
128	080	Telematic interworking not supported.
129	081	Short message Type 0 not supported.
130	082	Cannot replace short message.
143	08F	Unspecified TP-PID error.
144	090	Data coding scheme (alphabet) not supported.
145	091	Message class not supported.
159	09F	Unspecified TP-DCS error.
160	0A0	Command cannot be auctioned.

Code (Dec)	Code (Hex)	Meaning
161	0A1	Command unsupported.
175	0AF	Unspecified TP-Command error.
176	0B0	TPDU not supported.
192	0C0	SC busy.
193	0C1	No SC subscription.
194	0C2	SC system failure.
195	0C3	Invalid SME address.
196	0C4	Destination SME barred.
197	0C5	SM Rejected-Duplicate SM.
198	0C6	TP-VPF not supported.

199	0C7	TP-VP not supported.
208	0D0	D0 SIM SMS storage full.
209	0D1	No SMS storage capability in SIM.
210	0D2	Error in MS.
211	0D3	Memory Capacity Exceeded.
212	0D4	SIM Application Toolkit Busy.
213	0D5	SIM data download error.
224	0E0	Card reply timeout error **(SMS PRO proprietary code)**.
225	0E1	SIM reply timeout error **(SMS PRO proprietary code)**.
226	0E2	Missing SIM **(SMS PRO proprietary code)**.
227	0E3	The number was blocked by the ACR rules **(SMS PRO proprietary code)**.
228	0E4	Timeout receiving a reply from the ACR **(SMS PRO proprietary code)**.
229	0E5	Timeout attempting to connect to ACR **(SMS PRO proprietary code)**.
230	0E6	An invalid format was given as the destination number **(SMS PRO proprietary code)**.
231	0E7	No route was found by the ACR for the destination number **(SMS PRO proprietary code)**.
232	0E8	Gateway message queue is full **(SMS PRO proprietary code)**.

Code (Dec)	Code (Hex)	Meaning
232	0E9	No matching group found for message **(SMS PRO proprietary code)**.
240	0F0	SMPP: Invalid ESME Password **(SMS PRO proprietary code)**.
241	0F1	SMPP: Bind Failed **(SMS PRO proprietary code)**.

242	0F2	Message is too long **(SMS PRO proprietary code)**.
243	0F3	Invalid message format, for example: content does not match encoding type **(SMS PRO proprietary code)**.
255	0FF	Unspecified error cause.
300	12C	ME failure.
301	12D	SMS service of ME reserved.
302	12E	Operation not allowed.
303	12F	Operation not supported.
304	130	Invalid PDU mode parameter.
305	131	Invalid text mode parameter.
310	136	SIM not inserted.
311	137	SIM PIN required.
312	138	PH-SIM PIN required.
313	139	SIM failure.
314	13A	SIM busy.
315	13B	SIM wrong.
316	13C	SIM PUK required.
317	13D	SIM PIN2 required.
318	13E	SIM PUK2 required.
320	140	Memory failure.
321	141	Invalid memory index.
322	142	Memory full.
330	14A	SMSC address unknown.
331	14B	No network service.
332	14C	Network timeout.
340	154	NO +CNMA ACK EXPECTED.

Code (Dec)	Code (Hex)	Meaning
500	1F4	Unknown error.
512	200	MM establishment failure.
513	201	Lower layer failure.
514	202	CP error.

Table 15: Confirmation Codes

Code (Dec)	Code (Hex)	Meaning
0	00	Short message received by the SME.
1	01	Short message forwarded by the SC to the SME but the SC is unable to confirm delivery.
2	02	Short message replaced by the SC.
3-15	03-0F	Reserved.
16-31	10-1F	Values specific to each SC.
Temporary errors, SC still trying to transfer SM.		
32	20	Congestion.
33	21	SME busy.
34	22	No response from SME.
35	23	Service rejected.
36	24	Quality of service not available.
37	25	Error in SME.
38-47	26-2F	Reserved.
48-63	30-3F	Values specific to each SC.
Permanent errors, SC is not making any more transfer attempts.		
64	40	Remote procedure error.
65	41	Incompatible destination.
66	42	Connection rejected by SME.
67	43	Not obtainable.
68	44	Quality of service not available.
69	45	No interworking available.
70	46	SM Validity Period Expired.

Developer's API

71	47	SM Deleted by originating SME.
72	48	SM Deleted by SC Administration.
73	49	SM does not exist. The SM may have previously existed in the SC but the SC no longer has knowledge of it or the SM may never have previously existed in the SC.

Code (Dec)	Code (Hex)	Meaning
74-79	4A-4F	Reserved.
80-95	50-5F	Values specific to each SC.
Temporary errors, SC is not making any more transfer attempts.		
96	60	Congestion.
97	61	SME busy.
98	62	No response from SME.
99	63	Service rejected.
100	64	Quality of service not available.
101	65	Error in SME.
102-105	66-69	Reserved.
106-111	6A-6F	Reserved.
112-127	70-7F	Values specific to each SC.

7 Troubleshooting

Table 16. Power

Display	Problem	Solution
System does not start up	No power to the unit	Connect power cables
Alarm sounds every time the system boots up	When a dual power supply is used, one power unit is not functioning or only one power unit is present	Replace faulty power unit. Add a power unit.

Table 17. Cellular Cards

Display	Problem	Solution
No sync. with net-work (Green LED is off)	Antenna is not located properly	Position the antenna in a place with better reception.
No sync. with net-work (Green LED blinks)	No SIM card	Put a working SIM card in the appropriate channel
Error LED (Red) is blinking	Card is faulty	Reinsert the card and restart the system. If problem continues replace the card.
Ready LED (Yellow) does not light	Card is either not inserted correctly, or faulty	Reinsert the card and restart the system. If problem continues replace the card.

Table 18. MG Card

Display	Problem	Solution
Error LED (Red) is blinking (50% duty cycle, not twinkling)	Card is faulty	Reinsert the card and restart the system. If problem continues replace the card.
Ready LED (Yellow) does not light	Card is either not inserted correctly, or faulty	Reinsert the card and restart the system. If problem continues replace the card.