



G4FlashNet User Guide

SECURITY MANAGEMENT SYSTEM

9600-0593

© G4S Technology Limited 2012

All rights reserved. No part of this publication may be reproduced in any form without the written permission of G4S Technology Limited.

G4S Technology Limited cannot be held liable for technical and editorial omissions or errors made herein; nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference. In which case, the user will be required to correct the interference at his own expense.

**G4FlashNet User Guide
(9600-0593)**

Issue 1.1 – 8th March 2012

Applies to version 7.0 or later of the SMS Software, until superseded by a later issue of the manual.

All trademarks acknowledged.

Microsoft, Windows and Active Directory are registered trademarks of Microsoft Corporation.

Contents

About this Guide	ii
Chapter 1: Introduction.....	1
Overview of G4FlashNet	1
Software Installation and Licensing	1
Chapter 2: Using G4FlashNet	2
Selecting a Node	2
Configuring the Node's Connectivity	3
Connecting Through a Firewall	4
Upgrading Firmware.....	5
Remote Node Control.....	5
Encryption	6

About this Guide

This guide provides the following:

- A brief overview of the G4FlashNet tool.
- How to use G4FlashNet to configure EN-1DBC and EN-DBU nodes.

This guide is intended to be used by:

- Staff who are responsible for configuring EN-1DBC and EN-DBU nodes.

Chapter 1: Introduction

Overview of G4FlashNet

G4FlashNet is a software tool that enables users to configure EN-1DBC and EN-DBU units. Users may configure connectivity information, perform firmware upgrades, remote control the node, and enable encryption.

Whilst nodes can be configured within the SMS software, certain functionality such as the ability to perform firmware upgrades is not provided. For this, G4FlashNet is required.

Software Installation

G4FlashNet is a stand-alone utility that may be run independently from the SMS software. No additional SMS software or licenses need to be installed in order to use G4FlashNet.

Chapter 2: Using G4FlashNet

This chapter describes how to configure nodes using the G4FlashNet tool.

Selecting a Node

For most network configurations, G4FlashNet will automatically locate any nodes on your network and populate the drop down list found at the top of the tool (Figure 1). Simply select the node you wish to configure to proceed.

The screenshot shows the G4FlashNet application window. At the top, the 'Located Nodes (2)' drop-down list is highlighted, showing a selected node with the following details: MAC=00-15-bd-00-36-cc, HC=1002, 24430 03.63, and 1DBC (IP reader) STD APP. Below this, the 'Update Nodes' button is visible. The 'IP Information' section contains fields for MAC Address (00-15-BD-00-36-CC), Current IP Address (10.234.2.40), New IP Address, Gateway IP Address (10.234.3.252), Subnet Mask (255.255.252.0), Network Name (EN1DBC_00_36_CC), Primary Port number (3001), Host IP Address from Node (0.0.0.0), PC checkbox, Secondary Host IP Address (0.0.0.0), PC checkbox, and Rem Conn Value (Secs, 0 = Off). The 'Firmware Versions' section shows Boot (24431 03.63 - 1DBC (IP reader) BOOT APP) and Application (24430 03.63 - 1DBC (IP reader) STD APP). The 'Upgrade filenames and details' section has a file path (M:\Releases\Firmware\1DBC\v3.63) and buttons for Browse, Upgrade, and a radio button for Upgrade to a new APPLICATION. The 'Remote Node Control' section has buttons for Warmstart, Coldstart, and Reset IP, and a checkbox for Use Direct IP addressing (Care!). The 'Encryption' section has a text field and a Send button. At the bottom, the Hardware code (1002) and Distributor code (1) are displayed, along with a Help button.

Figure 1- G4FlashNet (Located Nodes drop-down list highlighted)

A count of all the nodes currently found appears in brackets next to the *Located Nodes* label (in Figure 1, the number of nodes found is 1). G4FlashNet will automatically add newly connected nodes to the list, provided the Update Nodes button is left selected (default). If the button is de-selected the program will not scan the network for further nodes.

Alternatively, you may want to connect to a node directly if you know its IP address; for example, if your network configuration prevents G4FlashNet from automatically finding nodes. Directly connecting to a node can be done by selecting the *Use Direct IP addressing* check-box as shown in Figure 2. In most situations, using the drop down list is preferred.

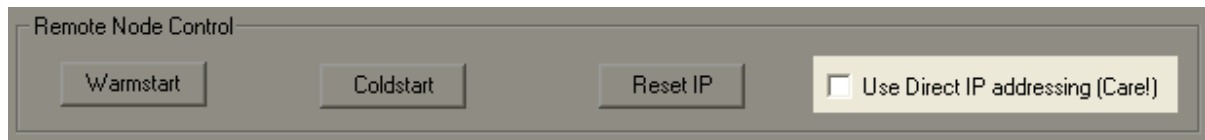


Figure 2 - Use Direct IP Addressing

Configuring the Node's Connectivity

Once a node has been selected you will be able to configure it. The first section of G4FlashNet allows you to configure a node's IP settings (Figure 3).

Figure 3 - Connectivity Information

The fields and their meanings are described below.

- **MAC Address** – displays the node's MAC address. It is populated automatically on node selection and is not configurable.
- **Current IP Address** – displays the node's current IP address. It is populated automatically on node selection.
- **DHCP** – enables the node to use DHCP when checked.
- **New IP Address** – used to specify a new IP address for the node.

-
- **Gateway IP Address** – used to specify the default network gateway’s IP address. This field is populated automatically on node selection, but may be edited by the user.
 - **Subnet Mask** – used to specify the subnet mask of the network to be used by the node. This field is populated automatically on selection, but may be edited by the user.
 - **Network Name** – used to specify the unique network name of the node. This field is populated automatically on selection, but may be edited by the user.
 - **Port Number** – the port used to communicate with the SMS software. This is set to 3001 by default and should not be changed unless instructed by Technical Support.
 - **Host IP Address (Primary)** – the IP address of the primary SMS server or client the node should connect to. Unless the node must establish the connection to the SMS software, this may be left as the default IP address (0.0.0.0). Please see *Connecting Through a Firewall* for more information.
 - **PC (checkbox)** – populates the corresponding *Host IP Address* field (primary or secondary) with the IP address of the current machine.
 - **Rem Conn Value (Remote Connection Value)** – how frequently a node should try reconnecting to the SMS server in the event of a connection failure. If your SMS server and nodes are not separated by a firewall this may be left as 0 (off).
 - **Host IP Address (Secondary)** – the IP address of the secondary (or backup) SMS server or client the node should connect to if it is unable to connect to the primary Host IP Address. This feature is only supported by certain versions of the SMS software and should be set to 0.0.0.0 in most circumstances. Please see *Connecting Through a Firewall* for more information.
 - **Configure** – must be pressed to send any changes made in G4FlashNet to the node. Once pressed, you may need to re-select the node from the drop down list if you want to configure it further.

Connecting Through a Firewall (only available with specific Symmetry software)

In order to manage nodes in the SMS software, a connection must be established between the two. By default, the connection is made *by* the SMS software *to* the nodes. However, certain network configurations may prevent this from happening. For example, if a node is situated behind a firewall, the connection mechanism must be reversed. That is, the connection is made by the node to the SMS software.

To be able to do this, the nodes must know the IP address of the SMS software they are to connect to. This can be set through G4FlashNet by entering the IP address in the *Primary Host IP Address* field. If you are running G4FlashNet on the same machine that runs SMS host you want to connect to, you may simply check the box named “PC”. This will populate the *Host IP Address* field with the IP address of the machine currently running the tool.

Some sites may have a secondary or backup host, which can be used in the event of the primary host failing. If the node is unable to connect to the primary host, it will attempt to connect to the secondary host. Its IP address should be entered in the *Secondary Host IP Address* field. If a secondary host is not present in your setup you may set this field to 0.0.0.0. Please note, this functionality is only provided by certain versions of the SMS software.

In the event of a failed connection attempt to either the primary or secondary host, the node will wait for a specified period of time before attempting to re-connect. This wait time can be set via the *Rem Conn Value* field.

Upgrading Firmware

G4FlashNet may be used to upgrade a node's firmware. The second and third sections (Figure 4) of the tool allow you to view the current firmware version and upgrade if necessary.

Figure 4 - Firmware Information

To upgrade a node's firmware simply use the *Browse* button to locate the folder where the new firmware files are stored. Then select the correct file from the drop down list, select whether you are upgrading to a new application or boot, and finally, press *Upgrade*. Under normal circumstances, only the Application firmware should be upgraded. Only when a valid firmware file has been selected will the Upgrade button be enabled.

In the case where you want to upgrade the Boot and Application firmware, it is recommended that the Boot should be upgraded first.

The upgrade process should complete within 60 seconds. G4FlashNet will notify you upon completion. You may need to re-select the node from the drop-down list after the upgrade has completed if you want to configure the node further.

Remote Node Control

G4FlashNet supports the ability to remotely control a node (Figure 5). Through the tool you are able to remotely restart a node, or reset its IP address to the default. If any of these commands are used, it may be necessary to re-select the node from the drop down if further configuration is needed.

Figure 5 - Remote Node Control

The buttons and their meanings are described below:

- **Warmstart** – Restarts the node without resetting any configuration details. Works as if the reset button on the node has been pressed.
- **Coldstart** – Restarts the node and resets its configuration database (but not its network settings). Works as if the reset button on the node has been held down for 10 seconds.
- **Reset IP** – Restarts the node and resets its connectivity information to the default. Works as if the node has been warm-started three times in 30 seconds.
- **Use Direct IP addressing** – Described in section *Selecting a Node*.

Encryption

G4FlashNet allows you to encrypt the connection between the node and the SMS software. G4FlashNet supports AES encryption at key sizes of 128 bits (32 characters), 192 bits (48 characters), or 256 bits (64 characters).

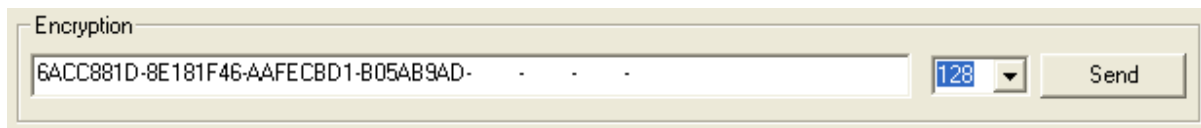


Figure 6 - 128bit Encryption Key Example

To enable encryption, enter a key of the desired size into the text field, select the key size from the drop down list and press *Send* (Figure 6). G4FlashNet will warn you if the key entered is not long enough for the key size selected.

Encryption keys are made up of the hexadecimal characters 0 – 9 and A – F. G4FlashNet will not allow you to enter other characters.

G4FlashNet will inform you if the node is already encrypted by setting the key size drop-down to the size currently used by the node. For example, if you select a node that already has 128-bit encryption applied, the key size drop-down will select 128 by default.

To remove encryption from an already encrypted node you must enter the same key that was used to encrypt the node and select “None” from the drop down list and then press *Send*.

G4FlashNet will carry out the encryption in a matter of seconds and notify you upon completion.

Warning: You will be unable to communicate with the node through the SMS software or change the encryption key if you do not know the currently used key. It is therefore important to keep a secure record of the key used to encrypt a node.