

MQ03-4I & MQ03 LTE-M Global Sim Universal communicators

Installation & Configuration Guide



- Μετάδοση LAN/GPRS 2G, LTE-M
- 4 Είσοδοι / 2 Έξοδοι
- Μετάδοση (polling) έως και ανά 20 sec
- Up/Downloading μέσω Tip/Ring σε πίνακες συναγερμού
GE (Caddx), Honeywell (Vista), DSC (Power), Paradox, Texecom, Teletek
- Εφαρμογή τελικού χρήστη iPhone/Android με push notification
(σπλισμός/αφσπλισμός, λήψη σημάτων realtime)
- Εφαρμογή εγκαταστάτη iPhone/Android για απομακρυσμένη διαμόρφωση
της συσκευής.

Πιστοποιήσεις:

EN-50131-1:2006, EN-50136-1, EN-50136-2-1:21998 SP5 (ATS-5)

Contents

Contents.....	1
Safety Instructions. Limited Liability and Manufacturer Warranty	3
General operating principles of MQ03 GSM/GPRS communicators	3
Key features and benefits.....	3
Different options to connect to alarm panels	4
Device Installation guide.....	4
Mounting	4
Configuration of terminals of MQ03-4I-DTMF GPRS Communicator.....	4
Device Configuration Guide.....	4
Your administrative tools – web site and mobile application	4
Most frequently used scenarios	4
Searching for devices.....	5
Viewing information about a specific controller	5
Alarm settings of the controller	6
Reporting to Central Monitoring Station (CMS)	6
Configuring the Site Number	6
Configuring different Site Numbers for different partitions	7
Reporting to Central Monitoring Station	7
Configuring the messages generated by the MQ03 communicators itself	7
Configuring periodic test messages.....	7
Programming messages from the digital inputs.....	7
Low battery and Mains power outage messages	7
Connection Lost message	7
Communication Channel messages.....	7
Jamming message.....	8
Alarm settings templates	8
SIM card assignment	8
Viewing history of events sent from a device	8
Connecting alarm panels via the DTMF dialer.....	8
Wiring the panel to the communicator	8
Guidelines for configuring the alarm panel.....	8
Configuring the working mode of the DTMF decoder	8
Account number reporting modes	9
Connecting alarm panels via the serial port	9
Selecting the type of the alarm panel	9
Configuring Teletek Eclipse series	10
Configuring Paradox Family panels	10
Configuring Texecom Premier & Elite panels.....	10
Configuring Remote Control of the panel.....	10
Configuring the Keyswitch option	10
Granting remote access to users	11
Technical details MQ03	11

Safety Instructions.

Limited Liability and Manufacturer Warranty

Please read and follow these safety instructions in order to maintain safety of operators and people around:

- ✓ GSM/GPRS communicators MQ03 (the Device) contain a radio transceiver operating in GSM 850/900/ 1800/1900 bands.
- ✓ Do not use the Device with medical devices, or where it can interfere with other devices and cause any potential danger.
- ✓ Do not expose the Device to high humidity, chemical environment or mechanical impacts.
- ✓ Do not use the Device in hazardous environment. Don't store or install the Device in overheated, dusty, wet or overcooled places.
- ✓ The Device is mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel. Don't disassemble or refit the Device. Do not attempt to personally repair it.
- ✓ Mains power must be disconnected before any installation or tuning work starts. The device installation or maintenance must not be done during stormy conditions.
- ✓ The device must be powered by DC 7-18V, 400mA power supply.
- ✓ Blown fuses or any other components of the Device must not be replaced by the user.
- ✓ Keep the Device dry. Any liquid, i.e. rain, moisture, may destroy or damage the inside circuitry.
- ✓ Handle carefully. Don't vibrate or shake it violently.
- ✓ Clear the Device with a piece of dry cloth. Don't clean in chemicals, detergent.
- ✓ Please read the user manual carefully before installation and operation of the Device. Otherwise, it may not work properly or be destroyed.

Limited Liability: The user agrees that despite the Device could reduce the risk of fire, theft, burglary or other dangers, it does not guarantee against such events. **ADESCO.** will not take any responsibility regarding personal, property or revenue loss while using the Device. **ADESCO.** responsibility according to local laws does not exceed value of the purchased system. **ADESCO.** is not affiliated with GSM operators providing cellular services, therefore is not responsible for network services, coverage or its operation.

Manufacturer Warranty: The Device carries a non-transferable hardware limited warranty by the manufacturer **M2M / ADESCO.** This warranty does not cover any postal or labor costs for the removal and reinstallation of the Device. This warranty does not cover any subscriber agreements or failure of services provided under the terms of such subscriber agreements, or failure of cellular, GPRS, LAN or other related networks functions and services. The warranty does not apply to any Device that has been modified or used in a manner contrary to its intended purpose and does not cover damage to the Device caused by installation or removal of the Device or any of its components. This warranty is voided if the Device has been damaged by improper maintenance, SIM card removal, accident or unreasonable use, negligence, acts of God, neglect, improper service or other causes not arising out of defect in materials or construction. This warranty does not cover the elimination of externally generated static or noise, or the correction of antenna problems or weak signal reception, damage to software, accessories or alarm system external components, cosmetic damage or damage due to negligence, misuse, abuse, failure to follow operating instructions, accidental spills or customer applied cleaners, damage due to environmental causes such as floods, airborne fallout, chemicals, salt, hail, windstorms, moisture, lightning or extreme temperatures, damage due to fire, theft, loss or vandalism, damage due to improper storage and connection to equipment of another manufacturer, modification of existing equipment, faulty installation or short circuit. In no event will **ADESCO.** be liable for any incidental, special or consequential damages (including loss of profits), and the Client shall have no claim against **ADESCO.** for termination of contracts, indemnification, compensation for loss of customers, loss of profits, prospective profits, distribution rights, market share, goodwill, investments made or any similar losses that may result from any faults in the operation of the Device and the services provided by **ADESCO.**

General operating principles of MQ03 GSM/GPRS communicators

This communication solution is a complete communication platform for data transfer from alarm systems at remote sites to Central Monitoring Stations (CMS) or end-user equipment (smart phones, tablets, PCs, and etc.). The platform allows bi-directional data transmission by using GPRS network and SMS messaging. The platform consists of hardware devices (such as MQ03 GSM/GPRS communicators) and Cloud Infrastructure Service (CIS). The CIS can be provided and supported either by **ADESCO.** or by its authorized local partners. The connection between the Device and any security alarm system is via digital inputs, serial port, or telephone line emulation with DTMF decoding. The GSM/GPRS communicators MQ03 maintain permanent connection to the Cloud Infrastructure Service. The CIS performs several administrative tasks, such as to constantly monitor the connections with all Devices; to send commands and queries to the Devices in real time (e.g. to retrieve the GSM signal level or the mains power voltage); to perform device configuration tasks and remote firmware updates; to distribute the alarm events to different end-user equipment and/or to CMS; and etc. In a scenario when the alarm system is monitored by a CMS, the CIS receives all events from the Device, buffers them and forwards them to the monitoring station using a protocol and interface that are supported by the monitoring station. The CIS can emulate some of the most popular hardware receivers' protocols, such as Sur-Gard MLR2, DC09 (SIA over IP), VISONIC, KP Electronics etc. In this way, different monitoring station software programs are supported.

The administrative access to configuration settings and service commands can be done through a web based software at <https://m2m.adesco.gr/admin> or through Android app 'RControl Admin' (available free of charge at GooglePlay). The user can create different administrative accounts with different permissions. For example, it can be specified that some users can only view communicator statuses and check the signal level without being able to change alarm configuration settings.

Key features and benefits

- High reliability due to multiple transmission channels (GPRS/SMS/GSM/PSTN) and redundant servers;
- Connection monitoring – adjustable fault reporting time as low as 20 seconds.
- Jamming detection – triggers notification through the alternative channel or activation of a digital output.
- Support of any security alarm system through digital inputs, serial port or telephone line emulation and DTMF decoding.
- Software-based receiver that emulates various hardware receiver protocols (Sur-Gard MLR2, DC09, Visonic RC4000, etc.).
- Web-based software and smartphone app for devices configuration and administration. Remote firmware updates.
- Remote servicing – virtual serial port to the alarm panel allowing remote programming with the panel manufacturer's software.

End-user smartphone app – supports push notifications, arming/disarming of the alarm system, video verification.

Different options to connect to alarm panels

The MQ03 communicators can receive events from any alarm panel via digital inputs, via telephone line communicator, or serial port, as follows:
 The digital inputs of MQ03 are pulled-up and activated by GND. Custom messages can be assigned to each edge of the input signal.
 The Device can emulate telephone line and can decode the DTMF signals from the telephone line communicator of the alarm panel. This is another universal way to integrate with any alarm panel and to retrieve extended information about partitions, zones and users.
 MQ03 communicators can also integrate with some alarm panels via the serial port. This feature gives the possibility for bi-directional communication and remote programming of the panel with the manufacturer’s programming software.

Device Installation guide

The Device can be installed in a metal or non-flammable plastic enclosure together with an alarm system unit. When the metal enclosure is used it is recommended to ground the enclosure using 0.50 mm² 1 thread cable. For the device connection to input/output connectors use 0.50 mm² 1 thread cable of up to 100 meters length.

Mounting

1. Connect the GSM antenna to SMA connector. Check if the antenna is fixed properly. It is not recommended to turn on the device without GSM antenna connected. **Warning:** It is recommended to install the GSM antenna away from the alarm system to ensure better quality of the signal. It is not recommended to install the antenna inside the metal enclosure.
 2. Connect the Device to the alarm panel according to the desired communication method (see **Configuration of Terminals**). Make sure that power supply is sufficient for the load of the module. The quiescent current of the module is up to 150mA, however it can reach up to 400mA during communication. **Warning:** Power supply at alarm system must be disconnected before any installation or maintenance work.
 3. Now the Device can be powered up. It should start in less than a minute. The GSM LED indicator should be ON indicating successful connection to GSM network. **LED indicator meaning:**
 - Off - the device is switched off
 - Slow flashing (once per second) - no connection to a server (CIS)
 - On - the device is connected to a server without data transfer
 - Fast flashing – data transfer
 5. Check the GSM signal strength through the **administrative web site** or **administrative mobile application**. It may happen that the signal strength is not sufficient in the desired mounting place. In this case the planned installation place can be changed before mounting the device. Signal levels below 10 are unacceptable. Recommended levels are above 14.
- Warning:** Do not mount the Device in places where it can be affected by strong electromagnetic disturbances (e.g. in the vicinity of electric motors, etc.). Do not mount the Device in wet places or places with high degree of humidity.

Configuration of terminals of MQ03-4I-DTMF GPRS Communicator



Terminals description:

IN1 – IN4: digital inputs, triggered by ground (-), pulled-up with 2.2KΩ to 5V
 OUT1 and OUT2: open collector outputs
 RING and TIP: connect to the RING and TIP of alarm panel
 RX and TX: serial interface TTL (4V)

Device Configuration Guide

Your administrative tools – web site and mobile application

Generally, devices will be shipped preconfigured according to the needs of each client. To request changes of your default settings, please contact your account manager.
 In most cases, when you install a device on site you will only need to wire it and configure the Site Number.
 Most of the configuration you would need to perform in your everyday routine as an installer or administrator could be performed via the **administrative mobile application** for Android smartphones that you can download from here:
<https://play.google.com/store/apps/details?id=m2m.AdminMobile> (**RControl Admin current**)
 The mobile application is designed to allow easy configuration via 3G and WIFI when you are on the move.
 You can also change the settings from **the administrative web site**: <https://m2m.adesco.gr/admin>
 Some of the settings that are seldom changed can be configure ONLY via the **administrative web site**.

Most frequently used scenarios

This chapter describes some of the most frequently used administrative scenarios. You can find the detailed description of the administrative site features in the chapters that follow after.

Configuring a new device via a template

It is recommended that the device is powered and is connected to the server (Connected = True). This will enable you to check and save all available settings, including the online settings.

Find the device by its Controller Name. Usually there is a label on the back of the device with the Controller Name (Serial Number).
Select the device and choose 'Alarm Settings' from the 'Commands' menu or from the context menu.
It is recommended to check the 'Enable Online Settings' option. Otherwise, the online settings from the template will not be applied.
Read current settings from the device by pressing the 'Get Current Settings' button.
Select and apply a template with the desired settings.
Enter the site number.
Note! If you enter the site number before, applying the template the site number will be deleted and you will have to reenter it again.
Save changes.
You can check the signal level by pressing the 'Signal Level' button. The device must be connected to the server and the 'Enable Online Settings' should be checked.

Saving settings as a template

Open the alarm settings of an appropriately configured device
Save the settings as a template with the button 'Save As Template'. Choose a new name for the template or overwrite an already existing template.

Check GSM signal level

Upon installation of the device onsite when making tests, it is recommended to check the signal level of the GPRS communicator. Signal level is measured on a scale from 0 to 31. Levels below 10 are not acceptable. Recommended levels are above 14.
Find the device by its Site Number or by the Controller Name written on the back of the device
Double click to open the details page of the device
Select the [Signal Level] command from the 'Command' list and press the 'Send Command' button.
The result has the format of '+ CSQ: 31,0'. In this case the signal level is 31. If the signal level is less than 14, try to find a better place for the communicator or try changing the place or rotating the antenna. If the range is less than 10, it may be necessary to use an antenna with longer cable or move the device to a different place.

Note! You can check the signal level from the Alarm Settings page, too.

Searching for devices

The main page of the **administrative web site** provides tools to search for devices by different criteria. You can also search for devices from the "Search Controllers" page of the **administrative mobile application**.

Basic search attributes – you can search by these attributes both in **the administrative web site** and the **administrative mobile application** for Android smart phones:

Serial Number – this is the unique identifier of the device that is printed on the label on the back of the device. Usually you will search by this attribute when you want to configure devices for the first time.

Controller Name - this is the custom name of the device that can be changed by the end customer. Initially it is the same as the Serial Number of the device.

Site Number - this is the unique identifier of the site where the device is installed on. This is the number that the device reports to the central monitoring station. You will usually search by this criterion when devices are already installed on the site. To configure the Site Number of the subject, please refer to the "Alarm settings of the controller" chapter.

IMEI – this is the unique identifier of the GSM module of the device. You can find it on a label on the GSM module inside of the communicator.

Additional search attributes – you can search by these attributes from the **administrative web site** only:

Connection state - filters device by whether they are currently connected to the server or not.

SIM Card Number – this is the unique identifier of the SIM card that you can find printed on the SIM card itself. It is relevant only if you have registered the SIM card with the device (See "SIM card registration" chapter)

Phone Number – this is the phone number of the SIM card inserted in the device. It is relevant only if you have registered the SIM card with the device (See "SIM card registration" chapter)

On the administrative site you can further perform some filtering and sorting of the data grid with the information about the devices.

Sorting the data: click on the header of a column to sort the data.

Filtering by multiple criteria simultaneously: put the cursor of the mouse over the header of a column and a triangle will appear. Pressing it will open a context menu. Select 'Filters' and enter the desired value of the filter attribute.

Showing and hiding columns: From the same context menu, select 'Columns' and tick the ones you want to see.

Viewing information about a specific controller

Double click a device from the list of controllers to open a new page with the details about it. From this page you can send commands to the device and see the answers.

Sending commands to the device

Since the device maintains a constant connection to the server, you can send administrative commands in real time and receive responses. This can be done from the details page of the controller. Select the desired command from the drop-down menu 'Command' and press 'Send Command' button. The result of the command is displayed in the text box. If you selected 'Auto Clear Response', the response from the previous command will be cleared before sending the next command.

Commands can be also sent from the page with the list of all devices. To do that, select the desired device and press the 'Send Command' button. This approach enables you to send commands to multiple devices simultaneously – e.g. when you want to restart multiple devices at once. However, if you choose this approach you cannot see the response of the executed command.

Note! To be able to send a command to a device, it must be connected to the server.

Description of commands:

Restart - restarts the device, for example after some configuration changes

Connection State – command that provides verbose information about inputs state, signal level, GSM operator selection mode, currently selected operator and LAN settings (if applicable).

Signal Level - check the level of GSM signal of the device. The response from the device is in the format '+ CSQ: 31,0'. In this case the signal level is 31. For the meanings of the different values of the range, refer to the 'RSSI Meanings.xls' document. In general, the recommended values are those above 14 and values below 10 are not acceptable.

Voltage - check the power supply voltage in millivolts.

Card No - reads the serial number of the SIM card inserted in the device. To assign a SIM card to a device, see 'Register SIM card' section.

You can also view current state of a communicator from the administrative mobile application for Android.

Search and navigate to the desired device. In the INFO tab for the device you can view the following important information:

Connection State – if the device is connected to the server, this is represented with a green icon, otherwise the icon is red. You can see if the device is connected via LAN or GPRS.

Inputs State – a graphical representation of the current state of the inputs

Voltage

Signal Level

Operator Selection Mode – if operator is automatically selected or if is manually selected from a list of specified operators.

Current operator – the code and the name of the GSM operator to whose network the device is currently registered.

Alarm settings of the controller

Alarm settings of the controller include Site Number (Account Number), programming the digital inputs, serial port configurations for integration with some alarm panels, as well as configuring reporting channels to a central monitoring station.

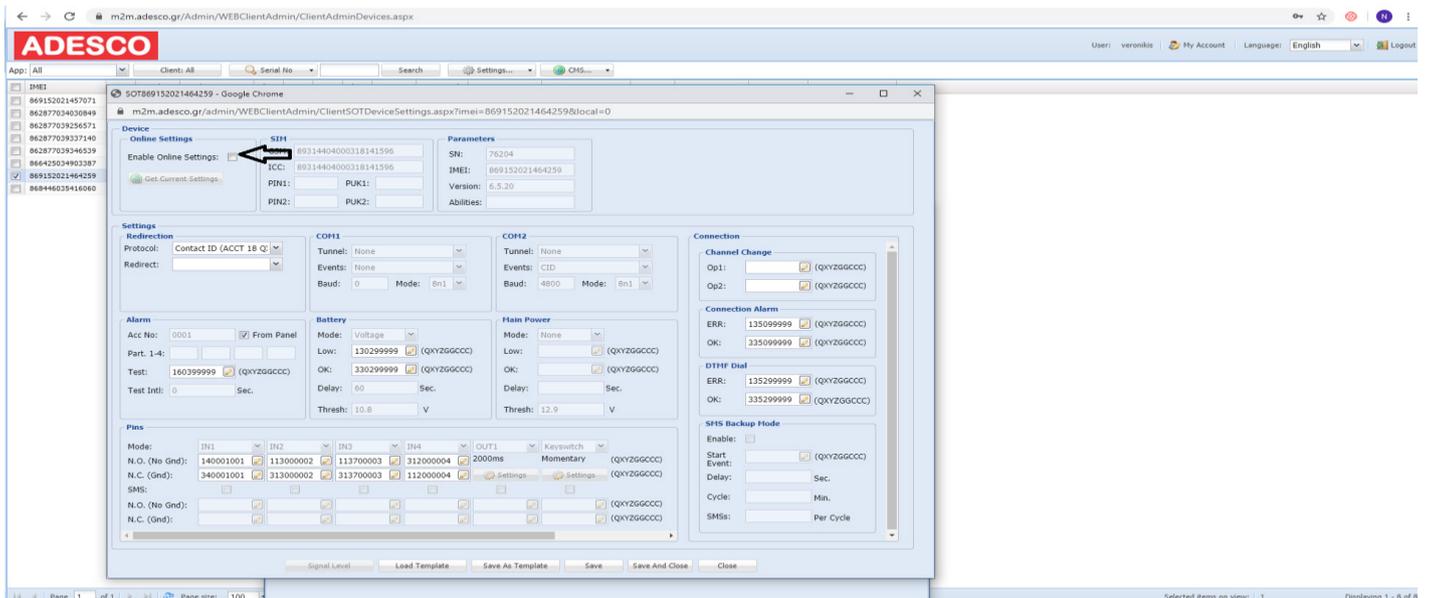
To edit the Alarm settings from the **administrative web site**, proceed as follows:

Search for the desired device (see “Searching for devices” section). Double click the device from the list of controllers matching your search criteria to open the Info page of the controller. From the Commands menu select Alarm Settings.

You can also check the device from the list of controllers, right-click it and select Alarm Settings from the context menu.

Most of the settings are stored only on the server so you don't need an active connection with the device. However, some of the settings need to be stored on device so it is required that the device is connected to the server. These settings are referred to as online settings.

To be able to change online settings from the **administrative web site** or the **administrative mobile application**, you have to check the "Enable Online Settings" checkbox. This option is disabled if the device is not currently connected.



When you edit some settings, the changed fields will be colored in yellow. Once you finished with the programming, press the Save button. The settings will be saved on server and if you have enabled the online options, they will also be written to the device. To edit the Alarm settings from the **administrative mobile application**, proceed as follows:

Search for the desired device (see “Searching for devices” section). Click the device from the list of controllers to open the Info page. Navigate to the Settings tab. Click the Alarm Settings menu to open the Alarm Settings page.

Below is a list of the settings you can configure.

Reporting to Central Monitoring Station (CMS)

Configuring the Site Number

When reporting events to the Central Monitoring Station, the device identifies itself by Site Number, also sometimes referred as Account Number. You can configure the Site Number from from the Alarm Settings page on both the **administrative web site** and the **administrative mobile application**.

Note! When the communicator is connected to the alarm panel via serial port or digital inputs, the events are reported using the Site Number assigned to the communicator. However, if the communicator is connected to the landline dialer of the alarm panel then the events from the

dialer are reported using the Site Number that is programmed into the alarm panel itself. Therefore, ensure that you have configured the same Site Number on both the communicator and the alarm panel.

Configuring different Site Numbers for different partitions

When the system is split into multiple partitions, you can provide different Site Number for each partition. In this way you can configure a single communicator to report events from different sites independently.

You can specify up to 4 additional Site Numbers in the SiteNo1 – SiteNo4 fields in the Alarm Settings section on the **administrative web site** and **administrative mobile application**. If an event from partition 1 is received it will be reported with SiteNo1. If SiteNo1 is not specified, then the event is reported with the generic SiteNo. If an event from a partition is outside the range 1-4 then again the generic SiteNo is used.

Note! The events from the dialer and from the serial port of the alarm panel contain extended data about the partition. Besides that, you can still split the system in partitions even if the panel is connected only to the digital inputs of the communicator. For example, you can specify that input 1 will generate alarm event from partition 1 and input 2 will generate alarm event from partition 2. (See “Messages from digital inputs” section). In this way you can again get event reports from different independent Site Numbers.

Note! The general events that are specific to the communicator itself will be reported only for one of the Site Numbers! Such general events for example are the Connection Lost event, Jamming Detected, Periodic Test.

Reporting to Central Monitoring Station

Besides sending the events to the client site and the client mobile application, the device can report also to Central Monitoring Station. For easy integration with most of the monitoring software, events can be redirected using different popular hardware receivers’ protocols such as SurGard MLR2, Visonic, KP RCI3300 etc. To enable redirecting data to a Central Monitoring Station, go to Alarm Setting page of the device in the **administrative web site** or in **the administrative mobile application** and check the “Report to CMS” checkbox.

Choose the transport protocol from the “Receiver protocol” list, e.g. SurGard MLR2.

The format of the messages that is used by default is Ademco Contact ID.

Configuring the messages generated by the MQ03 communicators itself

Configuring periodic test messages

You can configure the GPRS communicator to send test messages periodically over a specified time interval. This can be done **ONLY** from the **administrative web site**.

If the Test Intl. field is left blank, no test messages will be emitted by the GPRS communicator.

Note! It is very important to distinguish between periodic tests and the so called heartbeats that are used to monitor the connection between the device and the server. The device sends heartbeats to the server in very short intervals in order to maintain a constant connection with the server and to enable the server to detect when the device is disconnected and to send an alarm message. Generally, it might be from several seconds to several minutes. These heartbeats ARE NOT forwarded as events to the monitoring center. An alarm event is sent only when the server detects that a device is disconnected.

On the other hand, the periodic test message is sent to the monitoring center and is usually set at intervals of a few hours. Its purpose is to prevent the occurrence of events of the type 'No Event for Long Time' in the monitoring software.

Most of the traffic generated by the communicator is due to the keep-alive heartbeats. That’s why you CANNOT configure the heartbeats interval by yourself. It is part of your service agreement. If you want to change the heartbeats interval, please contact your account manager.

You can only configure the interval of the test messages that are sent to the monitoring software.

Programming messages from the digital inputs

You can configure the messages that will be reported when the state of a digital input is changed. This can be done from both the **administrative web site** and **administrative mobile application** from the Input pins section on the Alarm Settings page.

Generally, the digital inputs are activated with GND. Please refer to the hardware specification of your device.

You can configure the message that will be sent when the input level is high (GND not applied) from the “Raising/ON” field of each input. You can configure the message that will be sent when the input level is low (GND applied) from the “Falling/OFF” field of each input. Messages are entered using the Contact ID format. From the **administrative web site** click 'Edit' button for each field you want to edit. From the **administrative mobile application** click the field itself. A dialog will open and you should specify the event code, the partition and the zone/user components of the Contact ID message.

If a field is left blank, this digital input will not report events.

Low battery and Mains power outage messages

This message can be configured **ONLY** from the **administrative web site**.

The device monitors the power supply voltage and can report a message in case of missing mains power supply or low battery. You can configure the message code, as well as how long the voltage has to be below a set threshold before generating the alarm event. Detecting the mains power outage relies on the fact that when mains power is available, the voltage will be above 13.2V to be able to charge the battery. This threshold can also be configured.

Connection Lost message

This message can be configured **ONLY** from the **administrative web site** from the Connection Alarm section of the Alarm Settings page. The device maintains a constant connection to the server via GPRS and periodically sends keep-alive heartbeats to notify the server that it is working properly and that the connection is alive. If the server does not receive data from the device, it will report an alarm message about the disconnected device.

Most of the traffic generated by the communicator is due to the keep-alive heartbeats. That’s why you CANNOT configure the heartbeats interval by yourself. It is part of your service agreement. If you want to change the heartbeats interval, please contact your account manager.

Communication Channel messages

This message can be configured **ONLY** from the **administrative web site** from the Channel Change section of the Alarm Settings page. If you are using ADESCO SIM cards (provided by ADESCO) you can benefit of using the network of multiple operators with a single SIM card. If the network

of the main operator experiences some problems, the device will automatically connect to the network of the backup operator. After some time it will automatically try to reconnect back to the main operator.

The above functionality can also be achieved with the Dual SIM version of our devices, using local SIM cards from two different operators. You can configure the messages that the communicator will report when it switches between different communication channels. If you leave these fields blank the device will not report when it switches the channel. This will NOT affect the normal switching of the channels!

Jamming message

This message can be configured ONLY from the **administrative web site** from the Jamming section of the Alarm Settings page.

The device can detect jamming and can make difference between the jamming and network problems. In case of jamming the server will first report Connection Lost event. The device will report the jamming message ONLY after the connection is restored! If you use LAN+GPRS device, then the Jamming Message will be reported immediately when detected via the LAN channel.

Alarm settings templates

This feature is available ONLY from the **administrative web site**.

To facilitate the configuration of multiple devices you can save settings as a template.

To do this, enter the appropriate settings for a device and click the 'Save As Template' button. IMPORTANT! Device must be connected to the server and you must have selected the 'Enable Online Settings' option. This will allow all the settings to be saved in the template, including those that require a connection to the device. Enter a name for the template and save it. You can also overwrite an existing template. To apply a predefined template to a device, open the Alarm Settings page of the device, press the 'Load template' button and select the appropriate template. All the fields stored in the template will be filled with the values from the template, with the exception of the Site Number. Enter the appropriate Site number and click 'Save' button.

SIM card assignment

This feature is available ONLY from the **administrative web site**.

When a new SIM card is inserted into the device, you might want to assign it to this device in the database. This procedure is not mandatory but the information about mapping between the SIM cards and the devices might be helpful during some administrative procedures. Registration of the SIM card with the system is performed automatically when you configure the alarm settings of the device (see 'Alarm settings of the controller' section). You can also manually trigger the registration procedure for one or more devices by selecting the desired devices from the list on the main page and then selecting the 'Verify SIM Card' option from the context menu. The devices must be connected to the server. When the SIM card of a device is replaced for some reason, then you also need to trigger this operation. To view the last time when a SIM card is verified, you should unhide the hidden column 'SIM Card Verified'.

Viewing history of events sent from a device

The events from the communicators are sent not only to the monitoring center but can also be redirected to a client site targeting the end customers of the security services. You can access this site at <https://m2m.adesco.gr/admin>

In addition, the client site can be accessed directly from the administrative site. This is useful when you need to trace the history of the events generated by a device from any computer on the Internet when you have no access to the monitoring software.

To view the event history for an object, find the device in the administrative site, select it in the list of devices and select 'Client Site' from the context menu or from the 'Commands' menu. A new window opens, displaying the history of events for the device. You might need to allow pop-ups for this site. For the administrative site as well as for the client site you can create additional accounts with restricted permissions to see only some of the controllers. For example, you can give an end user rights to only see the history of the devices he owns. You can name the zones in your house, you can give names to the users who can access the alarm system etc. You can set up notifications via email or SMS for various events. There is an administrative application for Android to help accomplish some of the administrative tasks from your smart phone. There is also a client Android application so that the end-user can see the history of events and arm/disarm the alarm system from his smart phone.

Connecting alarm panels via the DTMF dialer

Wiring the panel to the communicator

Connect the TIP and RING of the alarm panel to the TIP and RING connectors of the MQ03 communicator. Switching the wires is allowed and will not affect the proper working.

Guidelines for configuring the alarm panel

Enable Telco communication of the panel

Select DTMF (Tone) dialing

Select Contact ID Full communication format

Enter a simple telephone number for dialing with repeating digits (recommended: 99999999). Avoid using one-digit telephone numbers.

Enter client account number in the panel. It should be 4 digits long. If there are '0' digits in account number, they should be entered as 'A'. For some panels you should enter the client account number for each partition, including the main partition 0.

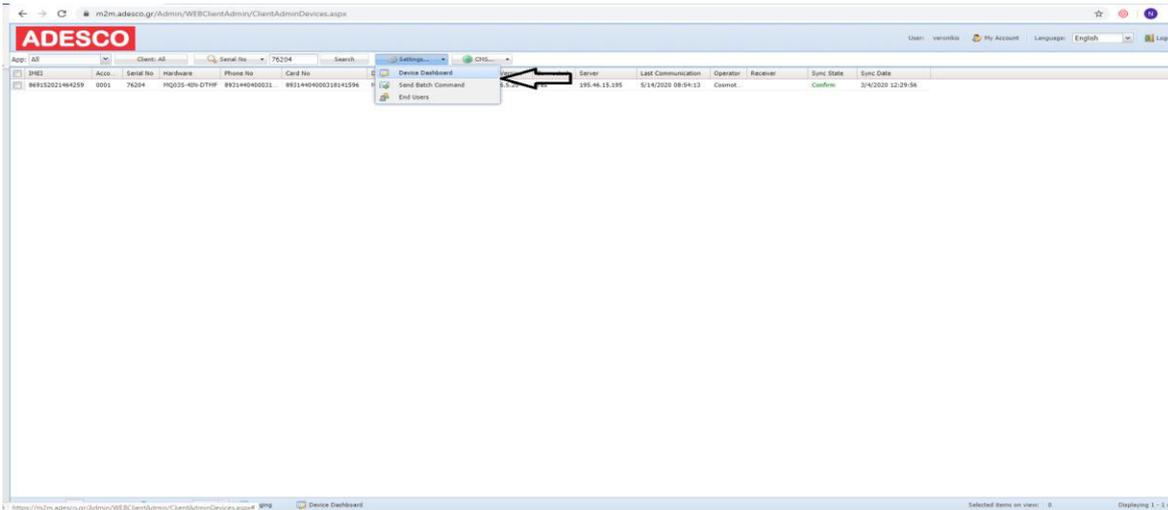
It is recommended to disable "telephone line monitoring" function

It is recommended to disable "wait for dial tone" option

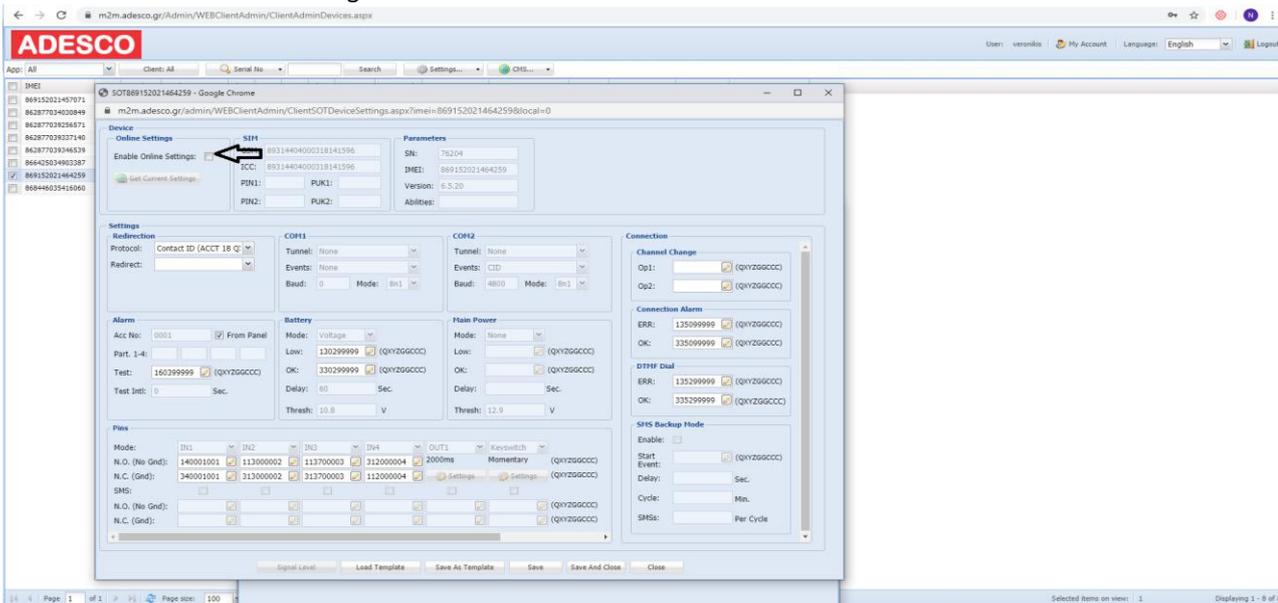
Configuring the working mode of the DTMF decoder

Usually, the devices that feature a DTMF decoder will be **already preconfigured** with the appropriate settings. However, if you need to change them, follow the instructions below:

From the **administrative web site**, navigate to the Menu Commands->Alarm Settings page.



Check the “Enable Online Settings” check box as shown below



Press “Get Current Settings” button to read settings from the device. The device should be powered and connected to the server, otherwise these fields will be disabled. From the COM Settings section select “None” in the Tunnel field and select “DTMF2” working modes in the Events field. This will automatically populate the correct baud rate and format (4800, 8n1). Press “Save” button.

Account number reporting modes

You can choose if the events from the DTMF dialer of the alarm panel will be transmitted with the Account number that is programmed on the panel itself, or with the Account number (SiteNo) of the communicator.

From the **administrative web site**, navigate to the Menu 'Commands' -> Alarm Settings. In the COM settings section, if DTMF mode is selected, you will see “Keep DTMF Account Number” checkbox. If it is checked, the alarm events will be transmitted with the account number that is specified in the alarm panel itself. This can be useful when you want to specify different account number for the different partitions in the alarm panel. Note: the events that are generated from the MQ03 communicator itself will be still reported with the SiteNo, specified in the alarm settings page for that communicator.

If you uncheck the “Keep DTMF Account Number” checkbox, all events will be reported with Account Number of the communicator. This is useful when you want to easily change the Account number without having to reprogram the alarm panel.

Connecting alarm panels via the serial port

MQ03 communicators support integration via the serial port with some alarm panels. Please verify that the model of the communicator supports your panel. For MQ03 communicators, verify that you have also purchased appropriate cable.

Selecting the type of the alarm panel

From the **administrative web site**, navigate to the Commands->Alarm Settings page. Check the “Enable Online Settings” check box and press “Get Current Settings” button to read settings from the device. The device should be powered and connected to the server, otherwise these fields will be disabled. From the COM Settings section select “None” in the Tunnel field and in the Events field select the brand and the model of the panel that you are connecting via the serial port. This will automatically populate the correct baud rate and format. You can change these settings if needed. For some alarm panels you might need to specify passwords that give the communicator access to the panel. Press the “Save” button.

See below for alarm panel specific settings.

Configuring Teletek Eclipse series

Following the instructions from the “Select the type of the panel section” and select the type of the panel to be Teletek Eclipse. In the Pass1 field you should enter the PCID password of the Teletek panel. If you haven't changed it, it should be 1234 by default. In the Pass2 you should enter the code of a valid user in the Teletek panel. It can be installer's code or user's code. If you don't enter anything, the default values are 1234 and 7777 respectively. If you are using the ProSTE software, these are the two passwords that you need to access the panel via the software. We recommend entering some user's code and not the installer's code for Pass2. You can even create a user that has limited permissions in the panel and use that user only for the communicator. Also, you will need Pass2 to be a valid manager's code and not an installer's code if you need to allow remote arming and disarming. Press Save to persist the new settings. Restart the device (either from the power, or by sending Restart command from the communicator info page). The version of the firmware of the communicator should be 4.2.16 or above. To update remotely the firmware, refer to the Remote Firmware Update section. Test if the communication with the panel is ok. Arm and disarm the panel and generate some alarm event and check if you will receive the events as expected.

Configuring Paradox Family panels

Follow the instructions from the “Select the type of the panel section” and select the type of the panel to be one of the supported Paradox series. The Paradox serial port communication protocol is uni-directional. This means that the panel sends events on the serial port but does not wait for confirmation that the communicator has actually received them. This means that there is a small probability that some events are missed. This might happen if there are strong external electromagnetic influences, for example if there is a radio transmitter in the same box where the alarm panel and the communicator are installed. For this reason, we highly recommend that you also configure a PGM of the panel to be activated on alarm event and to connect it to an input of the communicator. In this case you will have a backup general alarm event. You will receive the general alarm from the input of the panel and the event with the information about the zone from the serial bus.

Configuring Texecom Premier & Elite panels

Following the instructions from the “Select the type of the panel section” and select the type of the panel to be Texecom. In the Pass1 field you should enter the UDL password of the Texecom panel. If you haven't changed it, it should be 1234 by default.

Configuring Remote Control of the panel

The MQ03 communicators can add smart features to new and existing alarm systems. You can monitor current status of the system, look back in the events history and receive real-time notifications for important events. Even more, you can remotely arm/disarm the alarm panel from a smartphone.

You can download the mobile application for Android - Google Play (“RControl”) and for iOS - AppStore (“Residence Control”). Please find below links for how to:

<https://www.youtube.com/watch?v=f9KQ140RXaY&t=122s>

https://www.youtube.com/watch?v=hsfsYy9o_Zg&t=189s

To enable the **remote arm/disarm feature**, both the alarm panel and the communicator should be properly configured. For some of the alarm panels, the remote arming/disarming can be done via the serial port. For others, it can be done via the keyswitch feature of the panel. No matter what option you choose, you will need to create an end user for the mobile application and you will need to grant permissions for remote arming/disarming (refer to “Granting remote access to users” section).

Configuring the Keyswitch option

You can remotely arm and disarm virtually any alarm panel that supports **Momentary Keyswitch Arming**.

The general principle of working is as follows:

You should configure an output of the communicator as keyswitch. You should connect this output to a zone of the panel that is configured as a momentary keyswitch. When momentary activated, the output of the communicator will switch to ground for a predefined interval of time. Each pulse would alternately arm/disarm the system.

The communicator needs feedback from the alarm panel if it is actually armed or disarmed. For that reason, you should also configure a PGM of the alarm panel to activate (switch to ground) when the panel is armed and to deactivate when disarmed. You should connect this PGM to an input of the communicator that is configured as Status Feedback input.

Note! The keyswitch zone of the panel should be attached to Partition 1. The PGM of the alarm panel should also reflect to the arming status of Partition 1. Currently you can arm/disarm remotely via keyswitch **only Partition 1**.

Configuring the keyswitch feature of the communicator

To configure an output of the communicator as keyswitch, from the **administrative web site**, navigate to the Commands->Alarm Settings page. Check the “Enable Online Settings” check box and press “Get Current Settings” button to read settings from the device. The device should be powered and connected to the server, otherwise these fields will be disabled.

In the Pins section, choose the terminal you want to configure and select the Keyswitch option from the dropdown list. For some MQ03 models, only the IN1 terminal can be configured as keyswitch. For other MQ03 models, one of three terminals IN1, IN7 and IN8 can be configured as keyswitch. Once you choose the Keyswitch option for the terminal, a dialog will appear that will allow you to configure some of the parameters of the keyswitch:

“Peripheral Name” - the name which will appear as label in the mobile application.

“Impulse” - how long the impulse should be. It depends on the configuration of the alarm panel itself but usually the default value of 1000ms (1 second) is appropriate.

“Feedback Input” - select the input of the communicator where you will connect the feedback PGM of the alarm panel which will report if the panel is actually armed or disarmed.

“Armed Level” - specifies the level of the input when the panel is armed. It depends on how you have configured the Status PGM of the panel. If you keep the default value of LOW, you should configure the PGM of the panel to be N.O. – it should activate (switch to GND) when the panel is armed and should deactivate when the panel is disarmed. It is very important to understand that the inputs of MQ03 are managed by GND and not by +. So, the PGM of the panel should use negative trigger (0V), rather than positive trigger (12V).

General guidelines for configuring the keyswitch of the alarm panel

After you have configured the keyswitch options of the communicator, you should configure the keyswitch zone of the alarm panel itself. Please refer to the panel’s installer manual. Currently the communicator can work only with panels that support Momentary keyswitch. Maintained keyswitch is not supported. Also, please keep in mind that for some models of the alarm panels you might need to connect the output of MQ03 to the keyswitch zone of the panel through an EOL resistor.

Note: Side effect for shared input/output terminals

For all models of MQ03 communicator IN1 terminal is shared – it can be configured as either input or output. For some MQ03 models, IN7 and IN8 terminals are also shared. For other models, IN7 and IN8 can be configured only as clear outputs and not as inputs (they are marked as OUT1, OUT2). If a terminal is shared and can be configured as either input or output, there is an important side effect that you should understand and have it in mind. The inputs are pulled-up with 2.2KΩ to 5V, so the voltage measured between the + and the shared output terminal might be different than 0V even if the output is deactivated. In some cases, this might prevent the keyswitch zone of some alarm panels from working correctly. To solve this, you might need to use an external relay.

The models MQ03 that have **clear outputs** (OUT1, OUT2), you don’t have that side effect.

Note: After you have successfully configured both the communicator and the alarm panel, refer to the “Granting remote access to users” section to see how to allow end users to access this feature from the mobile application.

Granting remote access to users

Once you have properly configured both the alarm panel and the communicator for remote arm/disarm, you now need to create end user credentials and to give permissions to use the remote-control features with the smartphone application. If the user is not granted these permissions, he will not be able to do it even if the panel and communicator are configured correctly.

To grant remote access permissions to a user, navigate to Commands->Remote Users page. To create a new user, press the Add User button. To edit existing user, select it and press the Edit User button. In the new page, enter the required data. If you want to allow to the user to remotely arm/disarm the panel, press the Allow Remote Access checkbox. **Note:** Allow Remote Access option is active only if the communicator is configured for remote arming/disarming (either via keyswitch, either via serial port for the supported panels).

If Allow Remote Access checkbox is selected, the user is granted the default permissions to remotely arm and disarm Partition 1. If you want to change the default behavior, press the “Advanced” button. You can add new partitions to control (only for alarm panels that are supported via serial port) and you can specify if the user can arm and disarm.

Once permissions are granted, a Secure Pairing procedure must be completed before the user can control the panel remotely. The pairing procedure adds additional level of security. It requires physical access to the alarm panel to allow remote access. This is intended to prevent an installer to secretly add a new user that can remotely control the alarm panel.

Once you create a new user and have selected the Allow Remote Access option, you will be asked if you want to immediately start the pairing procedure. Also, you can start the pairing procedure by pressing the “Secure Pairing” button for an existing user. Finally, the pairing procedure can be started by the end user itself from the mobile application.

No matter which option you choose to start the pairing, you must specify the Remote PIN code that the end user will use from the mobile application to remotely arm and disarm the panel. Then you have 30 seconds to arm or disarm the alarm panel locally (e.g. using a valid user code from the panel keyboard). The best practice is the user for whom you are creating mobile application login to arm by himself from the keyboard. If this operation times out, you must start the pairing procedure again.

Note: it is important to understand that the Remote PIN is only used by the end user when he arms/disarms the panel remotely from the mobile application. The Remote PIN **might be different** from the alarm panel PIN used to locally arm/disarm the panel from the keyboard of the panel.

The Remote PIN adds additional level of security. Generally, the end user will need valid credentials to log in the smartphone app. However, he might stay logged on, so to prevent someone from abusing the phone without his knowledge, the Remote PIN will be requested every time when arming/disarming the panel remotely.

Note: If you are changing the permissions of an existing user, the user will need to log out and log in again from the mobile application to reload the new settings. Failing to do so will most probably result in not being able to remotely control the panel until you login again.

Technical details MQ03

Communications: GPRS

Supported Protocols: Ademco Contact ID® & SIA. Support of any security alarm system through digital inputs, serial port or telephone line emulation and DTMF decoding

GSM/GPRS: Quad-band (850/900/1800/1900 MHz); GPRS class 12

ARM9 processor, 512KB RAM, 1MB Flash

Up to 4 digital inputs, 2 digital outputs

Serial interface - UART,

Antenna connector: SMA, 50 ohms

Optional expansion modules:

- ✓ 868MHz radio transceiver
- ✓ RFID 125KHz or 13.56MHz MiFare / NFC Card Reader

Supply voltage: +7 to +18 VDC; Peak Current Consumption 400 mA max.

Current Used in Standby Mode: 150mA max

Dimensions: 90 x 63 x 32 mm

Operating temperature range: -20...+55°C

Weight: 150g (device only)