

Bridge DSC01 v4

User Manual

(Rev 1.4.9)

September 2021

This page was intentionally left blank

Content

Content.....	3
Overview	7
Features.....	7
Specifications	7
Installation instructions (Wiring).....	8
Connecting Accessories.....	8
Device Configuration.....	9
WiFi and AP configuration.....	9
Use cases	10
What to do in case of losing or forgetting AP password.....	11
Status indicator led	11
Home automation system integration	12
Home Assistant	12
Others MQTT home automation systems.....	13
Hardware and Firmware versions	13
Advance configuration	14
Device ID.....	14
MQTT server.....	14
MQTT server port (unsecure).....	14
MQTT user	14
MQTT password	14
MQTT Client ID	14
Access code	14
Status Topic	15
Birth Message.....	15
LWT Message (Last Will Message)	15
Disconnected Message.....	15
Partition Topic Prefix.....	15
Active Partition Topic	15
Zone Topic Prefix.....	15
Fire Topic Prefix.....	16
Trouble Topic.....	16

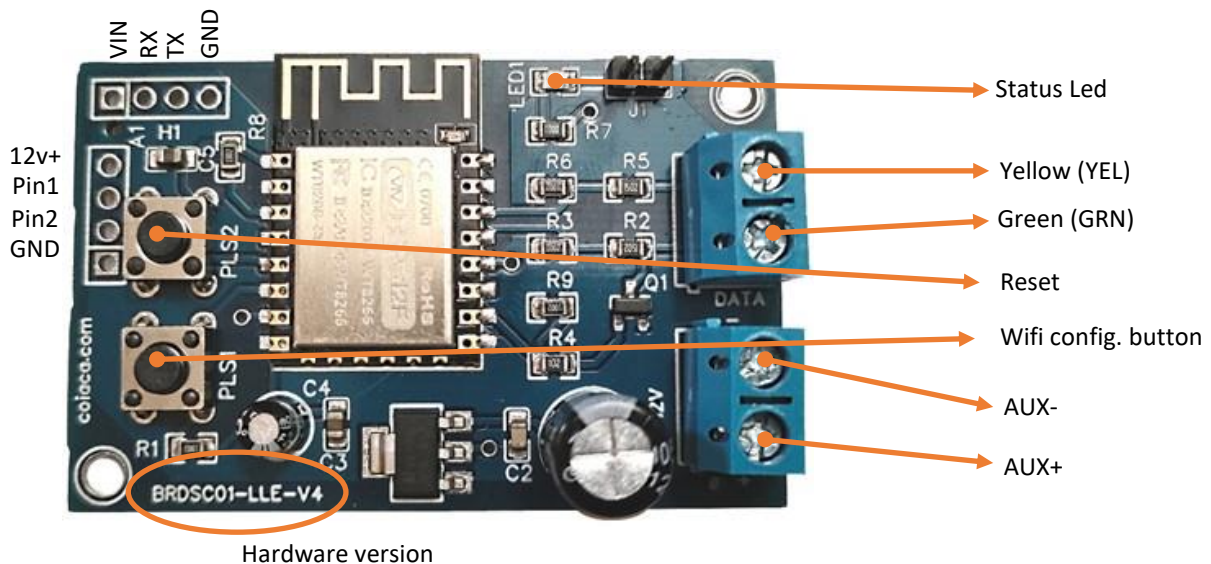
- Commands Topic..... 16
- Keep Alive interval (seconds) 16
- Keep Alive Topic 16
- Timer ON 16
- Timer String 16
- Publish Timer String 17
- NTP server 17
- Time Zone 17
- NTP Update interval (seconds)..... 17
- DST (Daylight Saving Time)..... 17
- MQTT Retain 18
- MQTT QoS 18
- Monitoring feature..... 18
 - Enable Monitoring parameter..... 18
 - Monitoring Topic Prefix..... 18
- Remote Management 19
 - Enable Remote Management 19
 - Remote Management Password..... 19
 - Remote Management MQTT server 19
 - Remote Management MQTT server port (TLS)..... 19
 - Remote Management MQTT user..... 19
 - Remote Management MQTT password 19
- Force all traffic through the secure connection..... 19
 - Remote Management Command Topic 20
 - Remote Management Result Topic..... 20
 - Remote Management MQTT Retain 20
 - Remote Management MQTT QoS..... 20
- MQTT Debugging feature..... 20
 - Enable MQTT Debug parameter 20
 - MQTT Debug Topic..... 20
- Disclaimer 20
- Warranty 20
 - Limited Hardware Warranty 21

Service after expiration of warranty	21
Warranty Limitations.....	21

This page was intentionally left blank

Overview

Coiaca **BRDSC01 v4** is an interface that allows DSC PowerSeries security systems to be controlled from any mobile or web application and to be easily integrated to automation systems that support MQTT protocol.



Features

- 1-8 partition status tracking of armed, disarmed, triggered and fire states
- Trouble status tracking
- 1-64 zones status tracking
- Enables writing keys to the panel for partitions 1-8
- Super easy wiring
- 2 digital PINs for connecting accessories.
- In circuit programming connectors
- TLS for secure communication channel
- Connection status indicator led
- WiFi password recovery button
- Remote Management
- Monitoring feature
- MQTT remote debug feature

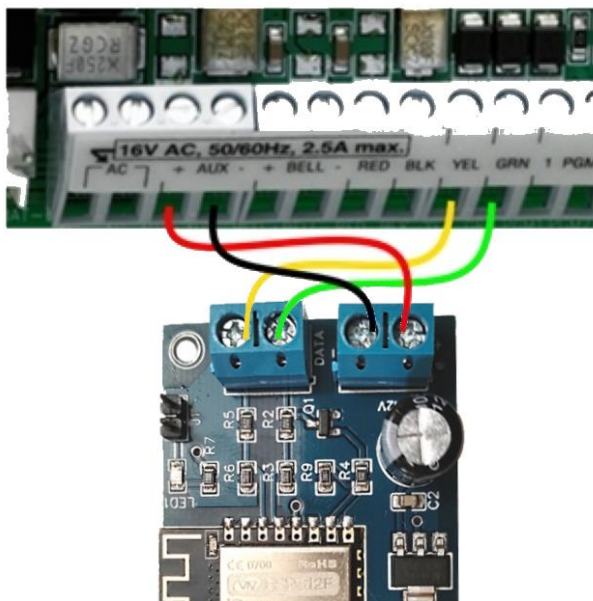
Specifications

- Dimensions: 75mm x 38mm x 20mm
- Power Supply: DC12V from alarm system.
- Wireless standard: WiFi 802.11 b/g/n
- Antenna built in +19.5dBm output power in 802.11b mode
- Security Mechanism: WEP/WPA-PSK/WPA2-PSK
- Protocols: MQTT (with Birth message and LTW support for availability status)

- TLS version: 1.2
- Current Consumption (typical): 115mA average, 500mA peak
- Operating Temperature: 0°C-40°C(32°F-104°F)

Installation instructions (Wiring)

Connecting the bridge to the alarm system y very simple. Using four wires make the following connections:



- The **CLK** terminal on the bridge to the **YEL** terminal on the alarm panel.
- The **DATA** terminal on the bridge to the **GRN** terminal on the alarm panel.
- The **+** terminal on the bridge to the **AUX+** terminal on the alarm panel.
- The **-** terminal on the bridge to the **AUX-** terminal on the alarm panel.

Probably, the terminals on the panel are already in use. Don't disconnect the connected wires, just add the new ones from the bridge to the terminals.

Because of the low voltage on the terminals, there is no risk of electric shock but while touching the wires, the alarm system could be triggered due the anti-vandalism mechanism. If this happen just disarm the system by entering the code on any keyboard.

If your alarm system is being monitored, be prepared to receive a contact from your monitoring service provider, in case alarm system is triggered. Other option is to put the monitoring service provider in aware of the installation beforehand, to make him dismiss the event.

Connecting Accessories

12v can be supplied from the alarm system through the device and digital Pins 1 and 2 can be used to connect external accessories to be controlled by de device.

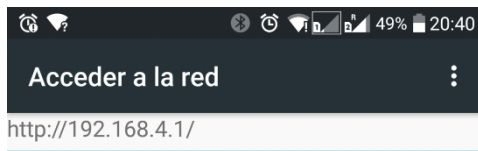
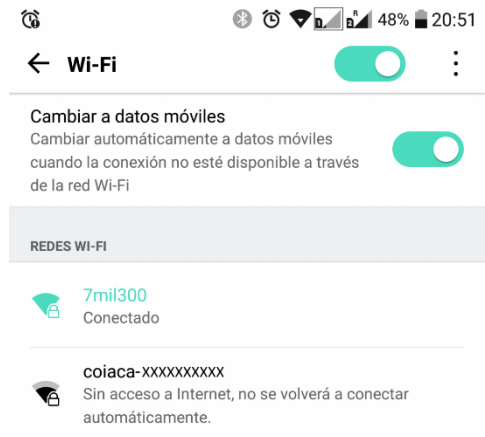
The way the pins are controlled depends on the firmware version. Please refer to the online documentation on coiaca.com to get the reference accordingly.

Device Configuration

WiFi and AP configuration

Every time device starts will be on AP mode (Access Point) for 30 seconds allowing clients to connect directly to make the configuration. Also, when no WiFi network is configured, or the configured network is unavailable, the device will listen for connections as AP.

- Search for available Wi-Fi networks.
- Connect to a network with SSID like coiaca-xxxxxxx (where xxxxxx is the deviceID of your device)
- Use configured password to connect. If device is new, you will find the password on the label sticked on the device. If you don't know the current password, see below.



Coiaca device

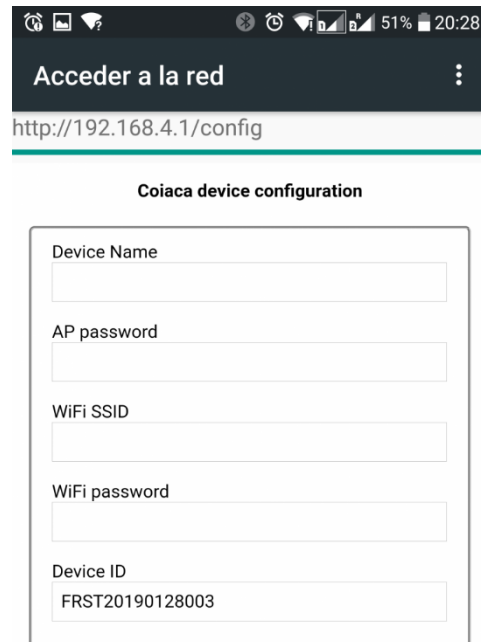
Device ID: **FRST20190128003**

[Config](#)

Once connected, a welcome page will show up. Click or tap on “Config” to enter configuration page.

Enter or edit the following parameters

- **Device Name:** is the SSID name that the device will show when acting as AP (Access Point)
- **AP password:** is the key to connect to the device when acting as AP to be configured. (It's mandatory to set this parameter if device is new. Fill and remember or save it in a safe place.)
- **WiFi SSID:** Is the name of the WiFi network the device will connect through.
- **WiFi password:** Is the password key of the WiFi access point.



Acceder a la red

http://192.168.4.1/config

Coiaca device configuration

Device Name

AP password

WiFi SSID

WiFi password

Device ID

FRST20190128003

Scroll down to the bottom of the page and click on “**Apply**” button to save the changes. The device will restart.

Apply

From now onwards, the device is configured to use the specified WiFi connection (WiFi SSID and WiFi password) and will connect to servers specified on the same config page. Configure servers accordingly to your needs or leave the default parameters to allow the device to be configured remotely later.

Use cases

1. **You turn your Coiaca device on for the first time:** It turns into AP (access point) mode and waits for you to connect. For the first connection the default factory password (printed on the label stucked on the device packaging) is requested. When you connect to the AP, your device will likely automatically pop up the configuration portal page. (a Captive Portal.) with a web interface to set up your local network, and other configurations. When configuration is done, you must disconnect from AP. Then, the device detects that no one is connected, and continues with normal operation.
2. **WiFi configuration is changed (or device is moved to another location with a different network):** When the device cannot connect to the configured WiFi, it falls back to AP mode, and waits for you to change the network configuration. When no configuration was made, then it keeps trying to connect with the already configured

- settings. The device will not switch off the AP while anyone is connected to it, so you must disconnect from the AP when finished with the configuration.
3. **You want to connect to the AP to configure but have forgotten the configured AP WiFi password you set up previously:** The device can be forced to start in AP mode with the default password shipped from factory, usually printed on a label stuck on the product packaging, instead the last configured one. For doing so, follow the steps described below on *“What to do in case of losing or forgetting AP password”* (From this point onwards operation continues as Case 1)
 4. **You want to change the configuration before the device connects to the Internet:** The device always starts up in AP mode and provides you a 30 seconds time frame to connect to it and make any modification to the configuration. You must use the password configured on Case 1 to connect. While anyone is connected to the AP (provided by the device) the AP will stay on until the connection is closed. So, take your time for the changes, the device will wait for you while you are connected to it.
 5. **You want to change the configuration at runtime:** Coiaca devices keeps the config portal up and running even after the WiFi connection is finished. You can connect to the device while connected to the same network entering the device IP address on any browser. In this scenario you will be prompted to enter username “admin” and the password (already configured) to enter the config portal. Note, that the password provided for the authentication is not hidden from devices connected to the same WiFi network. You might want to force rebooting the device to apply your changes and make them persistent.

What to do in case of losing or forgetting AP password.

If you lose or forget the AP password you have configured, you won't be able to access the devices configuration. In this case, the device can be forced to start in AP mode with the default password shipped from factory, usually printed on a label stuck on the product case, instead the last configured one.

- Disconnect the AUX+ wire
- Press the Wifi configuration button
- While pressed, reconnect the AUX+ wire, and then release the button. (Help from a third hand or a clamp could be needed to reconnect the wire while keeping the configuration button pressed)

After connecting the AUX+ wire, the device will start asking for the default credentials.

Status indicator led

This device has a led that represent the connection status.

- **Fast blink:** The device is in AP mode with default factory password waiting to be configured.
- **Fast blink, but mostly on:** The device is in AP mode, waiting for eventual configuration changes (password configured by user must be used).
- **Normal blinks:** Device is attempting connection to the configured WiFi network.

- **Mostly off with rare rapid blinks:** The device is connected to WiFi and is performing normal operation.

Home automation system integration

Coiaca **Bridge BRDSC01 v4** can be easily integrated to any home automation system that supports MQTT protocol.

MQTT broker, topics and some payloads can be configured by the user to integrate the device according to the system of preference.

Home Assistant

MQTT, MQTT Alarm Control Panel and Binary Sensor components are used to integrate Coiaca **BRDSC01 v4** to Home Assistant.

An MQTT broker needs to be already installed and configured on Home Assistant. As an example, the configuration file *configuration.yaml* should include the following:

For every partition a platform should be configured under `alarm_control_panel` component:

```
alarm_control_panel:  
- platform: mqtt  
  name: "Partition 1"  
  state_topic: "DSC01xxxxxxxxx/Partition1"  
  command_topic: "DSC01xxxxxxxxx/cmd"  
  availability_topic: "DSC0xxxxxxxxx/Status"  
  payload_disarm: "1D"  
  payload_arm_home: "1S"  
  payload_arm_away: "1A"  
- platform: mqtt  
  name: "Partition 2"  
  state_topic: "DSC01xxxxxxxxx/Partition2"  
  command_topic: "DSC01xxxxxxxxx/cmd"  
  availability_topic: "DSC010000000001/Status"  
  payload_disarm: "2D"  
  payload_arm_home: "2S"  
  payload_arm_away: "2A"
```

And for displaying zone status, a binary sensor should be configured for each zone:

```
binary_sensor:  
- platform: mqtt  
  name: Trouble  
  state_topic: "DSC01xxxxxxxxx/Trouble"  
  device_class: "problem"  
  payload_on: "1"  
  payload_off: "0"
```

- platform: mqtt
name: Main Door
state_topic: "DSC010000000001/Zone1"
device_class: "door"
payload_on: "1"
payload_off: "0"
- platform: mqtt
name: IRP Living Room
state_topic: "DSC01xxxxxxxxx/Zone2"
device_class: "motion"
payload_on: "1"
payload_off: "0"

Depending on the used interface on Home Assistant *groups.yaml* or *lovelace.yaml* files may need to be updated in order to display components.

Additionally, an access code needs to be configured to use the MQTT Alarm Control Panel component. See "Access Code" on "Advance Configuration".

Others MQTT home automation systems

This device can be integrated with any application or system that supports MQTT protocol. Most known systems are Home Assistant, OpenHab and Hubitat.

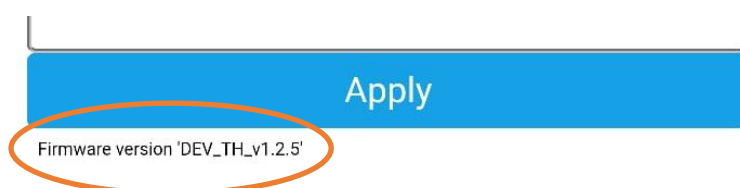
Refer to the application or automation system documentation to know how to configure MQTT options.

Hardware and Firmware versions

If knowing the hardware version of the device is needed, it can be found printed on the board. Refer to me image on the overview section of this document to know where to find it.

The firmware version the device was shipped from factory with, can be found on the printed label stucked on the packaging of the product or can be queried by scanning the QR code.

Since firmware can be updated, the current one could differ from the one originally shipped from factory. If the current firmware was officially provided by Coiaca, its version can be found on the config screen when connecting to the device via Wifi, on AP mode, at the bottom, next to the APPLY button.



Firmware version can also be queried with the Remote Management command `getConfigVersion`. (A complete Remote Management commands reference can be found on coiaca.com)

If device had been updated with a non Coiaca firmware, contact the firmware provider or developer to get support.

Advance configuration

When integrating the device, the configuration usually needs to be adjusted.

The following are the parameters that can be set according to the implementation needs:

Device ID

This is the unique identifier of the device. It's strongly recommended not to modify this parameter.

MQTT server

The server the device will connect to publish its state and to listen for commands. Can be specified as URL or IP address.

The connection to this server is unsecure. To use the device with a secure connection (TLS 1.2) "Force all traffic through this secure connection" option should be used. (See below)

MQTT server port (unsecure)

Is the port MQTT server listens for unsecured connections (usual and default value is 1883)

MQTT user

The username for connecting to MQTT server. This parameter is optional since some brokers may not require it.

MQTT password

The password for connecting to MQTT server. This parameter is optional since some brokers may not require it.

MQTT Client ID

Is the unique identifier that the device will use to connect to the MQTT broker.

When using other services or applications the vendor or provider may need to specify the value to be configured.

The default value is the concatenation of the word "Coiaca" and the default DeviceID (Ex: `CoiacaDSC01000000001`)

Access code

This is the access code required to disarm the DSC Alarm system and may be also required to arm based on panel configuration.

This parameter is mandatory when integrating with MQTT Alarm Control Panel component on Home Assistant



It's a good practice to configure a user code on the alarm system to be used exclusively with the device as Access Code in order to be able to identify the usage on the alarm system log.

Status Topic

The Status Topic is the MQTT topic where the device will publish the Birth Message when connected to the broker, and the Disconnected Message, in case connection with DSC alarm system is lost.

Birth Message

Is the payload of the birth message that the device will publish every time it connects to the MQTT broker or reconnects to DSC alarm system. Default value is "online"

LWT Message (Last Will Message)

Is the payload of the message that the broker will publish automatically on the Status Topic when the device disconnects from the broker. Default value is "offline"

Disconnected Message

Is the payload of the message that the device will publish on the Status Topic when connected to the broker but connection with the DSC alarm system is lost. Default value is "Alarm Disconnected"

Partition Topic Prefix

The device will append the partition number to this prefix to build the topic where the partition state will be published.

For instance, if this parameter is set to DSC01000000001/Partition the state of partition 1 will be published on topic DSC01000000001/Partition1, the state of partition 2 will be published on DSC01000000001/Partition2 and so on and so forth.

Payloads for partition states are: disarmed, armed_away, armed_home, triggered and pending.

Active Partition Topic

The device will publish the active partition on this topic. Meaning that every time user change to a partition to send a command, this data will change.

Zone Topic Prefix

The device will append the zone number to this prefix to build the topic where the zone state will be published.

For instance, if this parameter is set to DSC01000000001/Zone the state of zone 1 will be published on topic DSC01000000001/Zone1, the state of zone 2 will be published on DSC01000000001/Zone2 and so on and so forth.

Zone payloads are 1 for active and 0 for inactive.

Fire Topic Prefix

The device will append the partition number to this prefix to build the topic where the fire state of the partition will be published.

For instance, if this parameter is set to DSC010000000001/Fire the fire state of partition 1 will be published on topic DSC010000000001/Fire1, the fire state of partition 2 will be published on DSC010000000001/Fire2 and so on and so forth.

Fire payload is 1 when active and 0 when inactive.

Trouble Topic

The device will publish the trouble status in this topic.

Trouble payload is 1 when trouble reported and 0 when no trouble.

Commands Topic

This is the topic the device will subscribe to receive the commands and messages to send to the alarm system. Keys pressed on the virtual keypad will be also published on this topic.

Keep Alive interval (seconds)

If this parameter is greater than 0, the device will publish a keep alive message every time this interval is elapsed.

The message payload depends on firmware version but usually includes a timestamp, the state of the connection with the Alarm system and with MQTT brokers.

Keep Alive Topic

Is the topic where the keep alive message will be published.

Timer ON

If set to YES enables the timer feature. Default value is NO

For disarming alarm system with the timer, the Access Code, needs to be specified. (Please refer to “Access Code” parameter on this section)



Be aware that disarming the alarm system with a timer could imply a security risk.

Timer String

Is the string needed to program the timer feature.

Timer String format

Timer Strings contains 7 characters substrings including information about each action to be performed, the target partition, and the moment these actions will be triggered.

First characters of the substring represent the day of the week, or the day combination when the action will be triggered. Day combination character list is as follows:

A: Monday

B: Tuesday

C: Wednesday
D: Thursday
E: Friday
F: Saturday
G: Sunday
H: Mo, Tu, We, Th, Fr, Sa, Su
I: Mo, Tu, We, Th, Fr
J: Sa, Su
K: Mo, Tu, We, Th, Fr, Sa
L: Mo, We, Fr,
M: Tu, Th, Sa
N: Mo, Tu, We
O: Th, Fr, Sa
P: Mo, We, Fr, Su

Next four characters represent the time when action will be triggered, in 24hs format without separators. For instances 13:30hs is “1330” and 18:30hs is “1830”

Next character represents the action itself: 1 to arm stay, 2 to arm away and 0 to disarm.

The last character represents the target partition. Must be indicated with the partition number.

Example String:

Ex. “H090001H205911G030001G033021”

In the given example, partition 1 will be disarmed at 9hs and will be armed away at 20:59hs every day. Also, partition 1 will be disarmed every Sunday at 3am and will be armed stay at 3:30am, same day.

Publish Timer String

When enabled, this option will make the device to publish timer string every time keep alive message is published, if enabled. Default value is NO

NTP server

Is the time server to retrieve the date and time information from. Default value is pool.ntp.org

Time Zone

Indicates the time zone the device will operate timers.

NTP Update interval (seconds)

Is the interval in seconds between the attempts of NTP feature to retrieve the time from server to stay synced and updated. Default value is 300 (5 minutes)

DST (Daylight Saving Time)

When enabled, this option will apply DST (Daylight Saving Time) offset to the time retrieved from server. Default value is NO (disabled)

MQTT Retain

MQTT retain value for publishing MQTT messages. Default value is 0 (zero, false)

MQTT QoS

MQTT QoS value for publishing MQTT messages. Default value is 0 (zero)

Monitoring feature

When enabled, this feature will publish, in the Remote Management broker, the status of partitions and zones. The topics are built using the specified prefix on configuration and the information to be published depends on the level the feature is enabled on.

This feature requires the Remote Management MQTT broker configured in order to work properly.

Enable Monitoring parameter

This parameter defines the level of information to publish for monitoring purposes:

- If set to 0, the feature is disabled and no data will be transmitted.
- If set to 1, partitions statuses are always informed as NORMAL except when triggered that are informed as TRIGGERED. This is the option that discloses the less information while enabling the monitoring feature.
- If set to 2, partitions statuses are informed as ARMED HOME, ARMED AWAY, DISARMED, PENDING and TRIGGERED.
- If set to 3, partitions statuses are informed like option 2, but zone status will be also informed as ACTIVE or INACTIVE. This is the most information disclosive option

TROUBLE and FIRE statuses are informed in all options except on 0 (feature disabled). Payloads for Trouble and Fire are 1 when active and 0 when inactive.

Monitoring Topic Prefix

The device will build the topics of the monitoring feature using the prefix specified in this parameter.

Default value is MNTR/deviceId. "MNTR/DSC010000000001", for instance.

And taking the example above, topics shall be created as follows:

- MNTR/DSC010000000001/Trouble
- MNTR/DSC010000000001/Partition1
- MNTR/DSC010000000001/Partition2
- MNTR/DSC010000000001/Fire1
- MNTR/DSC010000000001/Zone1
- MNTR/DSC010000000001/Zone2
- MNTR/DSC010000000001/Zone3

Remote Management

Remote management is a feature that allows to control a Coiaca device remotely. Once this feature is enabled and configured on the device, you will be able to send commands and receive responses from the unit that lets you update configuration, perform operations and/or simulate user intervention.

All these remote management tasks can be performed without interfere on the main functionality of the device. That is why Coiaca devices are perfect for service providers that needs to control devices installed in places where physical access is difficult, restricted or sometimes unreachable.

Remote management commands reference can be found on coiaca.com

The following are the parameters for the Remote Management feature:

Enable Remote Management

When enabled, Remote Management feature is enabled. Default value is YES (enabled)

Remote Management Password

The password to be included as “pwd” param in JSON payload in MQTT messages to issue a Remote Management command.

This password is usually printed on a label sticked on the device. Be careful when updating this password because if forgotten, it won't be possible to control the device with Remote Management until this password is reseted. For resetting this password, connect locally when the device is acting as AP will be needed.

Remote Management MQTT server

The server the device will connect to listen for Remote Management commands and publish command results. The connection to this server mandatory secure (TLS 1.2)

Remote Management MQTT server port (TLS)

Is the port Remote Management MQTT server listens for secured connections (usual and default value is 8883)

Remote Management MQTT user

Username device will use to connect to Remote Management broker

Remote Management MQTT password

Password device will use to connect to Remote Management broker

Force all traffic through the secure connection

If enable, this option will force the device not to use the main MQTT server connection that is unsecure. Only the broker specified for Remote Management will be used for all matters and all traffic will take place though its secure connection.

Default value is YES (enabled)

Remote Management Command Topic

Is the MQTT topic the device will subscribe to listen for Remote Management commands. The default value is the concatenation of "RMgmt/" and the default DeviceID. (Ex: RMgmt/PSW3S1000000001)

Remote Management Result Topic

Is the MQTT topic where the device will publish the results after executing a Remote Management command. The default value is the concatenation of "RMgmt/", the default DeviceID and "/results". (Ex: RMgmt/PSW3S1000000001/results)

Remote Management MQTT Retain

MQTT retain value for publishing MQTT messages on Remote Management broker. Default value is 0 (zero, false)

Remote Management MQTT QoS

MQTT QoS value for publishing MQTT messages on Remote Management broker. Default value is 0 (zero)

MQTT Debugging feature

Sometimes is needed to know what is happening on the device and you don't have physical access to connect and debug. You can enable the MQTT debugging feature to get some debug information remotely.

This feature requires the Remote Management MQTT broker to be configured in order to work properly.

Enable MQTT Debug parameter

When enabled, the device will publish on the specified topic, everything that happens on the device in a readable format, including deviceID.

Default value is 0 (zero, disabled).

MQTT Debug Topic

Is the topic where debug messages are published when MQTT debug feature is enabled.

Disclaimer

It is prohibited to reproduce, transmit or distribute part or all of the contents of this document in any form, without written permission from Coiaca.

Coiaca reserves the rights to modify, improve, replace or cancel this product without any prior notification.

Coiaca reserves the rights to change or cancel the content of this document without any prior notification.

Warranty

This Limited Warranty applies to Coiaca products still within their original warranty period.

You may need only simple instructions to correct a problem with your product. Try our website at coiaca.com, rather than going to your retailer. If the problem cannot be solved with the troubleshooting information available online, you will be offered express factory service. Please do not send any products to Coiaca without contacting us first.

Limited Hardware Warranty

Coiaca warrants to the original purchaser that the hardware product shall be free from defects in material and workmanship for three (3) months from the date of purchase. If a defect covered by this warranty occurs during this warranty period, Coiaca will repair or replace the defective hardware product or component, free of charge.* The original purchaser is entitled to this warranty only if the date of purchase is registered at point of sale or the consumer can demonstrate, to Coiaca's satisfaction, that the product was purchased within the last 3 months.

Service after expiration of warranty

Please try our website at coiaca.com for troubleshooting information and repair or replacement options and pricing.*

* In some instances, it may be necessary for you to ship the complete product, FREIGHT PREPAID AND INSURED FOR LOSS OR DAMAGE, to Coiaca. Please do not send any products to Coiaca without contacting us first.

Warranty Limitations

This warranty shall not apply if this product has been damaged by products not sold or licensed by Coiaca (including, but not limited to, adapters, software, and power supplies).

In addition, this warranty shall not apply if this product (a) is used for commercial purposes (including rental); (b) is damaged by any unauthorized modifications or tampering; (c) is damaged by negligence, accident, unreasonable use, or by other causes unrelated to defective materials or workmanship; (d) has had the serial number altered, defaced or removed; or (e) has been intentionally modified using malicious code, malware, virus, bots, worms, trojans, backdoors, exploits, cheats, hacks, or hidden diagnostics that may harm the product or our systems.

Any applicable implied warranties, including warranties of merchantability and fitness for a particular purpose, are hereby limited in duration to the warranty periods described above. In no event shall Coiaca be liable for consequential or incidental damages resulting from the breach of any implied or express warranties.