

Bridge DSC01 v2.1

Manual de Usuario

(Rev 1.4.9)

Septiembre 2021

Esta página ha sido intencionalmente dejada en blanco

Contenido

Contenido	3
Introducción	7
Funcionalidades.....	7
Especificaciones técnicas	7
Instrucciones para la instalación (Cableado)	8
Conectando Accesorios	8
Configuración del dispositivo	8
Configuración de la conexión Wifi y el punto de acceso	8
Casos de uso	10
Qué hacer en caso de perder u olvidar la contraseña AP.	11
Led indicador de estatus	11
Integración a sistemas de automatización hogareña	12
Home Assistant	12
Otros sistemas de domótica MQTT.....	13
Versiones de Hardware y Firmware	13
Configuración Avanzada.....	14
Device ID.....	14
MQTT server.....	14
MQTT server port (unsecure).....	14
MQTT user	14
MQTT password	14
MQTT Client ID	14
Access code	15
Status Topic	15
Birth Message.....	15
LWT Message (Last Will Message)	15
Disconnected Message.....	15
Partition Topic Prefix.....	15
Active Partition Topic	16
Zone Topic Prefix.....	16
Fire Topic Prefix.....	16
Trouble Topic.....	16

- Commands Topic..... 16
- Keep Alive interval (seconds) 16
- Keep Alive Topic 16
- Timer ON 16
- Timer String 17
- Publish Timer String 18
- NTP server 18
- Time Zone 18
- NTP Update interval (seconds)..... 18
- DST (Daylight Saving Time)..... 18
- MQTT Retain 18
- MQTT QoS 18
- Función de monitoreo..... 18
 - Enable Monitoring parameter..... 18
 - Monitoring Topic Prefix..... 19
- Administración Remota..... 19
 - Enable Remote Management 19
 - Remote Management Password..... 19
 - Remote Management MQTT server 20
 - Remote Management MQTT server port (TLS)..... 20
 - Remote Management MQTT user..... 20
 - Remote Management MQTT password 20
- Force all traffic through the secure connection..... 20
 - Remote Management Command Topic 20
 - Remote Management Result Topic..... 20
 - Remote Management MQTT Retain 20
 - Remote Management MQTT QoS..... 20
- Funcionalidad de depuración (debugging) por MQTT 21
 - Enable MQTT Debug parameter 21
 - MQTT Debug Topic..... 21
- Renuncias 21
- Garantía..... 21
 - Garantía limitada del Hardware..... 21

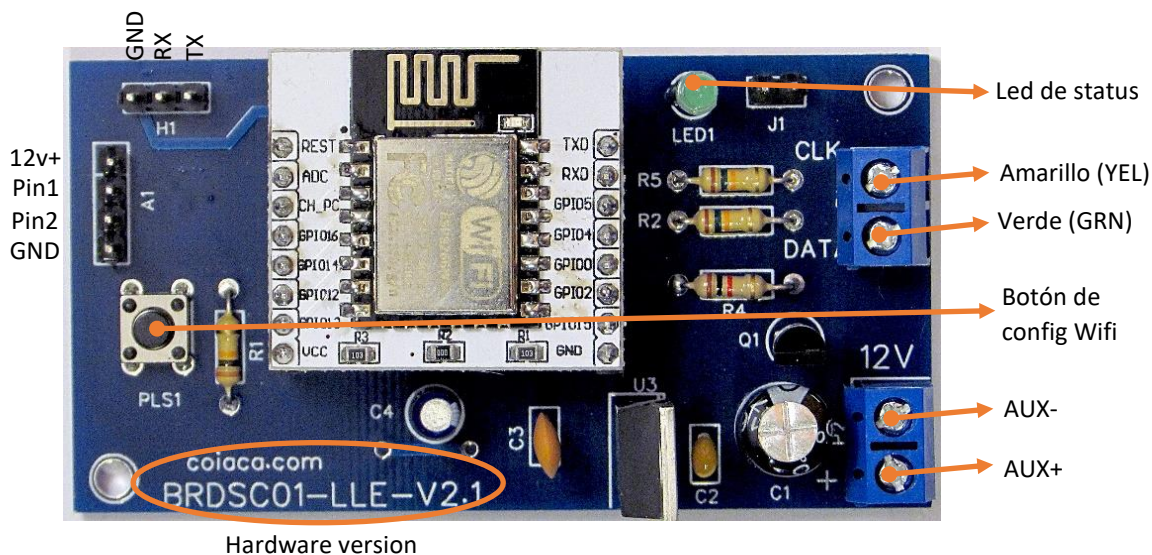
Servicio después del vencimiento de la garantía 22

Limitaciones de la garantía..... 22

Esta página ha sido intencionalmente dejada en blanco

Introducción

Coiaca **BRDSC01 v2.1** es una interface que permite controlar alarmas DSC PowerSeries con aplicaciones móviles y web e integrarla a sistemas de automatización que soporten el protocolo MQTT.



Funcionalidades

- Tracking de los estados de las particiones 1 a 8: armado, desarmado, disparo y fuego
- Tracking de estado de falla (Trouble)
- Tracking de los estados de las zonas 1 a 64
- Permite escribir en el panel para las particiones 1 a 8
- Cableado super fácil
- 2 pines digitales para conectar accesorios de entrada o de salida.
- Conectores de programación "in circuit"
- Canal de comunicación seguro mediante TLS
- Led indicador de estatus
- Pulsador para la configuración WiFi
- Administración Remota
- Capacidad para el monitoreo
- Funcionalidad de depuración MQTT

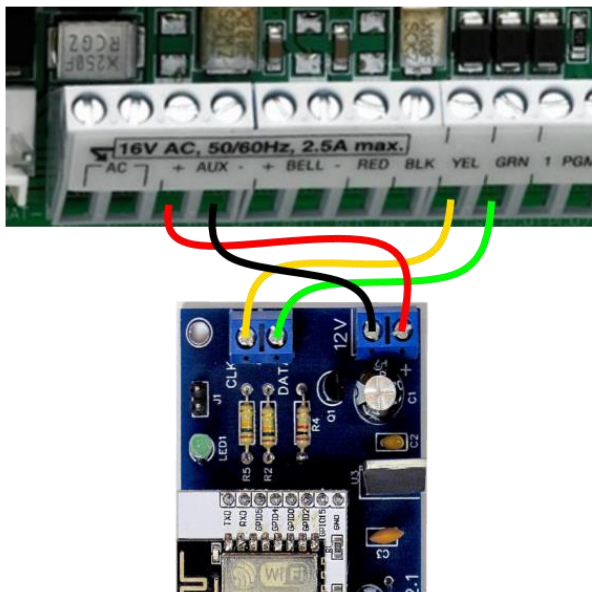
Especificaciones técnicas

- Dimensiones: 75mm x 38mm x 20mm
- Alimentación: DC12V desde el sistema de alarma.
- Standard inalámbrico: WiFi 802.11 b/g/n
- Antena incorporada +19.5dBm de salida en modo 802.11b
- Mecanismo de seguridad: WEP/WPA-PSK/WPA2-PSK
- Protocolo: MQTT (con Birth message y LTW para estatus de disponibilidad)
- TLS versión: 1.2

- Consumo (típico): 115mA promedio, 500mA pico
- Temperatura de operación: 0°C-40°C(32°F-104°F)

Instrucciones para la instalación (Cableado)

Conectar la interface al sistema de alarma es muy simple. Usando cuatro cables haga las siguientes conexiones:



- La terminal **CLK** de la interface al terminal **YEL** del sistema de alarma.
- La terminal **DATA** de la interface a la terminal **GRN** del sistema de alarma.
- El terminal **+** de la interface al a terminal **AUX+** del sistema de alarma.
- El terminal **-** de la interface al terminal **AUX-** del sistema de alarma.

Probablemente, los terminales ya estén en uso. No desconecte los cables conectados, solo agregue los nuevos de la interface.

Debido al bajo voltaje, el sistema de alarma podría dispararse por los mecanismos anti-vandalismo. Si esto sucede, simplemente desarme el sistema ingresando el código en cualquier teclado.

Si su sistema de alarma está siendo monitoreado y se dispara, recibirá un contacto de su proveedor de servicios de monitoreo. Una opción es informar a su proveedor de servicio de monitoreo de antemano acerca de la instalación para que ignore el disparo.

Conectando Accesorios

Puede suministrarse 12v DC desde el sistema de alarma a través de la interface y los pines 1 y 2 pueden ser usados para controlar accesorios.

La forma en que se controlan los pines depende de la versión del firmware. Consulte la documentación en línea en coiaca.com para obtener la referencia correspondiente.

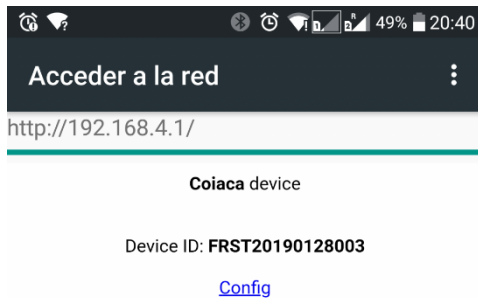
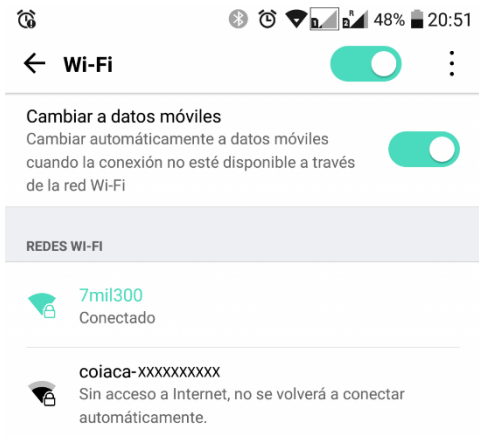
Configuración del dispositivo

Configuración de la conexión Wifi y el punto de acceso

Cada vez que se inicie el dispositivo, lo hará en modo AP (punto de acceso) durante 30 segundos, para permitir conexiones directas para realizar la configuración. Además, cuando no

hay una red WiFi configurada, o la red configurada no está disponible, el dispositivo escuchará las conexiones como AP.

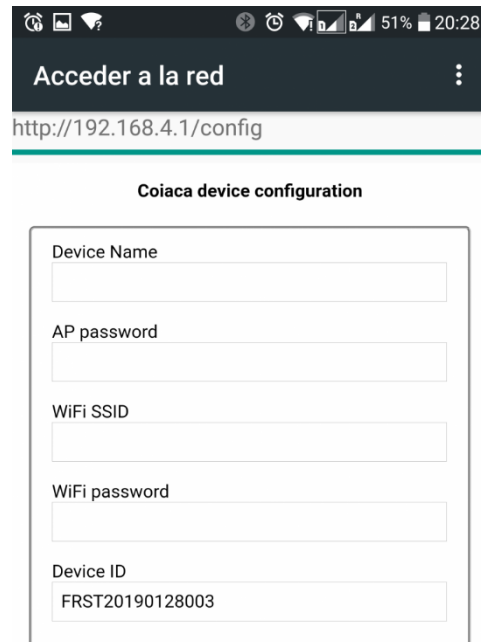
- Con una PC o un dispositivo móvil, busque las conexiones disponibles.
- Conéctese a una red con SSID similar a coiaca-xxxxxxx (donde xxxxxx es el deviceID de su dispositivo)
- Utilice la contraseña configurada previamente para conectarse. Si el dispositivo es nuevo, encontrará la contraseña en la etiqueta que acompaña el producto. Si no conoce la contraseña actual, lea más abajo.



Una vez conectado, verá una pantalla de inicio de sesión que aparecerá. Toque en “Config” para ingresar a la página de configuración.

Ingrese o edite los siguientes parámetros:

- **Device Name:** Es el SSID (nombre de la red Wifi) que se mostrará cuando el dispositivo se encuentre en modo AP (Access Point)
- **AP password:** es la contraseña para conectarse al dispositivo para configurarlo cuando éste se encuentra en modo AP. (es obligatorio configurar este parámetro. Complételo y recuérdelo o guárdelo en un lugar seguro.)
- **WiFi SSID:** Es el nombre de la red Wifi a la que el dispositivo se conectará para funcionar.
- **WiFi password:** Es la contraseña de la red Wifi a la que el dispositivo se conectará para funcionar.



Desplácese hasta el final de la página y toque en el botón **“Apply”** para guardar la configuración. El dispositivo se reiniciará.

Apply

Desde ahora, el dispositivo está configurado para usar una red Wifi específica y se conectará a los servidores especificados en la misma página. Configure los servidores de acuerdo con sus necesidades, o deje los campos sin modificar para utilizar los valores predeterminados. Podrá cambiar estos valores más tarde.

Casos de uso

1. **Enciende su dispositivo Coiaca por primera vez:** Inicia en modo AP (punto de acceso) y espera conexiones para ser configurado. Para la primera conexión, se solicita la contraseña predeterminada de fábrica (impresa en la etiqueta que acompaña al dispositivo). El dispositivo probablemente abrirá automáticamente la página del portal de configuración. (el portal cautivo) con una interface web para configurar su red local y otras configuraciones. Luego de realizar la configuración, debe desconectarse del AP, el dispositivo detecta que no hay nadie conectado y continúa con el funcionamiento normal.
2. **Se cambió la configuración de WiFi (o el dispositivo se movió a otra ubicación):** Cuando el dispositivo no puede conectarse a la red WiFi configurada, vuelve al modo AP para recibir conexiones para que se cambie la configuración de la red. Cuando no se realizó ninguna configuración, sigue intentando conectarse con las configuraciones ya configuradas. El dispositivo no apagará el AP mientras haya alguien conectado a él, por lo que debe desconectarse del AP cuando haya terminado con la configuración.

3. **Ud. quiere conectarse al AP para configurar el dispositivo, pero ha olvidado la contraseña que configuró anteriormente:** El dispositivo puede forzarse a iniciar en modo AP con la contraseña predeterminada enviada de fábrica, generalmente impresa en una etiqueta que acompaña al producto, en lugar de la última configurada. Para hacerlo, siga los pasos descritos a continuación en "*Qué hacer en caso de perder u olvidar la contraseña AP*" (a partir de ahí, la operación continúa como el Caso 1)
4. **Ud. quiere cambiar la configuración antes de que el dispositivo se conecte a Internet:** El dispositivo siempre se inicia en modo AP y le proporciona un intervalo de 30 segundos para conectarse y realizar cualquier modificación en la configuración. Debe usar la contraseña configurada en el Caso 1 para conectarse. Mientras alguien esté conectado al AP, este permanecerá encendido hasta que se cierre la conexión. Por lo tanto, tómate tu tiempo para realizar los cambios, el dispositivo esperará mientras este conectado a él.
5. **Ud. quiere cambiar la configuración mientras el dispositivo está funcionando:** Los dispositivos Coiaca mantienen el portal de configuración en funcionamiento incluso después de que finalice la conexión WiFi. Puede conectarse al dispositivo mientras está conectado a la misma red ingresando su dirección IP en cualquier navegador. En este escenario, se le pedirá que ingrese el nombre de usuario "admin" y la contraseña (ya configurada) para ingresar al portal de configuración. Tenga en cuenta que la contraseña provista para la autenticación no está oculta de los dispositivos conectados a la misma red WiFi. Es necesario el reinicio del dispositivo para aplicar sus cambios y hacerlos persistentes.

Qué hacer en caso de perder u olvidar la contraseña AP.

Si pierde u olvida la contraseña AP que configuró, no podrá acceder a la configuración de los dispositivos. En este caso, el dispositivo puede forzarse a iniciar en modo AP con la contraseña predeterminada enviada de fábrica, generalmente impresa en una etiqueta que acompaña al producto, en lugar de la última configurada.

- Desconecte el cable AUX+
- Presione el botón de configuración Wifi
- Con el botón presionado, reconecte el cable AUX+, y suelte el botón. (Podría necesitar ayuda de una tercera mano o una abrazadera para volver a conectar el cable mientras mantiene presionado el botón de configuración Wifi)

Luego de conectar el cable AUX+, el dispositivo iniciara en modo AP solicitando la contraseña predeterminada.

Led indicador de estatus

El dispositivo posee un led que representa el estado de la conexión

- **Parpadeo rápido:** El dispositivo está en modo AP con la contraseña predeterminada de fábrica a la espera de ser configurado.

- **Parpadeo rápido, mayormente encendido:** El dispositivo está en modo AP, esperando eventuales cambios de configuración (se debe usar la contraseña configurada por el usuario).
- **Parpadeo normal:** El dispositivo está intentando conectarse a la red WiFi configurada.
- **Mayormente apagado con parpadeos rápidos:** El dispositivo está conectado y operando normalmente.

Integración a sistemas de automatización hogareña

La interface Coiaca **BRDSC01 v2.1** puede ser integrada fácilmente a sistemas de automatización de hogar (domótica) que soporten el protocolo MQTT.

El broker MQTT, los tópicos y los contenidos de los mensajes pueden ser configurados para integrar el dispositivo de acuerdo al sistema de preferencia.

Home Assistant

Los components MQTT, MQTT Alarm Control Panel y Binary Sensor son utilizados para integrar la interface Coiaca **BRDSC01 v2.1** a Home Assistant.

Es necesario que un broker MQTT se encuentre instalado y configurado en Home Assistant. Como ejemplo, el archivo de configuración *configuration.yaml* deberá incluir lo siguiente:

Para cada partición debe configurarse una plataforma (platform) para el componente alarm_control_panel:

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: "DSC01000000001/Status"
 payload_disarm: "2D"
 payload_arm_home: "2S"
 payload_arm_away: "2A"
```

Y para mostrar los estatus de las zonas, debe configurarse un sensor binario (binary sensor) para cada zona:

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: "DSC01000000001/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"

Dependiendo de la interface implementada para el front end de Home Assistant, el archivo *groups.yaml* o *lovelace.yaml* deberán ser actualizados para visualizar los componentes.

Adicionalmente, el código de acceso debe ser configurado para utilizar el componente MQTT Alarm Control Panel. Ver "Access Code" en " Configuración Avanzada".

### Otros sistemas de domótica MQTT

Este dispositivo puede integrarse con aplicaciones y sistemas que soporten el protocolo MQTT. Entre los más conocidos se encuentran Home Assistant, OpenHab y Hubitat.

Consulte la documentación de la aplicación o del sistema de domótica para saber cómo configurar las opciones MQTT.

### Versiones de Hardware y Firmware

Si necesita conocer la versión de hardware del dispositivo, ésta se encuentra impresa en la placa. En la imagen incluida en la introducción de este manual podrá ver dónde encontrarla.

La versión de firmware con la que el dispositivo salió de la fábrica se encuentra en la etiqueta impresa que acompaña al producto.

Debido a que el firmware del dispositivo puede ser actualizado, el actual puede ser diferente del original. Si el firmware actual ha sido provisto oficialmente por Coiaca, su versión puede encontrarse en la pantalla de configuración conectándose por Wifi cuando el dispositivo se encuentra en modo AP, al pie, junto al botón APPLY.



La versión de firmware también puede ser consultada con el comando de Administración Remota `getConfigVersion`. (Una referencia completa de los comandos de Administración Remota, puede encontrarse en [coiaca.com](http://coiaca.com))

Si el dispositivo ha sido actualizado con una versión de firmware no provista por Coiaca, contacte al proveedor del firmware o al desarrollador para obtener soporte.

## Configuración Avanzada

Para ser integrado a otros sistemas, la configuración puede requerir ajustes.

Los siguientes son los parámetros que pueden ser especificados de acuerdo con las necesidades de cada implementación:

### Device ID

Es el identificador único del dispositivo. Es altamente recomendado no modificar este parámetro.

### MQTT server

El servidor al que se conectará el dispositivo para publicar su estado y escuchar los comandos. Se puede especificar como URL o dirección IP.

La conexión a este servidor no es segura. Para utilizar el dispositivo con una conexión segura (TLS 1.2), se debe utilizar la opción "Forzar todo el tráfico a través de ésta conexión segura". (Ver más abajo)

### MQTT server port (unsecure)

Es el puerto en el que el servidor MQTT escucha conexiones no seguras. (el valor usual y predeterminado es 1883)

### MQTT user

El nombre de usuario para conectarse al servidor MQTT. Este parámetro es opcional ya que algunos brokers pueden no requerirlo.

### MQTT password

La contraseña para conectarse al servidor MQTT. Este parámetro es opcional ya que algunos brokers pueden no requerirlo.

### MQTT Client ID

Es el identificador único que utilizará el dispositivo para conectarse al broker MQTT.

Al usar otros servicios o aplicaciones, el proveedor puede necesitar especificar este valor.

El valor predeterminado es la concatenación de la palabra "Coiaca" y el deviceID predeterminado (Ej: CoiacaDSC01000000001)

#### Access code

Este es el código de acceso requerido para desarmar el sistema de alarma DSC y también puede ser requerido para armar según la configuración del panel.

Este parámetro es obligatorio cuando se integra con el componente MQTT Alarm Control Panel en Home Assistant



**Es una buena práctica configurar un código de usuario en el sistema de alarma para que se use exclusivamente con el dispositivo como Código de Acceso para poder identificar el uso en el registro del sistema de alarma..**

#### Status Topic

El Status Topic es el tópico MQTT en el que el dispositivo publicará el birth message cuando se conecte al broker, y el "Disconnected Message", en el caso de que se pierda la conexión con el sistema de alarma DSC.

#### Birth Message

Es el contenido del "birth message" que el dispositivo publicará cada vez que se conecte al broker MQTT o se vuelva a conectar al sistema de alarma DSC. El valor predeterminado es "online"

#### LWT Message (Last Will Message)

Es el contenido del "Last Will Message" que el broker publicará en el Status Topic cuando el dispositivo se desconecte. El valor predeterminado es "offline"

#### Disconnected Message

Es contenido del mensaje que el dispositivo publicará en el Status Topic cuando se encuentra conectado al broker, pero se pierde la conexión con el sistema de alarma DSC. El valor predeterminado es "Alarm Disconnected"

#### Partition Topic Prefix

El dispositivo agregará el número de partición a este prefijo para construir el topico donde se publicará el estado de la partición.

Por ejemplo, si este parámetro se establece en DSC01000000001/Partition, el estado de la partición 1 se publicará sobre el tema DSC01000000001/Partition1, el estado de la partición 2 se publicará en DSC01000000001/Partition2 y así sucesivamente.

Los contenidos de los mensajes para los estados de partición son: disarmed (desarmado), armed\_home (armado en casa), armed\_away (Armado fuera de casa), triggered (disparada) y pending (pendiente).

#### Active Partition Topic

El dispositivo publicará la partición activa en este tópico. Lo que significa que cada vez que el usuario cambia a una partición para enviar un comando, este dato cambiará.

#### Zone Topic Prefix

El dispositivo agregará el número de zona a este prefijo para crear el tópico donde se publicará el estado de cada zona.

Por ejemplo, si este parámetro se establece en DSC01000000001/Zone, el estado de la zona 1 se publicará sobre el tema DSC01000000001/Zone1, el estado de la zona 2 se publicará en DSC01000000001/Zone2 y así sucesivamente.

El contenido de los mensajes para los estados de zona son 1 para activo y 0 para inactivo.

#### Fire Topic Prefix

El dispositivo agregará el número de partición a este prefijo para construir el tópico donde se publicará el estado de incendio de la partición.

Por ejemplo, si este parámetro se establece en DSC01000000001/Fire, el estado de incendio de la partición 1 se publicará sobre el tema DSC01000000001/Fire1, el estado de incendio de la partición 2 se publicará en DSC01000000001/Fire2 y así sucesivamente.

El contenido de los mensajes de estado del indicador de incendio es 1 cuando está activa y 0 cuando está inactiva.

#### Trouble Topic

El dispositivo publicará en este tópico si el sistema de alarma reporte problemas (trouble).

El contenido del mensaje cuando se reportan problemas es 1 y 0 cuando no existen problemas.

#### Commands Topic

Este es el tópico al que el dispositivo se suscribirá para recibir comandos y mensajes para enviar al sistema de alarma. Las teclas presionadas en el teclado virtual también se publicarán sobre este tópico.

#### Keep Alive interval (seconds)

Si este parámetro es mayor que 0, el dispositivo publicará un mensaje cada vez que transcurra este intervalo.

El contenido del mensaje depende de la versión del firmware, pero generalmente incluye una marca de tiempo, el estado de la conexión con el sistema de alarma, con los brokers MQTT y la intensidad de la señal Wifi.

#### Keep Alive Topic

Es el tópico donde se publicará el mensaje del punto anterior.

#### Timer ON

Si se establece en YES, habilita la función de temporizador. El valor predeterminado es NO

Para desarmar el sistema de alarma con el temporizador, es necesario configurar el Código de acceso. (Consulte el parámetro "Access Code" en esta sección)





**Tenga en cuenta que desarmar el sistema de alarma con un temporizador podría implicar un riesgo de seguridad.**

## Timer String

¿Es la cadena de caracteres con la que se configura la función del temporizador?.

### *Timer String format*

El Timer Strings contiene 7 partes que incluyen información sobre cada acción que se realizará, la partición de destino y el momento en que se desencadenarán estas acciones.

**La primera parte es el primer caracter de la cadena que representa el día de la semana o la combinación de días en los que se activará la acción.** Las combinaciones de días son las siguientes:

- A: Lunes
- B: Martes
- C: Miércoles
- D: Jueves
- E: Viernes
- F: Sábado
- G: Domingo
- H: Lunes, Martes, Miércoles, Jueves, Viernes, Sábado, Domingo
- I: Lunes, Martes, Miércoles, Jueves, Viernes
- J: Sábado, Domingo
- K: Lunes, Martes, Miércoles, Jueves, Viernes, Sábado
- L: Lunes, Miércoles, Viernes
- M: Martes, Jueves, Sábado
- N: Lunes, Martes, Miércoles
- O: Jueves, Viernes, Sábado
- P: Lunes, Miércoles, Viernes, Sábado

**Los siguientes cuatro caracteres representan la hora en que se activará la acción,** en formato de 24hs sin separadores. Por ejemplo 13: 30hs es "1330" y 18: 30hs es "1830"

**El siguiente personaje representa la acción:** 1 para armar en casa, 2 para armar fuera de casa y 0 para desarmar.

**El último carácter representa la partición sobre la que se ejecutará la acción.** Debe indicarse con el número de partición.

Ejemplo:

Ex. "H090001H205911G030001G033021"

En el ejemplo, la partición 1 se desarmará a las 9hs y se armará a las 20: 59hs todos los días. Además, la partición 1 se desarmará todos los domingos a las 3 a.m. y se mantendrá armado a las 3:30 a.m., el mismo día.

#### Publish Timer String

Cuando está habilitada, esta opción hará que el dispositivo publique el Tomer String cada vez que se publique un mensaje de Keep Alive, si está habilitado. El valor predeterminado es NO

#### NTP server

Es el servidor de hora de internet a la que el dispositivo se conectará para obtener la fecha y hora. El valor predeterminado es pool.ntp.org

#### Time Zone

Indica la zona horaria con la que el dispositivo operará los temporizadores.

#### NTP Update interval (seconds)

Es el intervalo de tiempo (en segundos) entre los intentos de la función NTP para obtener la fecha y hora para permanecer sincronizado y actualizado. El valor predeterminado es 300 (5 minutos)

#### DST (Daylight Saving Time)

Cuando está habilitada, esta opción aplicará el DST (horario de verano) a la hora obtenida del servidor. El valor predeterminado es NO (deshabilitado)

#### MQTT Retain

Valor del parámetro RETAIN para los mensajes MQTT. El valor predeterminado es 0 (cero, falso)

#### MQTT QoS

Valor del parámetro QoS para los mensajes MQTT. El valor predeterminado es 0 (cero)

## Función de monitoreo

Cuando está habilitada, esta función publicará, en el broker de Administración Remota, el estado de las particiones y zonas. Los tópicos se crean utilizando el prefijo especificado en la configuración y la información que se publicará depende del nivel en el que esté habilitada la función.

Esta función requiere que el broket MQTT de Administración Remota esté configurado para funcionar correctamente.

#### Enable Monitoring parameter

Este parámetro define el nivel de información a publicar para fines de monitoreo:

- Si se establece en 0, la función se desactiva y no se transmitirán datos.
- Si se establece en 1, los estados de las particiones siempre se informan como NORMAL, excepto cuando se disparan y se informan como TRIGGERED. Esta es la opción que revela la menor cantidad de información mientras la función de monitoreo se encuentra habilitada.
- Si se establece en 2, los estados de las particiones se informan como ARMED HOME, ARMED AWAY, DISARMED, PENDING and TRIGGERED.

- Si se establece en 3, los estados de las particiones se informan como en la opción 2, pero los estados de las zonas también se informarán como ACTIVO o INACTIVO. Esta es la opción que más información revelará.

Los estados de TROUBLE y FIRE se informan en todas las opciones excepto en 0 (función deshabilitada). Los contenidos de los mensajes para problema e incendio son 1 cuando está activo y 0 cuando está inactivo.

#### Monitoring Topic Prefix

El dispositivo creará los tópicos de la función de monitoreo utilizando el prefijo especificado en este parámetro.

El valor predeterminado es MNTR/deviceId. "MNTR/DSC010000000001", por ejemplo.

Y tomando como ejemplo el anterior, los tópicos se crearán de la siguiente manera:

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

## Administración Remota

La Administración Remota es una funcionalidad que permite controlar un dispositivo Coiaca de forma remota. Una vez que esta función esté habilitada y configurada en el dispositivo, podrá enviar comandos y recibir respuestas de la unidad, que permiten actualizar la configuración, realizar operaciones y/o simular la intervención del usuario.

Todas estas tareas de administración remota se pueden realizar sin interferir en la funcionalidad principal del dispositivo. Es por eso que los dispositivos Coiaca son perfectos para proveedores de servicios que necesitan controlar dispositivos instalados en lugares donde el acceso físico es difícil, restringido o, a veces, inalcanzable.

La referencia completa y actualizada de comandos Administración Remota se encuentra en [coiaca.com](http://coiaca.com)

Los siguientes son los parámetros para configurar la funcionalidad de Administración Remota:

#### Enable Remote Management

Cuando está habilitado, la función de administración remota está habilitada. El valor predeterminado es YES (habilitado)

#### Remote Management Password

La contraseña que se incluirá como parámetro "pwd" en contenido de los mensajes MQTT, en formato JSON, para ejecutar un comando de Administración Remota.

Esta contraseña se encuentra impresa en la etiqueta que acompaña al producto. Tenga cuidado al actualizar esta contraseña porque si la olvida, no será posible controlar el dispositivo con Administración Remota hasta que se restablezca esta contraseña. Para restablecer esta contraseña, conéctese localmente cuando el dispositivo esté actuando como AP.

#### Remote Management MQTT server

Es el servidor al que se conectará el dispositivo para recibir los comandos de Administración Remota y publicar los resultados de estos. La conexión a este servidor es obligatoriamente segura (TLS 1.2)

#### Remote Management MQTT server port (TLS)

Es el puerto en el que el servidor MQTT de Administración Remota escucha las conexiones seguras (el valor habitual y predeterminado es 8883)

#### Remote Management MQTT user

Es el nombre de usuario que el dispositivo usará para conectarse al broker de administración remota

#### Remote Management MQTT password

Es la contraseña que el dispositivo utilizará para conectarse al broker de Administración Remota

#### Force all traffic through the secure connection

Si se habilita, esta opción forzará al dispositivo a no usar la conexión del servidor MQTT principal que no es segura y solo se utilizará el broker especificado para la Administración Remota para todo. Y todo el tráfico se realizará a través de esta conexión segura. El valor predeterminado es YES (Habilitado)

#### Remote Management Command Topic

Es el tópico MQTT al que el dispositivo se suscribirá para recibir los comandos de Administración Remota. El valor predeterminado es la concatenación de "RMgmt/" y el deviceId predeterminado. (Por ejemplo: RMgmt/PSW3S1000000001)

#### Remote Management Result Topic

Es el tópico MQTT donde el dispositivo publicará los resultados después de ejecutar un comando de Administración Remota. El valor predeterminado es la concatenación de "RMgmt/", el deviceId predeterminado y "/results". (Ej: RMgmt/PSW3S1000000001/results)

#### Remote Management MQTT Retain

Es el valor del parámetro RETAIN para los mensajes MQTT de la Administración Remota. El valor predeterminado es 0 (cero, falso)

#### Remote Management MQTT QoS

Es el valor del parámetro QoS para los mensajes MQTT de la Administración Remota. El valor predeterminado es 0 (cero)

## Funcionalidad de depuración (debugging) por MQTT

A veces es necesario saber qué está sucediendo en el dispositivo y no se tiene acceso físico para conectarse y depurar. Puede habilitar la función de depuración MQTT para obtener información de depuración de forma remota.

Esta función requiere que el agente MQTT de Administración Remota esté configurado para funcionar correctamente.

### Enable MQTT Debug parameter

Cuando está habilitado, el dispositivo publicará en el tópico especificado, todo lo que sucede en el dispositivo en un formato legible, incluido el ID del dispositivo.

El valor predeterminado es NO (cero, deshabilitado).

### MQTT Debug Topic

Es el tópico donde se publican los mensajes de depuración cuando la función de depuración MQTT está habilitada.

## Renuncias

Está prohibido reproducir, transmitir o distribuir parte o la totalidad del contenido de este documento en cualquier forma, sin el permiso escrito de Coiaca.

Coiaca se reserva el derecho de modificar, mejorar, reemplazar o cancelar este producto sin previo aviso.

Coiaca se reserva el derecho de cambiar o cancelar el contenido de este documento sin previo aviso..

## Garantía

Esta garantía limitada se aplica a los productos Coiaca que aún se encuentran dentro del período de garantía original.

Es posible que solo necesite instrucciones simples para corregir un problema con su producto. Pruebe en nuestro sitio web en [coiaca.com](http://coiaca.com), en lugar de dirigirse al vendedor. Si el problema no se puede resolver con la información de solución de problemas disponible en línea, se le ofrecerá un servicio técnico desde fábrica. No envíe ningún producto a Coiaca sin contactarse primero.

### Garantía limitada del Hardware

Coiaca garantiza al comprador original que el producto está libre de defectos de material y mano de obra durante tres (3) meses a partir de la fecha de compra. Si se produce un defecto cubierto por esta garantía durante este período de garantía, Coiaca reparará o reemplazará el producto o componente de hardware defectuoso, sin cargo. \*El comprador original tiene derecho a esta garantía solo si la fecha de compra está registrada en el punto de venta o el consumidor puede demostrar, a satisfacción de Coiaca, que el producto fue comprado en los últimos 3 meses.

Servicio después del vencimiento de la garantía

Puede obtener en nuestro sitio web [coiaca.com](http://coiaca.com) información sobre solución de problemas y opciones de reparación o reemplazo y precios. \*

\* En algunos casos, puede ser necesario que nos envíe el producto completo, PAGO PREPAGADO Y ASEGURADO POR PÉRDIDA O DAÑO, a Coiaca. No envíe ningún producto a Coiaca sin contactarse primero.

Limitaciones de la garantía

Esta garantía no se aplicará si este producto ha sido dañado por productos no vendidos o licenciados por Coiaca (incluidos, entre otros, adaptadores, software y fuentes de alimentación).

Además, esta garantía no se aplicará si este producto (a) se utiliza con fines comerciales (incluido el alquiler); (b) está dañado por cualquier modificación no autorizada o manipulación; (c) está dañado por negligencia, accidente, uso irrazonable o por otras causas no relacionadas con materiales o mano de obra defectuosos; (d) ha alterado, borrado o eliminado el número de serie; o (e) ha sido modificado intencionalmente utilizando código malicioso, malware, virus, bots, gusanos, troyanos, puertas traseras, exploits, trampas, pirateos o diagnósticos ocultos que pueden dañar el producto o nuestros sistemas.

Cualquier garantía implícita aplicable, incluidas las garantías de comerciabilidad e idoneidad para un propósito particular, queda limitada por la presente a los períodos de garantía descritos anteriormente. En ningún caso Coiaca será responsable por daños consecuentes o incidentales que resulten del incumplimiento de cualquier garantía implícita o expresa..