Spectrum Brands
Z-Wave Plus™ v2
Behavior Guide

Kwikset WEISER BALDWIN®

Prepared by
Electronic Engineering Department

19701 Da Vinci
Lake Forest, CA 92610

CONFIDENTIAL

This document contains Spectrum Brands private information and should be treated with confidentiality as described under Confidentiality & Trade Secret Agreement and Mutual NDA . No part of this publication may be reproduced, photocopied, stored in a retrieval system or transmitted without the express written consent of the publisher.

Table of Contents

1. Objective 4
1.1 Lock Features 4
1.2 Security Enabled 4
1.3 Z-Wave™ Interoperability Device 4
2. Recommendations 5
2.1 Notifications 5
2.2 Communications 5
2.3 System Time 5
3. Command Classes 6
4. Lock Specific Descriptions 7
4.1 Manufacturer Specific 7
4.2 Door Lock 7
4.2.1 Lock Timeout Values 7
4.2.2 Auto-relock Time 8
4.3 User Codes 8
4.3.1 Maximum User Codes 8
4.3.2 User Code Types 8
4.3.3 Keypad modes 8
4.3.4 Master Code 8
4.3.5 Checksum 9
4.4 Master Code 9
4.5 User Code Scheduling 9
4.6 Battery Alarms 9
4.7 System Time 9
4.8 Association Groups 9
4.9 Notification Command Class 10
4.9.1 Access Control Events 10
4.9.2 Home Security Events 11
4.9.3 Power Management Events 11
4.10 Configuration Parameters 11
4.10.1 Configuration Parameter 1 11
4.10.2 Configuration Parameter 2 11
4.10.3 Configuration Parameter 3 11
4.10.4 Configuration Parameter 4 12
4.10.5 Configuration Parameter 10 12
4.10.6 Configuration Parameter 40 12
4.10.7 Configuration Parameter 46 13
4.11 Anti-Theft Command Class 13
4.11.1 A Brief Description 13
4.11.2 Enabling 13
4.11.3 Protected Command Classes 13
4.11.4 Unprotected Command Classes 14
4.11.5 Setting Anti-Theft 14
4.11.6 Disabling Anti-Theft 14
4.11.7 Anti-Theft Activated 14
4.12 Firmware Update MD Command Class 14
4.12.1 Target 0 14
4.12.2 Target 1 14
4.13 Indicator Command Class 15

CONFIDENTIAL

4.14 Basic Command Class 15

CONFIDENTIAL

1. Objective

The objective of this document is to describe the new Z-Wave Plus™ v2 lock offerings by Spectrum Brands, Inc. These locks will be the next generation Z-Wave™ locks that will encompass the different lock brands that are available from Spectrum Brands, Inc.

1.1 Lock Features

The Z-Wave Plus v2 lock is an advanced battery operated FLiRS Z-Wave device, offering more functionality then the existing Z-Wave Plus lock. The lock will also provide a more straightforward system integration along with a more straightforward network interface. This will give the installer and system integrator a better experience with the lock.

The Z-Wave Plus v2 lock is based off of Silicon Labs' ZGM 700 series Z-Wave system in package, offering the latest SDK available. Of the command classes offered, it will contain the latest versions, attempting to provide a more complete interface to the lock.

The functionality of the lock will also be provided through a standardization of the Z-Wave specifications. Most of the previous proprietary lock controls no longer exist in this lock, thus providing an easier interface for integration and end customer use.

1.2 Security Enabled

The Z-Wave Plus v2 lock will offer both S2 security. It is highly recommended that this product only be implemented in an S2 secure environment, even though for backward compatibility, it will still offer S0 security.

It will also provide SmartStart. This should allow those building up installs to easily include these locks into the systems. It is also recommended that distributors and installers take advantage of the SmartStart technology.

1.3 Z-Wave™ Interoperability Device

To assure interoperability, each Z-Wave product must pass a stringent conformance test to assure that it meets the Z-Wave standard for complete compliance with all other devices and controls. The Z-Wave identity mark assures consumers, integrators, dealers and manufacturers that their products will reliably perform with any other Z-Wave device. And, regardless of the vendor, always powered nodes may act as a repeater for Kwikset/Weiser/Baldwin products."

CONFIDENTIAL

2. Recommendations

This section will provide some recommendations that may assist with the overall user experience from the latest Z-Wave Plus™ v2 offerings.

2.1 Notifications

The lock is designed to notify a controlling device of any changes that occur locally to the lock, without the controlling device's knowledge. It will offer these notifications via the Lifeline association group, allowing up to 5 devices to receive these messages. These notifications center around lock usage such as locking / unlocking, user codes, battery life, etc.

Upon a power cycle, if the lock is already included within a network, it will send out a door lock operation report and a battery report, separated by 30 seconds.

The lock will also send battery reports every so often, whenever the battery is reduced by 10 percent. This, will hopefully, allow the controlling device to keep track of battery percentages during the lifetime of the lock.

For a list of notifications provided, please refer to the notification section for details.

2.2 Communications

All locks are battery operated FLiRS devices. They are set to wake up every second in order to locate a beacon for any required communication. With the availability of notifications, it is recommended that communications to the lock be limited and be performed when necessary. The lock will attempt to keep controlling devices updated whenever something changes locally.

Using the latest ZGM system in package, battery power is used sparingly, but extending battery life is always desirable.

For some set requests, such as door lock operation set (not wrapped inside a supervision message) and user code set, the lock will respond with a report message notifying the controlling device of the lock's response. With regards to the door lock operation set, if the lock is already at the requested setting, a report message will be sent right away. If the lock is required to operate the motor in order to satisfy the request, the report will be returned after the time needed to satisfy the request. This time period may be anywhere from 1 second to 5 seconds depending on battery life. If a door lock jam occurs, due to the retries, the time period may take up to 15 seconds to report back.

2.3 System Time

The locks have the capability of keeping track of system time. This allows systems to implement lock side scheduling. Lock side scheduling has advantages of keeping access control up to date, even during power outages.

If lock side scheduling is to be used, some recommendations are required. First recommendation is to have the controlling device set up the system time during inclusion mode. This is a good time, especially during initial setup and probing, to get the time programmed into the lock. Second recommendation is to have the controlling device keep the system time up to date in the lock. It is requested that the controlling device set the time once per month in the lock. This will take care of any drift that may occur in battery operated devices. It is also requested that, upon determination that the lock was power cycled, the controlling device set the time in the lock. Since it is battery operated, it will lose the time setting once the batteries are removed.

CONFIDENTIAL

3. Command Classes

This section shows the command classes that are available for the Z-Wave Plus v2 locks.

Application Command Class	Version	Security Level
AntiTheft	2	S2 / S0
Basic	2	S2 / S0
Configuration	4	S2 / S0
Door Lock	4	S2 / S0
Door Lock Logging	1	S2 / S0
Notification	8	S2 / S0
Schedule Entry Door Lock	3	S2 / S0
User Code	2	S2/ S0

Management Command Classes	Version	Security Level
Association	2	S2/ S0
Association Group Information	3	S2/ S0
Battery	1	S2/ S0
Device Reset Locally	1	S2/ S0
Firmware Update MD	5	S2/ S0
Indicator	3	S2/ S0
Manufacturer Specific	2	S2/ S0
Multi-Channel Associations	3	S2/ S0
Time Parameters	1	S2/ S0
Version	3	S2/ S0
Z-Wave Plus Info	2	None

Transport Encapsulation CC	Version	Security Level
Security S0	1	None
Security S2	1	None
Supervision	1	None
Transport Service	2	None

Network-Protocol CC	Version	Security Level
Power Level	1	S2/ S0

CONFIDENTIAL

4. Lock Specific Descriptions

This section will cover descriptions that are specific to Spectrum Brands, Inc. Z-Wave Plus v2 locks. These descriptions further help describe expectations with regards to how the lock responds to certain requests and situations.

4.1 Manufacturer Specific

The lock provides extra details within the Manufacturer Specific command class. For the Manufacturer Specific Report, the following information is provided. For model specific values, please see the QR code for the particular lock.

Parameter	Kwikset 869	Kwikset 892	Kwikset 893	Weiser GED1800
Manufacture ID	00 90	00 90	00 90	00 90
Product Type ID	08 11	08 11	08 11	08 11
Product ID	23 A8	03 A8	13 A8	06 A8

For the Device Specific Get, when requesting the Serial Number, the programmed SKU number will be provided. When requesting a Pseudo Random number, a UUID value will be provided.

For a Device ID of **00** or **02**, the information provided will be a Pseudo Random number that is unique to the device.

For a Device ID of **01**, the information provided will be the Serial Number, which in the case of the device will be the programmed SKU number.

4.2 Door Lock

The lock supports v4 of the Door Lock Command Class. This version provides extensive control surrounding the door lock function.

The following door lock modes are supported:

- Door Unsecured – 0x00
- Door Unsecured with timeout – 0x01
- Door Secured – 0xFF

Prior to using the Door Unsecured with timeout functionality, the timeout value is required to be set using the Door Lock Configuration Set command. If the Door Unsecured with timeout request is received by the lock and the Lock Timeout value is zero, the lock will convert the request to a Door Unsecured request.

In order for an unlock with timeout or an auto relock function to work, the lock must have <u>at least</u> one user code saved into the lock. If no user codes are present, the lock will remain unlocked until one is saved into the lock or until it receives a lock request.

4.2.1 Lock Timeout Values

The Lock Timeout Minutes and Lock Timeout Seconds in the Door Lock Configuration Set command can be used to setup a temporary auto lock function when a Door Unsecured with timeout request is sent to the lock. The minimum time the lock can perform is 6 seconds, but it is requested that the timeout be set to something much greater, allowing the user time to open and close the door.

CONFIDENTIAL

4.2.2 Auto-relock Time

The times allowed for the auto-relock time fields of the Door Lock Configuration Set command are as follows. Other than a value of 0, i.e. auto-relock disabled, any other values received by the lock shall be rejected.

- 30 seconds
- 60 seconds (1 minute)
- 180 seconds (3 minutes)
- 300 seconds (5 minutes)
- 600 seconds (10 minutes)

4.3 User Codes

The lock supports the User Code Command Class V2. This opens up different types of user codes allowed by the lock.

4.3.1 Maximum User Codes

The lock will support up to 250 user codes with scheduling information attached. Due to the high number of maximum user codes, the extended user code set and get commands are available. The specification calls out for a maximum bulk user code set and get command to be limited to 10. The lock will handle a Get request with up to 3 returned user codes and for a Set request with up to 3 included user codes. This will allow it to remain inside one S2 encapsulated packet.

4.3.2 User Code Types

The lock supports user code types as defined by the specifications for V2. The following types are supported by the lock:

- Available – user code slot is empty
- Enabled / Grant Access – user code slot has a valid code and is allowed to operate the lock
- Disabled – user code slot has a valid code but is disabled and will not be allowed to operate the lock
- Messaging – user code slot has a valid code and the code is used to message the controlling device only
- Passage Mode – user code slot has a valid code and the code can be used to operate the lock. No auto-relock will occur if unlocked by this user type.

4.3.3 Keypad modes

The User code keypad mode functionality is also supported. This gives the controlling device options for controlling the keypad as defined in the specifications. The following keypad modes are supported:

- Normal mode – normal operation
- Vacation mode – normal operation is not available for user codes, but adding/removing is available
- Privacy mode – normal operation is not available for user codes
- Locked Out mode – all operations per keypad are not available

4.3.4 Master Code

The lock provides an interface to its master code functionality. Both setting and removing/disabling a master code is supported. Since the master code resides in a separate location than normal user codes, the lock <u>will</u> allow a master code to be the same as a user code.

CONFIDENTIAL

4.3.5 Checksum

The User code checksum functionality is supported. The value calculated is per the specifications. It can be used in leu of retrieving all user codes, if the number of stored user codes is significant, in order to validate what is stored locally on the lock.

4.4 Master Code

The lock provides a Master Code that can be used to limit access to particular lock settings. If used, the Master Code will allow control over local adding and removing of user codes, local settings of the status LED, auto-relock settings, and buzzer settings. When enabled, the Master Code will be required to be entered prior to performing lock setting changes.

4.5 User Code Scheduling

Lock side user code scheduling is available. The only requirement is that the panel keep the system time updated within the lock. Please see section 4.7. Each user code will have 7 weekly schedules and 1 yearly schedule available. The option for repeating schedules is also available and will take the place of the 7 weekly schedules. Per the Z-Wave Specification, once a user code has been assigned a repeating schedule, that schedule type will be the only one allowed. This means that each user code offers either 7 weekly, single day, schedules or 7 weekly repeating schedules. The repeating schedules provide greater flexibility for lock side scheduling.

4.6 Battery Alarms

For these locks, there are only two battery alarms. These alarms will match up with existing power management event type notifications. The two alarms are Replace Battery Soon and Replace Battery Now. The Replace Battery Soon will be activated with roughly 10% battery life remaining, whereas the Replace Battery Now will be activated when the battery level reaches 0%. At the 0% level, it will be considered too low to operate and will only allow the door to unlock but will give an error for locking. This notifies the user that they should replace the batteries before they completely run out of any power left.

4.7 System Time

As was stated in a previous section, the lock is capable of maintaining system time, allowing lock side scheduling if so desired. Setting the time in the lock is done using the Time Parameter Command Class. If so desired, this command class can be used either for local time or for UTC time, as specified in the specification. If UTC time is used, the controlling device should set the local time offset using the Schedule Entry Lock command class and the Time Offset command.

If UTC time, along with Time Offset, is used, the monthly system time update will only need to update the UTC time. The time offset value will remain while the lock retains power. Once again, if the lock's power is removed, please make sure to setup both UTC and Time Offset upon power up notification.

4.8 Association Groups

The lock will only support one association group, i.e. Lifeline. It will support sending messages to a maximum of 5 nodes. The following unsolicited messages are provided:

Command Class	Command
Command Class Battery	Battery Report
Command Class Door Lock	Door Lock Operation Report
Command Class User Code v2	Master Code Report
Command Class Notification	Notification Report
Command Class Device Reset Locally	Device Reset Locally Notification

CONFIDENTIAL

Command Class Indicator	Indicator Report

4.9 Notification Command Class

Version 8 of the notification command class will be the only version of the notification/alarm command class that will be supported. Notification messages are used to notify the controlling device of changes made locally on the lock. Notification messages shall not be sent in response to requests made. When there is a user code involved with the notification message, the slot number will be provided in a 1-byte parameter value, except for those specifically defined to provide a 2-byte parameter value.

The following notification types are supported:

- 0x06 – Access Control
- 0x07 – Home Security
- 0x08 – Power Management

4.9.1 Access Control Events

The following events are supported for the Access Control notification type:

Event Name	Value
Manual Lock Operation	0x01
Manual Unlock Operation	0x02
RF Lock Operation	0x03
RF Unlock Operation	0x04
Keypad Lock Operation (with user ID info)	0x05
Keypad Unlock Operation (with user ID info)	0x06
RF Not Fully Locked Operation	0x08
Auto lock Operation	0x09
Auto lock Not Fully Locked Operation	0x0A
Lock Jammed	0x0B
All user codes deleted	0x0C
Single User Code Deleted (with user ID)	0x0D
New user code added (with user ID)	0x0E
New user code not added, duplicate	0x0F
Keypad Temporarily Disabled	0x10
New User Code ID entered (with user ID)	0x12
Entered Access code exceeds code limit	0x13
Messaging User Code Was Entered	0x20

CONFIDENTIAL

4.9.2 Home Security Events

The following events are supported for the Home Security Events notification type:

Event Name	Value
Tampering, product covering removed	0x03
Tampering, Invalid Code Entered	0x04

4.9.3 Power Management Events

The following events are supported for the Power Management Events notification type:

Event Name	Value
Replace battery soon	0x0A
Replace battery now	0x0B

4.10 Configuration Parameters

The Configuration Command Class allows the lock to provide extra functionality that is not found within existing command class controls. With the usage of the latest command classes, there are only but a few items that are not covered that will be covered here in this command class.

Some locks will allow configuration settings via the front panel. Some of those configurations are not included in command classes. They will be offered through configuration parameters within the Configuration Command Class. The following list shows the parameters that are available.

4.10.1 Configuration Parameter 1

Parameter Name: Status LED Control

Data Length: 1 byte

Default Value: 1

Possible Values: 0 – Status LED off; 1 – Status LED on

Description:

The configuration parameter 1 is a read/write parameter with a one-byte field, used to control the status LED. If set to on, the status LED will show the status of the latch every 6 seconds. If set to off, the status LED will not be shown.

4.10.2 Configuration Parameter 2

Parameter Name: Sound Control

Data Length: 1 byte

Default Value: 1

Possible Values: 0 – Sound (buzzer) is off; 1 – Sound (buzzer) is on

Description:

The configuration parameter 2 is a read/write parameter with a one-byte field, used to control the lock's buzzer. If set to on, the buzzer is enabled and will sound during normal events. If set to off, the buzzer is disabled, and the buzzer sound will not occur.

4.10.3 Configuration Parameter 3

Parameter Name: User Program Button Control

CONFIDENTIAL

Data Length: 1 byte

Default Value: 1

Possible Values: 0 – Program button is turned off and not available for use; 1 – Program button is turned on and is available for use.

Description:

The configuration parameter 3 is a read/write parameter with a one-byte field, used to control the user program button. If set to on, the program button is available for user code maintenance. If set to off, the program button is not available for user code maintenance.

4.10.4 Configuration Parameter 4

Parameter Name: Secure Screen Control

Data Length: 1 byte

Default Value: 1

Possible Values: 0 – Secure Screen is disabled; 1 – Secure Screen is enabled

Description:

The configuration parameter 4 is a read/write parameter with a one-byte field, used to control the secure screen functionality on touch locks only. This parameter is not used on non-touch locks and will be ignored. If set to enabled, the touch screen will display the secure screen functionality when woken. If set to disabled, the touch screen will not display the secure screen functionality when woken.

4.10.5 Configuration Parameter 10

Parameter Name: Handing Control

Data Length: 1 byte

Default Value: 0

Possible Values (GET): 1 – right-handed lock; 2 – left-handed lock

Possible Values (SET): 1 – run handing operation

Description:

The configuration parameter 10 is a read/write parameter with a one-byte field. When this parameter is read, it will return the handing of the lock. When this parameter is written, it will run a handing operation. When written with a value of 0x01, it will cause the lock to cycle through locking and unlocking until it determines the correct handing. It is suggested that this operation occur while the door is opened so that no obstructions will be in the way for the operation. After the completion of the handing process, a Configuration Report message will be sent back to the requestor. It will contain a non-zero value for success or a zero value for failure.

4.10.6 Configuration Parameter 40

Parameter Name: Factory Default Control

Data Length: 1 byte

Default Value: 0

Possible Values: 1 – Perform a factory reset and reboot the lock; 2 – Perform a factory reset, but do not reset the lock (production use only)

Description:

CONFIDENTIAL

The configuration parameter 40 is a write only parameter with a one-byte field, used to request the lock to perform a factory reset back to its default state. This control will place the lock back to its default state. When a read is issued for this parameter, a 0 will be returned. A Factory Reset will delete network settings from the lock but not from the panel. Please run the Exclusion process to properly remove this lock from the network before performing a factory reset.

4.10.7 Configuration Parameter 46

Parameter Name: Motor Load Value

Data Length: 4 bytes

Default Value: 0

Possible Values: Values range from 0x0000000 – 0x00FFFFFF

Description:

The configuration parameter 46 is a read only parameter with a four-byte field. It is used to retrieve the calculated sideload value from the last motor run that was performed. This value is used to represent the amount of power needed to run the motor, giving the opportunity to see if any resistance was encountered based on the value read from a free running motor with no resistance. *A higher number indicates that the motor had to work harder and use a greater amount of battery power to lock/unlock. Any number greater than the alarm thresholds in configuration parameters 48 and 49 is an indication that action should be taken to improve the lock or door installation.*

4.11 Anti-Theft Command Class

The lock has been implemented to support the Anti-Theft Command Class. This allows an owner to "lock down" this product, causing it to only work while on the network that issued the request. Per the Z-Wave Alliance, when using this command class, it is required to register using the SDS14622 registry.

4.11.1 A Brief Description

The Anti-theft Command Class is used to disable a subset of supported/controlled command classes in a device if the device is being excluded and re-included into a Z-Wave network again. This command class is typically used when installing a Z-Wave device in a public location such as a hotel room or conference center. The command class allows the user to lock the device to the actual Z-Wave network and to render it useless if it is removed from the local network without disabling Anti-Theft. Another application would be to protect service provider owned products from leaving the service providers network before they are paid for.

4.11.2 Enabling

When the lock protection is enabled, the lock does NOT change any operation with respect to supported/controlled command classes as long as the lock stays included into the original Z-Wave network.

4.11.3 Protected Command Classes

The following is a list of command classes that are protected when Anti-Theft is enabled.

Battery Command Class	**Door Lock Command Class**
Configuration Command Class	**Door Lock Logging Command Class**
User Code Command Class	**Notification Command Class**
Time Parameters Command Class	**Schedule Entry Door Lock Command Class**
Firmware Update MD Command Class	

CONFIDENTIAL

4.11.4 Unprotected Command Classes

The following is a list of command classes that are not protected and will be the only command classes available when Anti-Theft has been activated.

Version Command Class	**Manufacturer Specific Command Class**
Device Reset Locally Command Class	**Indicator Command Class**
Power Level Command Class	**Anti-Theft Command Class**
Association Command Class	**Multi-Channel Association Command Class**
Association Group Info Command Class	

4.11.5 Setting Anti-Theft

1. Set the Anti-Theft value to 0x01 (enable AT)
2. Provide a Magic Code to be used later for verification
3. The node information frame (NIF) will show all command classes available

4.11.6 Disabling Anti-Theft

1. Set the Anti-Theft value to 0x00 (disable AT)
2. Provide the correct Magic Code
3. The node information frame (NIF) will show all command classes available

4.11.7 Anti-Theft Activated

1. NIF will show reduced list of command classes
2. The Anti-Theft value will show 0x03 (activated AT)

4.12 Firmware Update MD Command Class

The lock provides the capability of updating the firmware for both the Z-Wave application, i.e. target 0, as well as the lock application, i.e. target 1.

4.12.1 Target 0

Target 0 represents the Z-Wave application layer. The OTA file format is the standard GBL file that is used by the SiLabs' Gecko Bootloader. When updating target 0, please use a file designated for the following APP_FIRMWARE_ID:

0x11	**0xA8**

4.12.2 Target 1

Target 1 represents the Lock Application layer. The OTA file format is also the standard GBL file that is used by the SiLabs' Gecko Bootloader. When updating target 1, the firmware ID that is accepted is made up of the first byte of the current ID, i.e. 0x45, but should not be the same as the second byte of the firmware ID. This byte represents the firmware version number. For example, if the current firmware is equal to 0x45 0x1C, the GBL file used to update should not be equal to 0x1C. To update the current 0x45 0x1C, an example would be the following:

0x45	**0x00**

CONFIDENTIAL

4.13 Indicator Command Class

The Indicator Command Class is included to assist with identifying the lock. It will provide Indicator ID 0x50, Node Identify. For Indicator ID 0x50, it will provide property IDs of 0x03, 0x04, and 0x05. These will allow control for the cycle time, cycle on time, and cycle count. When issuing a Indicator ON request with no data, the default Node Identify routine will run. The default Node Identify routine is defined as follows:

Buzzer will sound for 200ms

<start of cycle>

ON cycle = red status LED ON for 200ms

OFF cycle = green status LED ON for 200ms

<repeat cycle for 10 times>

<end of cycle>

Buzzer will sound for 200ms

This equates to a cycle time of 400ms, cycle on time of 200ms, and a cycle count of 10. Any of the property IDs may be changed as long as the cycle count remains greater than 0.

4.14 Basic Command Class

The basic command class is implemented per requirements for Lock DT Z-Wave Plus v2 products. It will NOT be advertised in the NIF but will be available if a request is received by the lock.

The following commands are mapped to the basic commands:

Basic Command	Mapped Command
Basic Get	Door Lock Op: current value, target value, duration
Basic Set (Value)	Door Lock Operation Set (Door Lock Mode)
Basic Report (Current Value == 0x00)	Door Lock Operation Report (Door Lock Mode = 0x00)
Basic Report (Current Value == 0xFF)	Door Lock Operation Report (Door Lock Mode > 0x00)

CONFIDENTIAL