Master Lock

Z-Wave® 800 Series System Integrators Guide

Master Lock Multi-Family Cylindrical Commercial Grade Lever Locks

Document Revision: 1.0

December 2025

Contents

* This command class requires security.

Revision History

Rev.	Details
1.0	Initial Release

Master Lock Z-Wave Plus® Product Info

Manufacturer ID: Fortune Brands Innovations, Inc. [FBIN] (0x0463)

Z-Wave® Device Type: Door Lock Keypad

Z-Wave® Role Type: Listening Sleeping End Node (LSEN)

Network Operations

Enroll/Add device to network (SmartStart)

SmartStart enabled products can be added into a Z-Wave® network by scanning the Z-Wave® QR Code present on the product with a controller providing SmartStart inclusion. No further action is required and the SmartStart product will be added automatically within 10 minutes of being switched on in the network vicinity.

- Open the Z-Wave® system's smart home app via smartphone or tablet and follow the in-app prompts to add a new device.
- SmartStart works when the Z-Wave® system has the DSK saved and one of the following are true:
    - The lock has the minimum Radio Module firmware version AND is in a factory-reset state:
        - AYR-MOD-ZW4-USA: v5.1.12
            - Version CC-Version_Report-FW 0 Version: 0x05 & FW 0 Sub Version: 0x01
            - Version CC-Version_ZWave_Software_Report-Application Version: 0x05 0x01 0x0C
    - The lock has the minimum Lock firmware version AND is in a factory-reset state:
        - MCB614/624/634/644 v1.5.18:
            - Version CC-Version_Report-FW Version: 0x0F & FW Sub Version: 0x12
    - An internal key has already been established.

Long Range Capabilities

The lock can be included via Z-Wave® Long Range SmartStart if the controller also supports Z-Wave® Long Range. However, the lock does not allow other nodes to be included via Z-Wave® Long Range.

Enroll/Add device to network (Classic Inclusion Mode)

- Enter the 4–8-digit Programming PIN code followed by the ⚙ key.
- Press the 7 key followed by the ⚙ key.
- Press the 1 key followed by the ⚙ key.
- Scan the QR code, if prompted, or…
- Enter the first five (5) digits of the DSK if prompted.

Un-enroll/Remove device from network (Exclusion Mode)

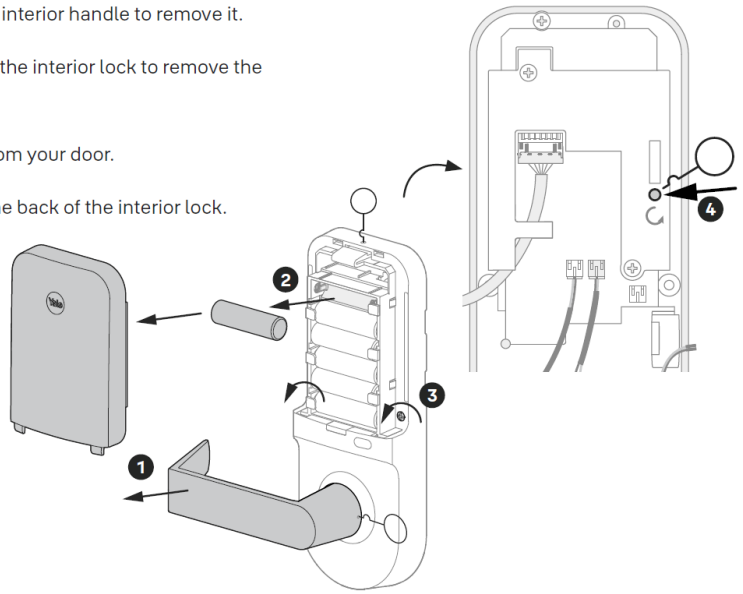
- Enter the 4–8-digit Programming PIN code followed by the ⚙ key.
- Press the 7 key followed by the ⚙ key.
- Press the 3 key followed by the ⚙ key.

When the Master Lock door lock is unenrolled/excluded from the network through the device menu mode, any changes previously made to the user code database and configuration settings will be retained, as opposed to set back to defaults.

Factory Reset

- Factory resetting the lock with the Z-Wave® module installed will clear the Z-Wave® network settings, causing the device to be removed from the network.
- The following is the method of performing a factory reset:

1. Insert the reset pin into the desginated hole on the interior handle to remove it.
2. Insert the reset pin into the desginated hole above the interior lock to remove the battery cover. Remove one battery.
3. Untighten the screws to remove the interior lock from your door.
4. Insert reset pin into the designated reset hole on the back of the interior lock.
5. Press and hold the reset pin.
6. While holding the reset pin, reinsert battery.
7. Keep holding the reset pin for 5 more seconds.
8. After the keypad numbers light up sequentially from 1, take out the reset pin.



Supported Command Classes

The Master Lock Z-Wave Plus® locks follow the Z-Wave® Command Class Specifications for all command classes that are implemented. Please refer to these specifications for specifics on how each command class works. The supported command classes are listed below, and certain sections contain details about operations that may be specific to the Master Lock door lock. If a section is blank, then please refer to the Z-Wave® specifications.

As a security device, most of the command classes supported by the lock are required to be sent securely with Z-Wave® security. During enrollment, the controller can use the Security Command Class to get this list directly from the lock. If a command class requires security, it is also indicated as follows.

Specification used: Z-Wave® Specifications Release 2025 A

Command Class Z-Wave Plus® Info, Version 2

The Z-Wave Plus® Info command class reports the following information:

- Role Type: Listening Sleeping End Node (0x07)
- Node Type: Z-Wave Plus® Node (0x00)
- Installer Icon Type: 0x0300
- User Icon Type: 0x0300

Command Class Manufacturer Specific, Version 2*

* This command class requires security.

The Manufacturer Specific command class reports the following information:

- Manufacturer ID: 0x0463
  - This is the manufacturer ID assigned to Fortune Brands Innovations, Inc. [FBIN].
- Product ID:
  - The Product ID can be used to differentiate between hardware platforms, as well as between ZW2, ZW3, and ZW4. See Table 1 - First 2 Digits of Product ID, below, for details.
  - Product IDs for the locks covered in this document are as follows:
    - Default 0x8B64 - MCB614-ZW4: Keyed Push Button interface
    - 0x8B65 or Default 0x8B64 - MCB624-ZW4: Keyed Touch Screen interface
    - 0x8B66 or Default 0x8B64 - MCB634-ZW4: Keyless Push Button interface)
    - 0x8B67 or Default 0x8B64 - MCB644-ZW4: Keyless Touch Screen interface
- Product Type ID:
  - 0x8132 for MCB614/624/634/644-ZW4 (Cylindrical lock)

Table 1 - First 2 Digits of Product ID

	Z-Wave® Type			**Platform**					**Hex Value**
[0x8132]-ZW2 ***(Not Tested for Cert)***	0	0	0	0	0	1	1	0	**0x0B**
[0x8132]-ZW3 ***(Not Tested for Cert)***	0	1	0	0	0	1	1	0	**0x4B**
0x8132]-ZW4	1	0	0	0	0	1	1	0	**0x8B**

Command Class Security, Version 1

This command class has been implemented by the Z-Wave® Specification.

Command Class Security 2, Version 1

This command class has been implemented by the Z-Wave® Specification.

Command Class Device Reset Locally, Version 1*

* This command class requires security.

The Master Lock door locks covered in this guide can be reset to their factory default settings by manual resetting (by following the procedure outlined in the specific lock's manual).

Upon factory reset, all Z-Wave® network settings are cleared, all the user codes are erased from the lock (including the programming code), and all configurable settings are reset to default values. A factory reset leaves the lock in a completely unsecure state (waiting for the programming code to be set), so care should be taken if using the configuration parameter to perform a remote reset. However, if the DUT is unenrolled/excluded from the network through the device menu mode, then the user code database and configuration settings will not be reset to the defaults.

Command Class Power Level, Version 1*

* This command class requires security.

This command class has been implemented by the Z-Wave® Specification.

The Power Level command class was implemented to allow controllers to set the transmit power for the door lock. This could be useful in large networks with many nodes, so that the lock can find working routes back to the controller while transmitting at a lower power. This ensures robust routes when the normal transmit power level is restored.

Currently there is no way to initiate a low power enrollment; this command class can only be used once the lock is enrolled successfully.

Command Class Version, Version 3*

* This command class requires security.

The Master Lock locks are a multi-processor system with 1 additional firmware target. All processors can be updated through the Firmware Update Meta Data command class. The firmware targets are numbered as follows:

- Firmware Target 0 = Z-Wave® Chip
- Firmware Target 1 = Lock Processor

To identify the firmware version for each target, the hex data in the firmware version report must be converted to decimal prior to combining major and minor version into the full version.

After a controller sends a Version Get command the log will display the Version Report like the below:

```
Send VERSION_GET to node 16 started
Send VERSION_GET to node 16 completed in 00:00:01.242
Rx [S2_ACCESS] VERSION_REPORT(86 12) + 03 07 10 02 22 02 01 2C 00
```

The above Version Report will be defined as this in the Z-Wave® sniffer tool, Zniffer:

Command Class Version ver.3

Version Report

Z-Wave Library Type:	0x03
Z-Wave Protocol Version:	0x07
Z-Wave Protocol Sub Version:	0x10
Firmware 0 Version:	0x02
Firmware 0 Sub Version:	0x22
Hardware Version:	0x02
Number of firmware targets:	0x01
▾ vg 1:	2C 00
Firmware Version:	0x2C
Firmware Sub Version:	0x00

For Firmware Target 0, the Firmware 0 Version (0x02) and Sub version (0x22) translate to module firmware decimal value of "2.34".

For Firmware Target 1 (the data under vg1), Firmware Version (0x2C) and Sub version (0x00) translate to lock firmware decimal value of "4.3.00".

Command Class Battery, Version 1*

* This command class requires security.

Per the Z-Wave Plus® Specification, the lock will send a Battery Report with a value of 0xFF to the Lifeline node when a critical battery level is reached (at about 6.0V). In addition, Master Lock Locks provide 2 earlier low battery alarms through the notification command class (see Table 7 - Command Class Notification, Version 8*).

Low battery alarms will be generated if the lock is in a low battery state during one of the following events: any motor activation (keypad lock/unlock, RF lock/unlock, etc.), controller sends Get Battery command, or the unsolicited battery report was triggered. Master Lock locks will generate an unsolicited Battery Report every power cycle and every 8 hours if a node is listed in the Lifeline Group.

Command Class Door Lock, Version 4*

* This command class requires security.

Master Lock Z-Wave Plus® locks support three door lock modes: Door Secured (0xFF), Door Unsecured (0x00), and Door Unsecured with timeout (0x01). When Auto Relock is enabled, the lock will automatically relock after all unlock events. Master Lock Z-Wave Plus® locks do not support any of the "Door Unsecured for outside Door Handles" (0x20, 0x21) or "Door Unsecured for inside Door Handles" (0x10, 0x11) modes.

Command Class Door Lock Logging, Version 1*

* This command class requires security.

This command class has been implemented by the Z-Wave® Specification.

Command Class User Code, Version 2*

* This command class requires security.

NOTE: A controller should use only one of the command classes (CC) to manage credentials in the lock. User Code CC or User Credential CC and never both. If User Code CC is chosen to manage credentials, schedules can be applied to User Codes via Schedule Entry Lock CC.

Versions 1 and 2 of this command class can address user code slots 1 through 250 via the User Code Set/Get/Report commands. Version 2 of this command class also includes extended versions of each of these commands, used to address the extended range of users.

Table 2 – Expected Reports for Set/Get Commands

Command	Slots 1-250	Slot 251	Slots 252-254	Slot 255	Slots 256-500
User Code CC v1/v2: User Code Get	User Code Report	User Code Report	User Code Report	User Code Report	N/A
User Code CC v1/v2: User Code Set	User Code Report	Admin Code Report	User Code Report	User Code Report	N/A
User Code CC v2: Extended User Code Get	Extended User Code Report	Extended User Code Report	Extended User Code Report	Extended User Code Report	Extended User Code Report
User Code CC v2: Extended User Code Set	Extended User Code Report	Extended User Code Report	Extended User Code Report	Extended User Code Report	Extended User Code Report

The admin code can be accessed (read/write) using slot 251 (0xFB), if using version 1 of this command class. For version 2, the Admin Code Set/Get/Report commands must be used.

Master Lock locks do not support bulk commands (setting or getting multiple user codes at once) or CRC functionality for this command class.

It should be noted that the lock's operation mode (called "User Code Keypad Mode" in this command class) can be modified through Version 2 of this command class, or through parameter 8 of the Configuration command class. This is the only parameter that can be modified through more than one command class.

The following implementation notes apply specifically to non-access user codes:

- The usage of non-access users has changed slightly with ZW3/ZW4, compared to ZW2, but is still backwards compatible. If a User Code Set is transmitted using version 1 of the command class, then the lock will accept a value of 0x04 as the status for the non-access user.
- Previously, a value of 0x04 was reserved for setting up non-Access users, as stated above. When using version 2 of this command class, a non-Access (now called "Messaging") user ID status is assigned a value of 0x03. This value of 0x03 should be used with the Extended User Code Set command.
- A non-access user can be identical to a "normal" PIN code, aside from the fact that it does *not* grant access.
- Any available user code slot (except the admin code) can be used to store non-access user code.
- Schedules can be applied to non-access users.

Master Lock locks support the following User ID Status values:

Table 3 - User ID Status User Code CC v1 vs v2

User ID Status	**User Code CC v1 Set**	**User Code CC v1 Report Value**
Description	*Value*	*Value*
Available	0x00	0x00
Enabled / Grant Access	0x01	0x01
Disabled	0x02	0x03
	0x03	
Messaging: The user code is accepted, but the lock does not grant access to the user. Instead, it generates an alarm to the Lifeline and does NOT take preventative actions for further attempts to enter the User ID and/or User Code.	0x04	0x04
One-Time Use: This PIN is disabled immediately after being used for a successful unlock operation.	0x06	0x06
Expiring: This PIN is disabled once a specified amount of time has passed after being used for a successful unlock operation. The expiration time is set through the Configuration command class.	0x07	0x07

User ID Status	User Code CC v2: Extended User Code Set	User Code CC v2: Extended User Code Report Value
Description	*Value*	*Value*
Available	0x00	0x00
Enabled / Grant Access	0x01	0x01
Disabled	0x02	0x02
Messaging: The user code is accepted, but the lock does not grant access to the user. Instead, it generates an alarm to the Lifeline and does NOT take preventative actions for further attempts to enter the User ID and/or User Code.	0x03	0x03
One-Time Use: This PIN is disabled immediately after being used for a successful unlock operation.	0x06	0x06
Expiring: This PIN is disabled once a specified amount of time has passed after being used for a successful unlock operation. The expiration time is set through the Configuration command class.	0x07	0x07

Command Class User Credential, Version 1*

* This command class requires security.

This command class has been implemented by the Z-Wave® Specification.

NOTE: A controller should use only one of the command classes (CC) to manage credentials in the lock. User Code CC or User Credential CC and never both. If User Credential CC is chosen to manage credentials, schedules via Schedule Entry Lock CC are not supported. User Credential CC will support schedules once Active Schedule CC becomes available.

The Cylindrical Master Lock locks allow the controller to apply 5 Credentials per User within a maximum of 500 Users. The total number of Credentials is 500 pin codes (**Additional Credentials for RFID will be supported at a future date.).*

When Credential Learn Start is sent to our Master Lock locks for Pin code credentials, we limit the Credential Learn Timeout values from 1-30 seconds (if the timeout value is set > 30, the lock will default back to 30 seconds). For the Credential Learn Report (Started): Credential Learn Steps Remaining, Pin Code credential has a value of 1.

Command Class Schedule Entry Lock, Version 3*

* This command class requires security.

Master Lock locks support Year Day Schedule types and Daily Repeating Schedule types. Master Lock locks allow the controller to apply multiple schedules to a single user code slot. Each user code slot has 1 Year Day Schedule slot (Slot ID 1) and 7 Daily Repeating slots (Slot IDs 1 – 7). If user scheduling is used in the lock, then the controller **MUST** set the lock's time using the Time Parameters command class.

Command Class Time Parameters, Version 1*

* This command class requires security.

The controller must set the Time Parameters in the lock anytime the lock loses power. After 10 seconds of lock enrollment, if there are no messages from the controller the lock will initially request the Time (by sending Time Get and Time Parameter Get commands). If the time is not set by the controller, then user codes with schedules applied to them cannot be granted access. When the lock is powered up, it will generate a Notification Report to indicate to the controller that power has been applied (Alarm V1 Type = 0x82, Alarm V1 Level = 0x00, Event Type = 0x08, Event Value = 0x01). This indicates to the controller that the lock no longer has a valid time set.

If the controller does not support either the Time CC or Time Parameters CC, then scheduled users will not have access.

Command Class Time, Version 2

The controller must set the Time Parameters in the lock anytime the lock loses power. Even though the Time CC is not secure, the Time Set command must be issued at the same or higher security level as when the device was enrolled for time to be set otherwise it will be rejected by the device. After 10 seconds of lock enrollment, if there are no messages from the controller the lock will initially request the Time (by sending Time Get and Time Parameter Get commands). If the time is not set by the controller, then user codes with schedules applied to them cannot be granted access. When the lock is powered up, it will generate a Notification Report to indicate to the controller that power has been applied (Alarm V1 Type = 0x82, Alarm V1 Level = 0x00, Event Type = 0x08, Event Value = 0x01). This indicates to the controller that the lock no longer has a valid time set.

If the controller does not support either the Time CC or Time Parameters CC, then scheduled users will not have access.

A time sync should occur every 8 hours, starting with the Time CC. If there is no response within a minute, the next step is to issue a Time Parameters Get to sync time.

Command Class Firmware Update Meta Data, Version 5*

* This command class requires security.

Master Lock Z-Wave Plus® locks support over-the-air (OTA) upgrading of 2 firmware targets:

1. Firmware Target 0: Z-Wave® chip
2. Firmware Target 1: The lock main processor

Firmware Target 0 is used to determine the correct Z-Wave® processor image to download. Firmware Target 0 ID is always 0xA600, to signal this is a Fortune Brands Innovation, Inc. Z-Wave® image.

Firmware 1 target will depend on which version of the lock is in use (mapped to the Product Type ID).

- For MCB614/624/634/644-ZW4 (Cylindrical lock), Firmware 1 ID = 0x8132

After an OTA is performed (a Firmware Update Status Report should return with successful), there is an additional step internally where we write/apply the image to the lock/module. When the image is being applied to the lock, the lock is unresponsive until completion of the applied image. Once the completion of the OTA image is applied the lock silently reboots and a Notification Report is sent. For Module OTA, Notification Report with Alarm Type 0x82 is sent while for Lock OTA, Notification Report with Alarm Type 0x51 is sent to indicate the OTA is completed and the lock can now be used.

The following is the time it takes for each product to complete OTA packet transfer + image apply phase:

- For Z-Wave® Radio Chip
  - Non-Long-Range Node
    - ~6 minutes (full image total time*)
  - Long-Range Node
    - ~3 minutes (full image total time*)
- For MCB614/624/634/644-ZW4 (Cylindrical lock),
  - Non-Long-Range Node
    - ~>=32 minutes (full image total time*)
    - ~2 minutes (patch/differential image total time *)
  - Long-Range Node
    - ~>=21 minutes (full image total time*)
    - ~2 minutes (patch/differential image total time *)

** Total Time includes packet transfer from controller to module and then writing time from module. After an OTA, Master Lock has an additional step internally where we write/apply the image to the lock and the lock is unresponsive. For this lock, it takes ~1.5 minutes (patch) or ~15 minutes (full) to complete the writing of the Lock OTA image and then silent reboots the lock. The internal step also occurs for radio OTA, but it takes seconds to apply the radio image. **

Command Class Association, Version 2*

* This command class requires security.

This command class has been implemented by the Z-Wave® Specification.

Command Class Multi Channel Association, Version 3*

* This command class requires security.

This command class has been implemented by the Z-Wave® Specification.

Master Lock door locks support only one group, which can contain up to 5 nodes.

Command Class Association Group Info, Version 3*

* Command Class Requires Security

Master Lock locks support the Lifeline Association Group.

Table 5 - Association Table

Group ID	Maximum Nodes	Description	Commands

1	5	Lifeline	• Command Class Door Lock (0x62)
			  ○ Door Lock Operation Report (0x03)
			  ○ Door Lock Configuration Report (0x06)
			• Command Class Notification (0x71)
			  ○ Notification Report (0x05)
			• Command Class User Code (0x63)
			  ○ User Code Report (0x03)
			  ○ Extended User Code Report (0x0D)
			  ○ User Code Keypad Mode Report (0x0A)
			  ○ Admin Code Report (0x10)
			• Command Class User Credential (0x83)
			  ○ User Report (0x07)
			  ○ Credential Report (0x0C)
			  ○ User Credential Association Report (0x13)
			  ○ Admin Pin Code Report (0x1C)
			• Command Class Battery (0x80)
			  ○ Battery Report (0x03)
			• Command Class Device Reset Locally (0x5A)
			  ○ Device Reset Locally Notification (0x01)
			• Command Class Indicator (0x87)
			  ○ Indicator Report (0x03)

The following are the actions to trigger the reports:

Table 6 – Lifeline Report Trigger Table

Report Command	**RF Trigger**	**Manual Trigger**
Battery Report	Any RF Lock Operation when lock is under the battery thresholds	Any keypad Lock Operation when lock is under the battery thresholds or Power Cycle Lock
Notification Report (Access Control)	Any RF Lock Operation	Manual or Keypad Unlock/Lock
Notification Report (Power Management)	Any RF Lock Operation when lock is under the battery thresholds	Any keypad Lock Operation when lock is under the battery thresholds or Power Cycle Lock
Door Lock Operation Report	Door Lock Operation Set Command	Keypad Unlock/Lock
Door Lock Configuration Report	Door Lock Configuration Set Command	Enable/Disable Auto-Relock Feature via Keypad
Indicator Report	Indicator Set Command	
Device Reset Locally Notification		HW Factory Reset
User Code Report	Add/Delete User Code via User Code Set Command	Add/Delete User Code via Keypad from Slots 1-250
Extended User Code Report	Add/Delete User Code via Extended User Code Set Command	Add/Delete User Code via Keypad from Slots 251-500
User Code Keypad Mode Report	User Code Keypad Mode Set Command	Enable/Disable Vacation Mode or Privacy Mode (refer to Installation Manual)
Admin Code Report	Admin Code Set Command	Update/Modify Admin/Programming Code via Keypad
User Report	RF Add/Delete User Code via User Set Command	Add/Delete User Code via Keypad
Credential Report	Add/Delete User Credential (pin code or RFID [future use]) via Credential Set	Add/Delete User Credential (pin code or RFID [future use]) via Keypad
Admin Pin Code Report	Admin Pin Code Set Command	Update/Modify Admin/Programming Code via Keypad
User Credential Association Report	User Credential Association Set Command	

Command Class Notification, Version 8*

* This command class requires security.

Table 7 - Notification Table

Alarm Reports	Alarm type	Alarm Level	Description	Notification Type	Event
Credential Unlock	0x00	0x00	Where Event Parameter represents the User Slot, Credential Slot, and Credential Type	0x06	0x24
Credential Lock	0x00	0x00	Where Event Parameter represents the User Slot, Credential Slot, and Credential Type	0x06	0x23
Deadbolt Jammed [0]	0x09	0x01	Deadbolt jammed while locking	0x06	0x0B
		0x02	Deadbolt jammed while unlocking	0x06	0x0B
Keypad Lock	0x12	0x (01 - FF)	Where Alarm level represents user slot number (0x00 = Master Code). Where Event Parameter represents User Code Report. (Use Event Parameter to determine pin code used)	0x06	0x05

		0x (0100 – 01F4)	Alarm level represents a truncated user slot number. Where Event Parameter represents Extended User Code Report. (Use Event Parameter to determine slot number and pin code used)	0x06	0x21
Keypad Unlock	0x13	0x (01-FF)	Where Alarm level represents user slot number (0x00 = Master Code). Where Event Parameter represents User Code Report. (Use Event Parameter to determine pin code used)	0x06	0X06
		0x (0100 – 01F4)	Alarm level represents a truncated user slot number. Where Event Parameter represents Extended User Code Report. (Use Event Parameter to determine slot number and pin code used)	0x06	0x22
Manual Lock	0x15	0x01 [0]	by key cylinder or inside thumb-turn	0x06	0x01
		0x02	by touch function (lock and leave)	0x06	0x01
		0x03	By inside button	0x06	0x01
Manual Unlock [0]	0x16	0x01	By key cylinder or inside thumb turn	0x06	0x02
		0x02	By inside button	0x06	0x02
RF Operate Lock	0x18	0x01	by RF module	0x06	0x03

RF Operate Unlock	0x19	0x01	by RF module	0x06	0X04
Auto Lock Operate Locked	0x1B	0x01	Auto re-lock cycle complete, locked.	0x06	0x09
User deleted	0x21	0x (01-max users)	User code was deleted. Alarm level = user slot number	0x06	0X0D (single)
		0x00 [1]	All User codes were deleted		0X0C (all)
Non-Access /Messaging User	0x26	0x (01-max users)	A Non-Access/Messaging Credential was entered at the lock (Where Event Parameter represents the User Code Slot or User Slot, Credential Slot, and Credential Type)	0x06	0x33
Non-Access/Messaging Pin Code		0x (01-FF) user code slot			0x20
Lever Rotated (Rx)	0x29	0x00	Interior Lever was rotated. Only active when Escape Return Mode is enabled or during Shutdown Mode	0x06	0xFE
Door State	0x2B	0x00	Door is open	0x06	0x16
		0x01	Door is closed	0x06	0x17
		0x02	Door Propped (Door Open for longer than configurable door propped time)	0x06	0xFE
Lock message for FOTA	0x51	0x00	Lock FOTA completed	0x09	0xFE

Daily Repeating Schedule Set/Erased	0x60	0x (01-max users)	Schedule(s) has been set/erased for specified user ID	0x06	0xFE
Year Day Schedule Set/Erased	0x62	0x (01-max users)	Schedule(s) has been set/erased for specified user ID	0x06	0xFE
All Schedule Types Enabled/Disabled	0x65	0x (01-max users)	Schedule(s) has been enable/disabled for specified user ID. If Alarm Level = 0xFF then all users were affected.	0x06	0xFE
Programming Code Updated/Modified	0x70	0x00	Programming code was changed at keypad or via RF	0x06	0x12
User Code Added		0x (01-max users)	User added. Alarm level = user slot number	0x06	0X0E
Duplicate User Code error	0x71	0x (01-max users)	Where alarm level represents user slot numbers 1-255 and Alarm level represents a truncated user slot numbers 256-500 therefore use Event Parameter to determine slot number An Alarm is generated in response to add user via RF. This alarm is not generated when attempting to add duplicate pin at the Keypad (The lock simply denies it and plays the "Denied" sound.) Trying to duplicate the master code will result in a 0x71 0x00 alarm report.	0x06	0x0F

Battery is fully charged	0x80	0x05	After a low battery alert was observed, the lock was powered down and powered back up with full battery.	0x08	0x0D
Door Lock needs Time set / RF Module Power Cycled	0x82	0x00	Power to the lock was restored and the lock's RTC was cleared. The controller should set the time to ensure proper logging.	0x08	0x01
Disabled user entered at keypad	0x83	0x (01-max users)	A disabled user pin code was entered at the keypad (Valid credential access denied due to User Active State being set to Occupied Disabled). Alarm level represents a truncated user slot numbers 256-500 therefore use Event Parameter to determine slot number.	0x06	0x2F
Valid user but outside of schedule	0x84	0x (01-max users)	A valid user can be both a normal user and a non-Access user. If a non-access user is out of schedule this alarm will be sent instead of the non-access alarm.	0x06	0x30
Invalid Credential Entered	0xA0	Number of Credentials in Attempt (0x01~0x03)	Invalid credential used to access the node	0x06	0x32
Tamper Alarm	0xA1	0x01	keypad attempts exceed code entry limit	0x06	0X10
		0x02	front escutcheon removed from main	0x09	0x06
Low Battery Alarms [3]	0xA7	0x (Current %)	*Low Battery* Starting at 7.2V	0x08	0x0A
	0xA8	0x (Current %)	*Critical Battery Level* Starting at 6.8V	0x08	0x0B

[0] These notifications are not supported with this Lock but supported in a shared module firmware.

[1] Deleting all user codes will also delete any associated schedules (year day and daily repeating scheduled pin codes) assigned to user codes.

[2] The Master Lock lock also supports a 3rd low battery alarm: too low to operate. This alarm is sent out as a Battery Report (with value = 0xFF) through the Battery Command Class. This is the last low battery alarm level before the product stops functioning. Starting at 6.0V

Command Class Configuration, Version 4*

* This command class requires security.

Table 8 - Configurable Parameters

Param. Num.	Name	Length	Configuration Properties			Info	Length of Info String
			Min	Max	Default		(Max length allowed is 90)
1	Volume	1 byte	0x01 (High Volume)	0x03 (Silent)	0x01 (High Volume)	Set Volume Level to high (1), low (2), or silent (3).	53
2	Auto Relock	1 byte	0x00 (Disable)	0xFF (Enable)	0xFF (Enable)	Set Auto Relock feature to enable or disable.	45
3	Relock time [1]	1 byte	0x01 (1 seconds) [1]	0xB4 (180 seconds)	0x03 (3 seconds)	Adjust the time your lock will auto relock.	43
4	Wrong Code Entry Limit	1 byte	0x03	0x0A	0x03	Adjust the limit for wrong code entries allowed by your lock.	61
7	Shut down time	1 byte	0x0A (10 seconds)	0x84 (132 seconds)	0x3C (60 seconds)	Adjust the time your lock is shutdown after reaching its wrong code entry limit.	80

8	Operating mode[2]	1 byte	0x00 (Normal Mode)	0x03 (Passage Mode)	0x00 (Normal Mode)	Set the Operating Mode to normal mode, keypad disable mode, privacy mode or passage mode.	89
11	One Touch Locking	1 byte	0x00 (Disable)	0xFF (Enable)	0xFF (Enable)	Set One Touch Locking feature to enable or disable.	51
12	Privacy Button	1 byte	0x00 (Disable)	0xFF (Enable)	0x00 (Disable)	Set Privacy Button feature to enable or disable.	48
13	Lock Status LED	1 byte	0x00 (Disable)	0xFF (Enable)	0x00 (Disable)	Set Lock Status LED feature to enable or disable.	49
16	Escape Return Mode	1 byte	0x00 (Disable)	0xFF (Enable)	0x00 (Disable)	Enable or Disable Escape Return Mode	36
18	Door Propped Timer [4], [5]	1 byte	0x00 (Disable) [4]	0xFE (2540 seconds) [4]	0x00 (Disable) [4]	Adjust the time to receive an alert when the door is propped open.	66
19	DPS Alarms (DoorSense™) [5]	1 byte	0x00 (Disable)	0xFF (Enable)	0xFF (Enable)	Enable or Disable DPS Alarms	28
28	Expiring Pin Code Enabled Time	1 byte	0x00 (Disable)	0xFF (127 Hours)	0x00 (Disable)	Timeout value used to determine time after first entry is triggered.	68

35	Invalid Credential Entry Alarms	1 byte	0x00 (Disable)	0xFF (Enable)	0x00 (Disable)	Set Invalid Various Credential Entry Alarms On/Off Using Mask	61

[1] Even though we accept value 0x01 for Auto Relock Time, we limit the lock's minimum to value of 0x03. Therefore, if user tries to set Auto Relock Time to values 0x01 or 0x02, it will always report back value of 0x03. After every power cycle where the lock was left unlock, the lock does a one-time auto-handing/auto relocking even if auto-relock feature is disabled.

[2] When Operation Mode feature is set to Passage Mode, this also results in disabling the following configuration parameters 2 (Auto Relock feature). The Passage Mode feature can only be set when Passage User Pin Code is used to unlock the lock.

[3] When this Escape Return Mode feature is enabled, this also results in disabling the following configuration parameters 2 (Auto Relock feature) and 11 (One Touch Locking feature).

[4] The Door Propped value is represented as seconds X 10. (ie a value of 4 would mean a door-propped timer of 40 seconds).

[5] Additional hardware required. These parameters are only active if the optional Door Position Switch has been installed with the lock and calibrated via Lock Settings.

Command Class Application Status, Version 1

This command class has been implemented by the Z-Wave® Specification.

Command Class Transport Service, Version 2

This command class has been implemented by the Z-Wave® Specification.

Command Class Supervision, Version 1

This command class has been implemented by the Z-Wave® Specification.

Command Class Indicator, Version 3*

* This command class requires security.

The indicator feature is set by using Indicator ID 0x50 to identify the node and Property ID 0x02 or 0x03, 0x04 and 0x05.

Table 9 – Lock UI for Indicator Set Overview

Indicator Set	**Lock Exterior**
OFF	Keypad LED is OFF
ON	MCB624/644: Numbers 0-9 on Touch Screen Flash MCB614/634: All buttons Flash

To set the Indicator ID 0x50 with Property 0x02, set values to 0x00 for off and 0x01…0x63 or 0xFF for on.

To properly set the Indicator ID 0x50 with Properties 0x03, 0x04 and 0x05, we had to map the values to our lock's specific blink rate.

Table 10 – Minimum Values for Indicator Set Property IDs 0x03, 0x04, & 0x05 to trigger Lock UI

Property ID 0x03 (On/Off Periods) Fixed Value	**Property ID 0x04 (On/Off Cycles) Minimum Value**	**Property ID 0x05 (On time within an on/Off period) Fixed Value**
0x13*	0x00...0xFF (per Z-Wave® Spec)	0x0A*

**NOTE: If Property IDs 0x03 and 0x05 are set to value other than the above, then the lock will blink at a different number of cycles than what you have set. **

Command Class Basic, Version 2*

* This command class requires security.

This command class is mapped to Door Lock CC:

Table 11 – Basic Mapping Overview

Basic Command	Door Lock Mapped Command
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 = 0xFF)

The Basic Get Current Value, Basic Get Duration, and Basic Get Target Value are mapped to Door Lock Operation Get and Basic Set is directly mapped to Door Lock Operation Set where the Duration is returned as is, but the Value and Target Door Lock State Value of the Basic Report use the following mapping:

Table 12 – Basic Report: Value

Value	Level	State	Door Lock State
0 (0x00)	0%	Off	Unsecure
1..253 (0x01...0xFD)	Reserved	Reserved	
254 (0xFE)	Unknown	Unknown	Unknown
255 (0xFF)	100%	On	Secure