



Schlage

Schlage Connect Smart Deadbolt

SKU: BE469ZP



Quickstart

This is a **secure Door Lock - Keypad** for **U.S. / Canada / Mexico**. Please make sure the internal battery is fully charged. To add this device to your network execute the following action:

One-button Add lock to Z-Wave Network (Inclusion) 1.Place your home automation system or panel into the Add or Inclusion Mode (Refer to the respective documentation for that specific home automation system or panel device for details). 2.Remove the battery cover of the deadbolt. 3.Press then release the button on the PCB.4.An LED will flash amber indicating the Add or Inclusion process is in progress. If the Security Scheme is Security 2 (S2), verify the DSK of the lock at the Z-Wave Controller. The PIN Code portion of the Z-Wave DSK will be needed.5.When a green LED turns ON, the Add or Inclusion has completed successfully. 6.If a red LED turns ON, try repeating steps 1-3Interactive Instruction for Add<https://instructions.allegion.com/instr/86/2543>

Attention: This manual is automatically generated from [Z-Wave Alliance](#) Product data and may be incomplete. Please refer to the [Manufacturers Manual](#) for more information.

What is Z-Wave?

Z-Wave is the international wireless protocol for communication in the Smart Home. This device is suited for use in the region mentioned in the Quickstart section.

Z-Wave ensures a reliable communication by reconfirming every message (**two-way communication**) and every mains powered node can act as a repeater for other nodes (**meshed network**) in case the receiver is not in direct wireless range of the transmitter.

This device and every other certified Z-Wave device can be **used together with any other certified Z-Wave device regardless of brand and origin** as long as both are suited for the same frequency range.

If a device supports **secure communication** it will communicate with other devices secure as long as this device provides the same or a higher level of security. Otherwise it will automatically turn into a lower level of security to maintain backward compatibility.

For more information about Z-Wave technology, devices, white papers etc. please refer to www.z-wave.info.



Product Description

The Schlage Connect Smart Deadbolt combines advanced features and compatibility with your home automation or security system, allowing you to control your lock from anywhere and freeing you from the hassles of lost keys, getting locked out, or hiding a spare for friends and family. The lock comes preprogrammed with two access codes and can hold up to 30 unique codes for family members and trusted friends. The fingerprint-resistant touchscreen helps access codes stay private, minimizing tell-tale wear that can tip off possible intruders. The Schlage Connect Smart Deadbolt is battery-powered with a low battery warning that gives you weeks of advanced notice before it runs out. With guaranteed fit on standard doors, its easy for homeowners to install in minutes with just a screwdriver. The touchscreen continues to work in the event of a power outage, so you don't have to worry about getting locked out plus, a back-up key is included with the lock for peace of mind. The Schlage Connect Smart Deadbolt incorporates Z-Wave Plus S2 technology, an enhanced security protocol that features an additional layer of AES encryption of wireless signals. The Z-Wave technology allows you to integrate your exterior door locks with other Z-Wave smart home devices, such as cameras, motion detectors, lights and thermostats, bringing the safety, simplicity and style of Schlage to your smart home.

Prepare for Installation / Reset

Please read the user manual before installing the product.

In order to include (add) a Z-Wave device to a network it **must be in factory default state**. Please make sure to reset the device into factory default. You can do this by performing an Exclusion operation as described below in the manual. Every Z-Wave controller is able to perform this operation however it is recommended to use the primary controller of the previous network to make sure the very device is excluded properly from this network.

Reset to factory default

This device also allows to be reset without any involvement of a Z-Wave controller. This procedure should only be used when the primary controller is inoperable.

Steps for One-button Factory Default Reset 1.Remove the battery cover of the deadbolt.2.Press and hold the button on the PCB for 7 (seven) seconds. While holding the button pressed, after 1 sec LED will be lit for 2 sec. and turn OFF; continue to press and hold the button until the LED will be lit again and release the button.3.The LED will blink red three times and the green check on the touchscreen will blink if the Factory Default Reset is successful. 4.To check that the lock was reset, press the Schlage Button and enter one of the Default User Codes. If the reset was successful, the Default User Codes will unlock the deadbolt. NOTE: Please use this procedure only when the network primary controller is missing or otherwise inoperable.

Inclusion/Exclusion

On factory default the device does not belong to any Z-Wave network. The device needs to be **added to an existing wireless network** to communicate with the devices of this network. This process is called **Inclusion**.

Devices can also be removed from a network. This process is called **Exclusion**. Both processes are initiated by the primary controller of the Z-Wave network. This controller is turned into exclusion respective inclusion mode. Inclusion and Exclusion is then performed doing a special manual action right on the device.

Inclusion

One-button Add lock to Z-Wave Network (Inclusion) 1.Place your home automation system or panel into the Add or Inclusion Mode (Refer to the respective documentation for that specific home automation system or panel device for details). 2.Remove the battery cover of the deadbolt. 3.Press then release the button on the PCB.4.An LED will flash amber indicating the Add or Inclusion process is in progress. If the Security Scheme is Security 2 (S2), verify the DSK of the lock at the Z-Wave Controller. The PIN Code portion of the Z-Wave DSK will be needed.5.When a green LED turns ON, the Add or Inclusion has completed successfully. 6.If a red LED turns ON, try repeating steps 1-3Interactive Instruction for Add<https://instructions.allegion.com/instr/86/2543>

Exclusion

One-button Remove lock from Z-Wave Network (Exclusion) 1.Place your home automation system or panel into the Remove or Exclusion Mode (Refer to the respective documentation for that specific home automation system or panel device for details). 2.Remove the battery cover of the deadbolt. 3.Press then release the button on the PCB. 4.An LED will flash amber indicating the Remove or Exclusion process is in progress. 5.When a green LED flashes 3 times, the Remove or Exclusion process is completed successfully. 6.If a red LED turns ON, try repeating steps 1-3 Interactive Instruction for Remove<https://instructions.allegion.com/instr/86/2581>

Quick trouble shooting

Here are a few hints for network installation if things dont work as expected.

1. Make sure a device is in factory reset state before including. In doubt exclude before include.
2. If inclusion still fails, check if both devices use the same frequency.
3. Remove all dead devices from associations. Otherwise you will see severe delays.
4. Never use sleeping battery devices without a central controller.
5. Dont poll FLIRS devices.
6. Make sure to have enough mains powered device to benefit from the meshing

Association - one device controls an other device

Z-Wave devices control other Z-Wave devices. The relationship between one device controlling another device is called association. In order to control a different device, the controlling device needs to maintain a list of devices that will receive controlling commands. These lists are called association groups and they are always related to certain events (e.g. button pressed, sensor triggers, ...). In case the event happens all devices stored in the respective association group will receive the same wireless command wireless command, typically a 'Basic Set' Command.

Association Groups:

Group Number	Maximum Nodes	Description
1	2	Z-Wave Lifeline

Configuration Parameters

Z-Wave products are supposed to work out of the box after inclusion, however certain configuration can adapt the function better to user needs or unlock further enhanced features.

IMPORTANT: Controllers may only allow configuring signed values. In order to set values in the range 128 ... 255 the value sent in the application shall be the desired value minus 256. For example: To set a parameter to 200 it may be needed to set a value of 200 minus 256 = minus 56. In case of a two byte value the same logic applies: Values greater than 32768 may needed to be given as negative values too.

Parameter 10: Lock Specific Alarm Kick Sensitivity

This configuration setting indicates the sensitivity setting of the Forced Entry function of the built-in alarm.

Size: 1 Byte, Default Value: 3

Setting	Description
1 - 5	Alarm Forced Entry Sensitivity

Parameter 11: Lock Specific Alarm Disable Local Controls

This configuration setting controls the ability to ENABLE or DISABLE local control of the built-in alarm function.

Size: 1 Byte, Default Value: -1

Setting	Description
0	Alarm Disable Local Controls
-1	Alarm Enable Local Controls

Parameter 12: Get Electronic Transition Count

This configuration setting indicates the number of transitions from locked to unlocked or unlocked to locked state via electronic activation.

Size: 4 Byte, Default Value: 0

Setting	Description
0 - -1	Electronic State Change Count

Parameter 13: Get Mechanical Transition Count

This configuration setting indicates the number of transitions from locked to unlocked or unlocked to locked state via mechanical activation.

Size: 4 Byte, Default Value: 0

Setting	Description
0 - -1	Mechanical State Change Count

Parameter 14: Get Electronic Failed Count

This configuration setting indicates the number of failed electronic activation attempts for this lock.

Size: 4 Byte, Default Value: 0

Setting	Description
0 - -1	Failed Electronic Activation Count

Parameter 15: Auto Lock

This configuration setting controls the lock feature that automatically throws the deadbolt 30 seconds after a valid User Code has been entered at the keypad.

Size: 1 Byte, Default Value: 0

Setting	Description
-1	Enable Auto Lock
0	Disable Auto Lock

Parameter 16: User Code PIN Length

This configuration setting controls the length of all User Codes stored in the lock. The values are 4 to 8 with default set to 4.

Size: 1 Byte, Default Value: 4

Setting	Description
4 - 8	User Code PIN Length

Parameter 17: Get Electrical High Preload Transition Count

This configuration setting indicates the number of transitions from locked to unlocked or unlocked to locked state via electronic activation that indicated a high preload on the deadbolt. This value is a subset of Parameter 12.

Size: 4 Byte, Default Value: 0

Setting	Description
0 - -1	Electronic State Change Count with High Preload

Parameter 18: Get Bootloader Version

This configuration setting returns the version number of the bootloader in the lock.

Size: 1 Byte, Default Value: 0

Setting	Description
0 - -1	Get Bootloader Version

Parameter 3: Beeper

This configuration setting controls the keypad beeper of the deadbolt allowing the keypad beeper to be turned ON or OFF

Size: 1 Byte, Default Value: -1

Setting	Description
-1	Enable Beeper
0	Disable Beeper

Parameter 4: Vacation Mode

This configuration setting controls the keypad entry of User Codes allowing all User Codes to be turned ON (disable Vacation Mode) or OFF (enable Vacation Mode)

Setting	Description
-1	Enable Vacation Mode
0	Disable Vacation Mode

Parameter 5: Lock and Leave Mode

This configuration setting controls the use of the u0022Schlageu0022 button on the keypad for single button push for throwing the deadbolt.

Size: 1 Byte, Default Value: -1

Setting	Description
-1	Enable Lock and Leave Mode
0	Disable Lock and Leave Mode

Parameter 6: User Slot Bit Field

This configuration setting indicates the occupied slots (from 1 to 30) that contain User Codes that will activate the deadbolt when entered on the keypad.

Size: 4 Byte, Default Value: 0

Setting	Description
0 - -1	User Slot Bit Field

Parameter 7: Lock Specific Alarm Mode

This configuration setting indicates the Mode of the built-in alarm function of the lock.

Size: 1 Byte, Default Value: 0

Setting	Description
0 - 3	Lock Specific Alarm Mode

Parameter 8: Lock Specific Alarm Alert Sensitivity

This configuration setting indicates the sensitivity setting of the Alert function of the built-in alarm.

Size: 1 Byte, Default Value: 3

Setting	Description
1 - 5	Alarm Alert Sensitivity

Parameter 9: Lock Specific Alarm Tamper Sensitivity

This configuration setting indicates the sensitivity setting of the Tamper function of the built-in alarm.

Size: 1 Byte, Default Value: 3

Setting	Description
1 - 5	Alarm Tamper Sensitivity

Technical Data

Hardware Platform	ZM5101
Device Type	Door Lock - Keypad
Network Operation	Listening Sleeping Slave
Firmware Version	HW: 3 FW: 3.03:10.08
Z-Wave Version	6.81.02
Certification ID	ZC10-18106281
Z-Wave Product Id	0x003B.0x0001.0x0469
Supported Notification Types	Access ControlPower ManagementSystem
Door Lock Type	Deadbolt
Security V2	S2_ACCESS_CONTROL

Supported Command Classes

- Antitheft V2
- Association Grp Info
- Association V2
- Basic
- Battery
- Configuration
- Device Reset Locally
- Door Lock V2
- Firmware Update Md V3
- Manufacturer Specific
- Notification V8
- Powerlevel
- Schedule Entry Lock V3
- Security 2
- Security
- Supervision
- Time
- Transport Service V2
- User Code
- Version V2
- Zwaveplus Info V2

Controlled Command Classes

- Time

Explanation of Z-Wave specific terms

- **Controller** — is a Z-Wave device with capabilities to manage the network. Controllers are typically Gateways, Remote Controls or battery operated wall controllers.
- **Slave** — is a Z-Wave device without capabilities to manage the network. Slaves can be sensors, actuators and even remote controls.
- **Primary Controller** — is the central organizer of the network. It must be a controller. There can be only one primary controller in a Z-Wave network.
- **Inclusion** — is the process of adding new Z-Wave devices into a network.
- **Exclusion** — is the process of removing Z-Wave devices from the network.
- **Association** — is a control relationship between a controlling device and a controlled device.
- **Wakeup Notification** — is a special wireless message issued by a Z-Wave device to announces that is able to communicate.
- **Node Information Frame** — is a special wireless message issued by a Z-Wave device to announce its capabilities and functions.