ELAN®

Integration Note

Manufacturer:	Baldwin, Kwikset, Schlage, Yale
Model Number(s):	**Baldwin 8252.112.AC3, 8252.112.AC3X, 8285.150.AC3, 8285.150.AC3X** **Kwikset Deadbolt 99100-0xx (where xx = 04, 05, 06, 011, 012, 013, 014)** **Schlage Deadbolt BE369, BE469** **Schlage Lever FE599, FE599NX** **Yale Deadbolt ARYD210, ARYD220** **Leviton RS-232 Adapter Vizia RF + 3 VRC0P-1LW**
Core Module Version:	5.7 or newer required
Document Revision Date:	4/14/2014

OVERVIEW AND SUPPORTED FEATURES

The Baldwin, Kwikset, Schlage, and Yale Door Locks are wireless Z-Wave Door Locks. The Baldwin, Kwikset and Yale Door Locks have a motorized deadbolt which can be extended or retracted via Z-Wave commands. The Schlage BE369 Door Lock receives Z-Wave commands which enable the deadbolt to be manually extended or retracted using the exterior knob. The Schlage FE599 Door Lock receives Z-Wave commands which enable the exterior lever to open the door latch.   These Door Locks are remote controllable over Z-Wave 900mhz wireless mesh networks via the use of a Z-Wave RS-232 adapter, enabling 2-way control and feedback from **g!**.

In addition to being controlled by Z-Wave commands, these Door Locks can be secured and unsecured by entering a user code on the keypad attached to the Lock, by turning an interior lever, or by using a physical key (as in traditional door locks).

The **g!** System will support up to 32 Door Locks in a Z-Wave network.

Note: Z-Wave RF operates at 900MHz. Any other devices operating on the same frequency may cause interference and might need to be relocated or removed. Leviton recommends the system in installations of 7500 square feet or less and installing devices typically no more than 30 feet apart. A maximum of 232 devices can be included in a Z-Wave network. Please refer to the Leviton **Vizia RF Systems Guide** (www.ViziaRF.com) for other installation considerations and details on proper setup of the Z-Wave networks. Additional information can be found at www.z-wave.com.

THE BALDWIN, KWIKSET AND YALE DOOR LOCKS SUPPORT THE FOLLOWING FEATURES:

Secure Lock: The Lock can be secured (ie, deadbolt extended) either by Z-Wave command, pressing a “lock” button on the exterior keypad, interior lever, or a traditional physical key.

Unsecure Lock: The Lock can be unsecured (ie, deadbolt retracted) either by Z-Wave command, user access code, interior lever, or a traditional physical key.

THE SCHLAGE BE369 DEADBOLT DOOR LOCKS SUPPORT THE FOLLOWING FEATURES:

Secure Lock: The definition of “Secure Lock” for the Schlage Deadbolt is different from the definition used for the Baldwin, Kwikset and Yale Locks. To “Secure a Lock” means to enable the deadbolt to be extended. The deadbolt can be extended in the following ways:

1. Send the “Secure Lock” Z-Wave command to the Lock; within 5 seconds, turn the exterior knob to extend the deadbolt.
2. Press the button labeled “Schlage” on the keypad; within 5 seconds, turn the exterior knob to extend the deadbolt.
3. Insert a physical (traditional) key into the key hole and turn the exterior knob to extend the deadbolt.
4. Turn the interior lever to extend the deadbolt.

Unsecure Lock: The definition of “Unsecure Lock” for the Schlage is different from the definition used for the Baldwin, Kwikset and Yale Locks. To “Unsecure a Lock” means to enable the deadbolt to be retracted. The deadbolt can be retracted in the following ways:

1. Send the “Unsecure Lock” Z-Wave command to the Lock; within 5 seconds, turn the exterior knob to retract the deadbolt.
2. Enter a user access code on the keypad; within 5 seconds, turn the exterior knob to retract the deadbolt.
3. Insert a physical (traditional) key into the key hole and turn the exterior knob to retract the deadbolt.
4. Turn the interior lever to retract the deadbolt.

THE SCHLAGE FE599 LEVER DOOR LOCKS SUPPORT THE FOLLOWING FEATURES:

Secure Lock: The definition of “Secure Lock” for the Schlage Lever is different from the definition used for the Baldwin, Kwikset and Yale Locks.. To “Secure a Lock” means to enable the exterior lever to operate the door latch. The door latch can be operated in the following ways:

1. Send the “Secure Lock” Z-Wave command to the Lock; the exterior lever will not be able to operate the door latch.
2. Press the button with the lock icon on the interior side of the Lock; the exterior lever will not be able to operate the door latch.

Unsecure Lock: The definition of “Unsecure Lock” for the Schlage is different from the definition used for the Baldwin, Kwikset and Yale Locks. To “Unsecure a Lock” means to enable the lever to operate the door latch. The door latch can be operated in the following ways:

1. Send the “Unsecure Lock” Z-Wave command to the Lock; the exterior lever will now be able to operate the door latch.
2. Enter a user access code on the keypad; for a period of 5 seconds, the exterior lever will be able to operate the door latch.
3. Insert a physical (traditional) key into the key hole and turn the key clockwise; the exterior lever will now be able to operate the door latch. (NOTE: To remove the key, turn the key counter-clockwise to the original position and remove the key. Doing this will resecure the Door Lock by disabling the exterior lever.)
4. Turn the interior lever to operate the door latch.

ALL DOOR LOCKS SUPPORT THE FOLLOWING FEATURES:

Auto Discovery: Door Locks may be auto-detected and added into **g!**.

Shared Z-Wave Network: A single Leviton Vizia RF Z-Wave network may contain Door Locks, Thermostats, and Lights. All three may be controlled over a single RS-232 Z-Wave adapter. See the appropriate Z-Wave Thermostats and Z-Wave Lighting Integration Notes for details.

ALL DOOR LOCKS SUPPORT THE FOLLOWING EVENTS:

Battery Alert: The battery level is low and should be replaced soon.

Failed user code attempt at lock: A user failed to enter a valid user code after multiple attempts. The exact number of attempts is defined by the Door Lock itself. Refer to the appropriate Door Lock documentation.

Secured: The Door Lock is “secured” – for Baldwin, Kwikset and Yale Locks, this means the deadbolt is extended; for the Schlage Locks, this means the deadbolt or door latch cannot be operated from the outside knob/lever.

Unsecured: The Door Lock is “unsecured” – for Baldwin, Kwikset and Yale Locks, this means the deadbolt is retracted; for the Schlage Lever Door Lock, this means the exterior lever will operate the door latch; for the Schlage Deadbolt Door Lock, this means the deadbolt can be operated by the exterior knob.

There are 5 types of “Unsecured” Events:

1. By any method – Lock unsecured by any of the following methods
2. Manually –
    a. For Baldwin, Kwikset and Yale: Lock unsecured by using a traditional key from the outside, or by manually turning the knob/lever on the inside
    b. For Schlage Deadbolt: Lock unsecured by using a traditional key from the outside, or by manually turning the knob/lever on the inside, or by entering the User Code and then manually turning the exterior knob
    c. For Schlage Lever: pressing the Unlock Icon on the interior side of the Lock
3. By the controller – the **g!** System sent the command to unsecure the Lock
4. By the master code – the master code was entered on the keypad to unsecure the Lock (currently, only the Yale Locks have this feature)
5. By user X (where X = 1-30) – User X Access Code was entered on the keypad to unsecure the Lock

Note: Using the traditional key or entering the User Code does NOT generate the “Unsecured” event for the Schlage Lever Lock.

User codes modified: The User Codes have been modified at the Door Lock

THE BALDWIN, KWIKSET AND YALE DOOR LOCKS SUPPORT THE FOLLOWING ADDITIONAL EVENTS:

Jammed: The motorized deadbolt jammed and could not be extended.

THE G! SYSTEM DOES NOT SUPPORT THE FOLLOWING FEATURES:

User Access Codes: The **g!** System will not require the user to enter an User Access Code to unsecure a Lock from the **g!** System User Interface. User Access Codes are required to be entered at the Lock’s keypad when unsecuring a Lock at the keypad.

Programming User Access Codes: The **g!** System will not support programming of User Access Codes. User Access Codes must be programmed at the Lock itself or through other third-party software.

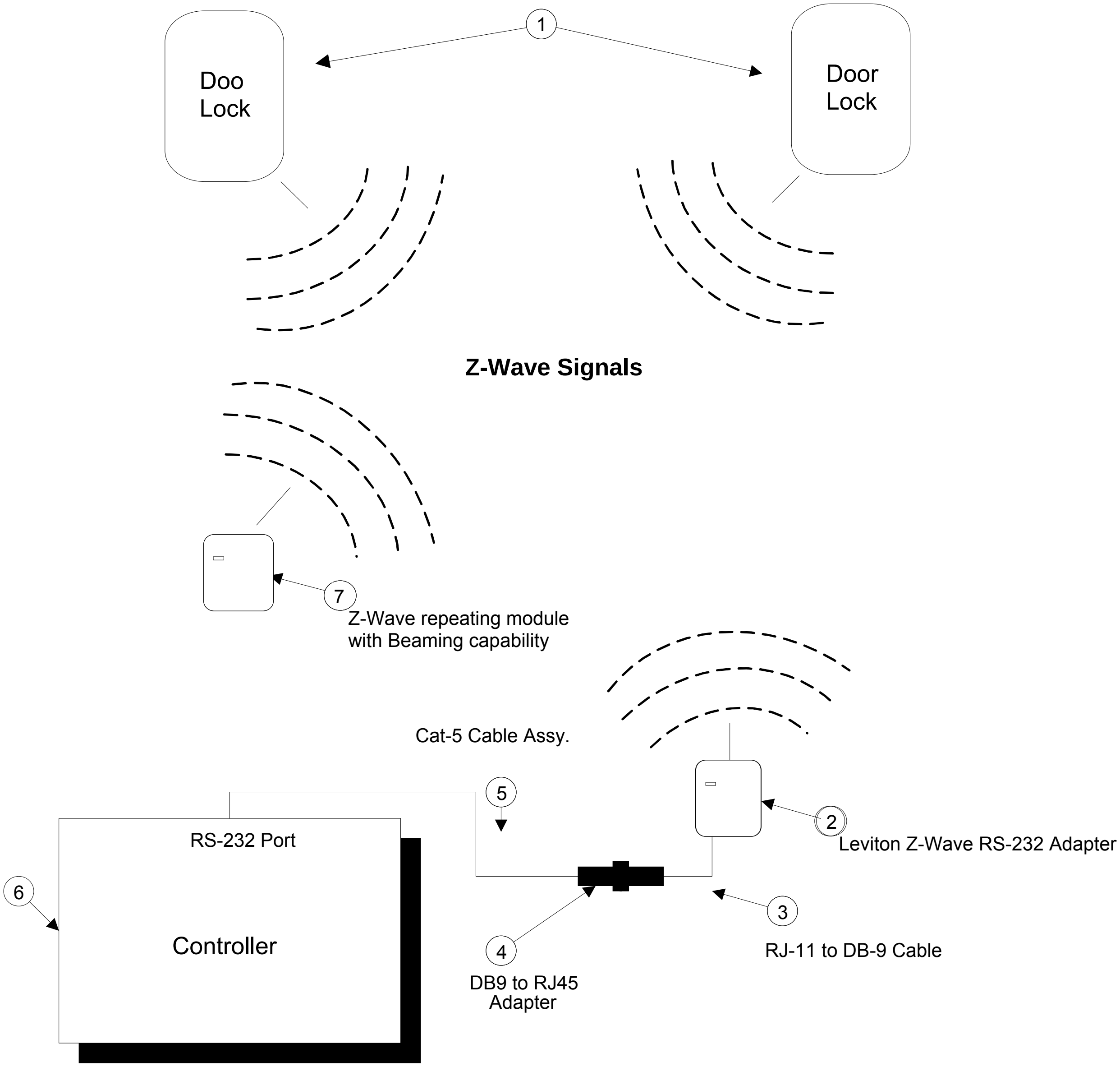
Any feature not specifically noted as supported should be assumed to be unsupported.

INSTALLATION OVERVIEW

1. Install the Door Locks according to the Installation Manual for that Door Lock.
2. Test the Door Locks using the User Access Codes to verify that the Locks can be secured and unsecured properly.
3. Install a Leviton RS-232 Z-Wave adapter in a location convenient for both a serial run to the **g!** controller and within range of other Z-Wave devices.
4. Run a Cat-5 or serial cable to the location of the Z-Wave RS-232 location.
5. Using a Primary Controller, such as a programming remote (ex. Leviton VRCPG) or controlthink ThinkEssentials, create a Z-Wave network and add Door Locks and the RS-232 adapter according to standard procedures.
6. Connect the Serial Cabling to the Z-Wave RS-232 adapter electrically. See the wiring diagrams.
7. Configure **g!** for the Door Locks and confirm communication between the Door Locks and the **g!** system controller.
8. Test the system by securing and unsecuring the Door Locks, confirming that the various components in the system respond as expected.

CONNECTION DIAGRAMS

.



BILL OF MATERIALS

#	Device	Manufacturer	Part Number	Protocol	Connector Type	Notes
1	Door Locks	Baldwin	8252.112.AC3 8252.112.AC3X 8285.150.AC3 8285.150.AC3X	Z-Wave	RF	Has motorized deadbolt
		Kwikset	99100-0xx	Z-Wave	RF	Has motorized deadbolt
		Schlage	BE369, FE599	Z-Wave	RF	Enables deadbolt, door latch operation
		Yale	ARYD210,	Z-Wave	RF	Has motorized deadbolt
2	Zwave RS-232 Adapter	Leviton	VRC0P-1LW	Z-Wave/RS-232	RJ-11 Female	Needs to be the Vizia RF + 3 version
3	RJ-11 to DB9 Cable	Leviton	N/A	RS-232	RJ-11 Male/DB9 Female	Included with VRC0P
4	DB9 to RJ45 Adapter	ELAN	HA-CB-307	RS-232	RJ-45 Female X DB-9 Male	
5	Cat5 Cable Assy.	Installer	N/A	RS-232	RJ-45 Male X Wire	Must terminate all 8 conductors
6	Controller	ELAN	Various (ex. HC-12)	RS-232	RJ-45 Female	Use COM1, 2, 3, etc
7	Z-Wave Modules that support "Beaming"	Leviton	VRCS4-M0	Z-Wave	RF	
		Leviton	VRCZ4-M0	Z-Wave	RF	
		Leviton	VRP03-1LW	Z-Wave	RF	
		GE	Lamp Module 45602	Z-Wave	RF	
8	Programming Remote **OR** ThinkEssentials **OR** Vizia RF+ Installer Tool	Leviton	VRZCPG	Z-Wave	N/A	Not shown, needed for programming
		Leviton	CTZUS-1US	Z-Wave	USB	Not shown, needed for programming
		Leviton	VRUSB-1US	Z-Wave	USB	Not shown, needed for programming

Z-WAVE NETWORK PROGRAMMING

Program the Z-Wave according to standard procedures. Regardless of device function, the basic setup of Z-Wave networks is the same.

Typically a Z-Wave network is programmed using its Programmer/Remote Control (such as the Leviton VRZCPG) or Think Essentials Software to enroll devices into the Z-Wave Network. The method for using the VRZCPG and Think Essentials/USB Z-Wave adapter are both detailed below. Note that these instructions assume you are familiar with Z-wave programming concepts. If you require further detail or clarification, you may wish to see Leviton Vizia RF (www.ViziaRF.com), or Baldwin, Kwikset / Schlage / Yale documentation/technical support for assistance.

PROGRAMMING USING THE LEVITON *VRCPG-BSG* REMOTE:

Setup steps below are created using a VRCPG-BSG remote. Your steps may vary somewhat if version/remote model differ, but the basic process should be the same.

1. **Confirm all devices are at factory default and have not been setup in any Z-Wave Network.**
2. Start up the Leviton Remote and begin the **Installation Checklist**.
    a. Perform **Step 1** of the Install Checklist, **Include Dim/Switch**, and enroll (include) the first Door Lock into the network.
    b. When prompted by the remote, perform the following action on the Door Lock (based on the brand).The VRZCPG will automatically assign a unique node ID to the Door Lock during this process.

i. Baldwin, Kwikset – Remove the cover from the interior side of the Door Lock; press the small white button in the upper left section.

ii. Yale – Enter the Master Code, press "#", enter "7" ("Wireless Setting Mode"), press "#", enter "1".

iii. Schlage – Enter the Master Code, press the "Schlage" button, enter "0".

It is best practice to give the Door Lock a descriptive name when prompted, like Front Door, for future reference. Note that this name is not saved in the Door Lock and will not be automatically read into ***g!****. You may wish to keep notes of the location of each Door Lock and their Node ID, as the only identification available to* ***g!*** *is the Node ID.*

3. Repeat Step 2 for each additional Door Lock being added to the network.
4. Perform **Step 2** of the Install Checklist, **Include Controller**, to enroll (include) the RS-232 interface controller VRC0P-1LW (+3) into the network. Note that to include Controllers, they must be in Program Mode. To set the VRC0P-1LW into programming mode, press and hold the button (clear tab on face of unit) until the light blinks amber.
5. Perform **Step 3** of the Install Checklist, **Update Controller**, to update all of the controllers following the inclusion of all devices. This will create the proper mapping between devices.
6. In a Door Locks only network, you may skip Step 4 (**Create Areas**) and choose Step 5, **Set Associations**.
7. Perform **Step 5** of the Install Checklist, **Set Associations**, to associate each Door Lock with the controller.
8. Choose **Step 6** of the Install Checklist, **Install Complete**, to finish the installation.

PROGRAMMING USING THINKESSENTIALS AND USB Z-WAVE ADAPTER:

Setup steps below are created from version 2.5.5 of ThinkEssentials. If you are running a different version, your steps may be somewhat different than below, but the basic process is the same.

1. **Confirm all devices are at factory default and have not been setup in any Z-Wave Network.**
2. In the **Design Tab**, press the **include devices** button to enroll all devices into the network. The laptop running ThinkEssentials must be within three feet of the Door Lock. The Door Locks are included by performing the following action when the VRZCPG prompts to press a key on the dimmer.The VRZCPG will automatically assign a node ID to each Door Lock during this process.
   a. Baldwin, Kwikset – Remove the cover from the interior side of the Door Lock; press the small white button in the upper left section.
   b. Yale – Enter the Master Code, press "#", enter "7" ("Wireless Setting Mode"), press "#", enter "1".
   c. Schlage – Enter the Master Code, press the "Schlage" button, enter "0"

It is best practice to give the Door Lock a descriptive name when prompted, like Front Door, for future reference. Note that this name is not saved in the Door Lock and will not be automatically read into ***g!****. You may wish to keep notes of the location of each thermostat and their Node ID, as the only identification available to* ***g!*** *is the Node ID. Likewise, drawing rooms in the Design tab of the ThinkEssentials software may be beneficial to you during setup, but will have no effect on integration with* ***g!*** *and is optional.*

3. In the **Design Tab**, press the **Include Controller** button to enroll Controllers into the network. The laptop running ThinkEssentials must be within three feet of the Controller. Controllers include the RS-232 interface module (VRC0P-1LW). Note that to include Controllers, they must be in Program Mode. To set the VRC0P-1LW into programming mode, press and hold the button (clear tab on face of unit) until the light blinks amber.
4. In the **Design Tab**, associate each Door Lock to the Controller:
    a. Move to within three feet of the Door Lock
    b. Right-click on the Door Lock icon and select "Properties"; in the lower right-hand corner of the display, the status message "Loading status from the device" appears; wait until the status message changes to "Done loading status."
    c. Switch to the "Device Associations" tab
    d. For the Baldwin, Kwikset and Yale Door Locks, select "Button #1" in the drop down menu; for the Schlage Door Locks, select "Button #2"
    e. Press the "Edit" button – a pop up appears
    f. Left-click on the Controller icon to make the association, then click on "Done" in the pop up

TESTING THE Z-WAVE NETWORK

Once the Z-Wave Network is set up, it can be tested by sending "Secure" and "Unsecure" commands to the Door Locks and verifying that the Door Locks operate as expected. Also, when the Door Locks change state, one should verify the status message is sent. This testing can be done using a terminal services program (such as "hyperterm", which the following instructions will assume is being used).

1. Hyperterm set up:
    a. Baud = 9600; Data bits = 8; Parity = None; Stop bits = 1; Flow Control = None
    b. Under Settings / Ascii Setup / Ascii Sending, select the following two options by placing a check in the checkbox:
        i. Send line ends with line feeds
        ii. Echo typed characters locally
2. Commands – Each command begins with the character '>' and ends with a Carriage Return and a Line Feed ("<CR><LF>"). With the above settings, Hyperterm will append the line with a "<CR><LF>" when the Enter key is pressed.
    a. Secure Lock = ">NxSS98,1,255<CR><LF>", where 'x' is the Node ID of the Door Lock
    b. Unsecure Lock = ">NxSS98,1,0,<CR><LF>", where 'x' is the Node ID of the Door Lock
3. Status Messages
    a. For the Baldwin, Kwikset and Yale Locks, the format of the Lock Status message looks like this:

        "<nxxx,000,113,005,yyy,zzz" - where "xxx" is the Node ID (eg, "002" for Node ID 2),
        and "yyy" is the status as defined below,
        and "zzz" is the User Code entered (if applicable)

        i. 018 – Lock secured by Keypad
        ii. 019 – Lock unsecured by Keypad (and "zzz" will be the User Code entered)
        iii. 021 – Lock secured manually
        iv. 022 – Lock unsecured manually
        v. 024 – Lock secured by Z-Wave command
        vi. 025 – Lock unsecured by Z-Wave command

b. For the Schlage Locks, there are two formats.

i. The first is similar to the one above for the Baldwin, Kwikset and Yale locks, but the only value for “yyy” is “016” which means a User Code was entered and the User Number is in the “zzz” field.

ii. The second format looks like this:

“<nxxx:000,098,003,yyy,000,000,254,254” – where “xxx” is the Node ID, and “yyy” is the status defined below:

1. 000 – Lock is unsecured
2. 255 – Lock is secured

4. Other Messages – There are other messages that will appear in the Hyperterm window, but they are not important for the purpose of testing the Z-Wave Network.
5. Connect the RS-232 port of the PC running Hyperterm to the VRC0P.
6. To test Baldwin, Kwikset or Yale locks, perform the following steps:

a. Start with all locks unsecured

b. Enter the “Secure Lock” command for one of the locks (eg, “>N2SS98,1,255,<CR><LF>” for Lock with Node ID = 2). Verify the following:

i. The Lock extends the deadbolt, thus becoming “Secured”

ii. The Lock Status Message is received on Hyperterm stating the Lock is secured

c. Enter the “Unsecure Lock” command for the same Lock. Verify the following:

i. The Lock retracts the deadbolt, thus becoming “Unsecured”

ii. The Lock Status Message is received on HyperTerm stating the Lock is unsecured

d. At the Door Lock, perform the following actions and verify the corresponding Lock Status Message is received on Hyperterm:

i. Manually secure the lock

ii. Manually unsecure the lock

iii. Press the “***lock***” button on the Door Lock to secure the lock

iv. Enter the User Code on the Keypad to unsecure the lock

e. Repeat the above steps for each lock in the Z-Wave Network.

7. To test the Schlage Deadbolt Lock, perform the following steps:

a. Start with all locks unsecured

b. Enter the “Secure Lock” command for one of the locks (eg, “>N2SS98,1,255,<CR><LF>” for Lock with Node ID = 2). Verify the following:

i. The deadbolt can be extended by turning the exterior door knob (this must be done within 5 seconds because the Schlage lock will automatically relock itself after the 5 second interval)

ii. The first Lock Status Message received on Hyperterm states the Lock is unsecured – this is in response to the “Secure Lock” message, but the deadbolt has not yet been extended so the lock is still unsecured

iii. The second Lock Status Message received on Hyperterm will state that the Lock is now secured – this is received in response to the deadbolt being manually extended

c. Enter the “Unsecure Lock” command for the same lock. Verify the following:

   i. The deadbolt can be retracted by turning the exterior door knob (this must be done within 5 seconds because the Schlage lock will automatically relock itself after the 5 second interval)

   ii. The first Lock Status Message received on Hyperterm states the Lock is secured – this is in response to the “Unsecure Lock” message, but the deadbolt has not yet been retracted so the lock is still secured

   iii. The second Lock Status Message received on Hyperterm will state that the Lock is now unsecured – this is received in response to the deadbolt being manually retracted

d. At the Door Lock, perform the following actions and verify the corresponding Lock Status Message is received on Hyperterm:

   i. Manually secure the lock

   ii. Manually unsecure the lock

   iii. Press the “***Schlage***” button on the Door Lock to enable the knob to extend the deadbolt, and turn the knob to extend the deadbolt

   iv. Enter the User Code on the Keypad to enable the knob to retract the deadbolt, and turn the knob to retract the deadbolt

e. Repeat the above steps for each lock in the Z-Wave Network.

8. To test the Schlage Lever Lock, perform the following steps:

   a. Start with all locks unsecured

   b. Enter the “Secure Lock” command for one of the locks (eg, “>N2SS98,1,255,<CR><LF>” for Lock with Node ID = 2). Verify the following:

      i. The lever will not operate the door latch – the lock is “secured”

      ii. The Lock Status Message received on Hyperterm states the Lock is secured

   c. Enter the “Unsecure Lock” command for the same lock. Verify the following:

      i. The lever will operate the door latch – the lock is “unsecured”

      ii. The Lock Status Message received on Hyperterm states the Lock is unsecured

   d. Press the “Lock” button on the interior side of the Door Lock. Verify the following:

      i. The lever will not operate the door latch – the lock is “secured”

      ii. The Lock Status Message received on Hyperterm states the Lock is secured

   e. Press the “Unlock” button on the interior side of the Door Lock. Verify the following:

      i. The lever will operate the door latch – the lock is “unsecured”

      ii. The Lock Status Message received on Hyperterm states the Lock is unsecured

   f. Press the “Lock” button to secure the lock. Enter a valid User Code on the Keypad. Verify the following:

      i. The lever will operate the door latch for 5 seconds

      ii. The only Lock Status Message received on Hyperterm is the “User Code Entered” message

   g. Repeat the above steps for each lock in the Z-Wave Network.

NOTES REGARDING THE USE OF REPEATER MODULES THAT SUPPORT BEAMING:

The VRC0P can communicate to any Z-Wave device that is within 75 feet line of sight. But due to the walls and other obstacles in a house, the VRC0P can communicate to another device that is up to 30 feet away. To communicate to devices beyond 30 feet, a repeater is needed.

Most Z-Wave device modules today also act as repeaters. If the VRC0P cannot communicate directly to a Z-Wave device directly, the programming software (eg, Vizia RF Installer) will build routing tables that directs the VRC0P to send commands to a repeater which will then send the commands on to the target device. This is called “hopping” and a command may “hop” up to four times.

For any device to communicate to a Door Lock (or any other battery operated device), that device must support “beaming”. Battery operated devices sleep to conserve battery life and wake up once a second, turn on their radio for 4ms to listen for a “beaming” message directed to them. If they sense a “beaming” message for them, they respond to the message; if they do not sense a “beaming” message for them, the go back to sleep.

Not every repeating device supports beaming. Be sure to only use repeaters that support beaming when using Door Locks.

NOTES REGARDING THE TRACKING OF Z-WAVE DEVICES:

In general **g!** will keep track of the states of all of the Z-Wave Network Devices; however there is latency in the reporting back of the devices from the Z-Wave network. The result is that **g!** will update its states as the devices report back. This is evident when watching the viewer interface after a change is made at the device. The viewer controls will update sequentially over a few seconds (or more on larger systems) as the devices report their state.

With no repeaters in the Z-Wave network (or if the Door Locks are close enough to the VRC0P to be able to communicate to it directly without going through a repeater), it takes about 3 seconds to secure or unsecure a door. From the time a user presses a button on the **g!** System UI till the Door Lock is secured or unsecured is about 3 seconds. It will take another 2 seconds for the lock status to be reported by to the **g!** System. The reason for the delay is inherent in the Z-Wave communication protocol. Because the Lock is battery operated, it is normally in a sleep state and wakes up once a second to see if the controller has any messages / commands for it. Then it goes through some handshaking to establish a secure path (using encrypted data for the transmission). This is what accounts for the apparent slow response time.

To secure or unsecure four locks will take about 30 seconds. To secure or unsecure 18 locks will take about 2 minutes and 35 seconds. In both cases, commands are sent down to the VRC0P one at a time and before the next one is sent, the **g!** System makes sure all communication between the VRC0P and the Lock is complete.

If the VRC0P must go through a repeater to get to the Door Lock, then the above times become longer. This is because each message transmitted by the VRC0P or the Door Lock has to now be retransmitted by the repeater. In the above example of four locks, if each lock had a repeater between it and the VRC0P, the time to secure or unsecure the four locks would be about 45 seconds instead of 30 seconds. If there were two or three repeaters between each lock and the VRC0P, the time would be even longer.

NOTES REGARDING SIMULTANEOUS OPERATION OF Z-WAVE DEVICES:

If two Z-Wave devices attempt to transmit messages to the VRC0P at the same instant, there is about a 10% chance that one of the messages won't make it through. Both Locks will attempt to transmit over RF their message and they may step on each other. There is a retry mechanism built into the Z-Wave protocol, but it is not fool-proof. This means that if two users were at two different Door Locks, and they both locked their lock at the same time, there is a 10% chance that the UI's on the **g!** System would show only one of the locks as secured. However, the odds of two people locking two locks at the same time is extremely small and this should not be a problem.

Another scenario is when one user is using the **g!** System UI to secure Door Lock #1, and the other user is at Door Lock #2 and locks Door Lock #2. Again, there is a 10% chance that not all the messages would be transmitted and received intact. This too could result in the **g!** Sytem's UI not reflecting the correct state of one of the locks. There is also a small chance within that 10% failure rate, that the message that failed to be transmitted and received was the "Secure Door Lock #1" command – meaning Door Lock #1 would not be secured. Again, the odds of two people operating locks at the same time (one from a UI, the other from the lock itself) is extremely small.

Each Door Lock is polled by the **g!** system 60 minutes after the last interaction with the Door Lock. So if the Door Lock Status on the **g!** System UI did get out of sync with the true Door Lock Status, it would be updated to the correct status in 60 minutes.

A third scenario involves two users using the **g!** System UI to control two different Locks at the same time. This is NOT a problem, because the Z-Wave Lock driver will only send one command at a time to the VRC0P and will wait for the Lock to respond before sending another command. No messages are lost in this scenario.

NOTES REGARDING THE EVENT "LOCK UNSECURED BY THE MASTER CODE":

Only the Yale Locks allow a Lock to be unsecured by entering the Master Code. Therefore, the event "Lock Unsecured by the master code" will only be generated for the Yale locks. This event will never occur for the Baldwin, Kwikset and Schlage locks.

IMPORTANT NOTES ABOUT THE NON-MOTORIZED SCHLAGE B369 DOOR LOCKS

1. The deadbolt is not motorized, therefore a person must be physically present at the Door Lock to extend / retract the dead bolt. This means the homeowner can NOT send a command from the **g!** System UI to "lock" the door (ie, extend the deadbolt).
2. The "Unsecure Lock" command sent from the **g!** System will "unsecure" the lock by making the deadbolt operable by the exterior knob for a period of 5 seconds only; after that, the deadbolt becomes un-operable again (ie, the lock automatically relocks).
3. The event "Lock unsecured by user X" is not generated by the Schlage Deadbolt Lock; the event "Lock unsecured manually" is generated instead.

IMPORTANT NOTES ABOUT THE SCHLAGE FE599 LEVER DOOR LOCKS

1. When the User Code is entered, the lever will operate the door latch for a period of 5 seconds; after that time, the door automatically "relocks" making the door latch un-operable from the outside.
2. When the key is used to unlock the door, the door is relocked when the key is removed. There are NO events generated when the Door Lock is "secured" or "unsecured" in this manner.
3. When the User Code is entered to open the door, there are NO events generated when the Door Lock is "unsecured" or when it is "secured" after the 5 second interval.

CONFIGURATION DETAILS

The following table provides settings used in the **g!** Configurator when connecting to a Z-Wave thermostat network. Please refer to the *Configurator Reference Guide* for more details.

In the table below:

o “<Select>” in the Configurator.	Select the appropriate item from the list (or drop-down)
o “<User Defined>”, etc.	Type in the desired name for the item.
o “<Auto Detect>”, etc.	The system will auto detect this variable.

Devices	Variable Name	Setting	Comments
Communication Devices	**Name**	<User Defined> (Default New Device)	
	Type	**Serial Port**	
	Communication Type	**Leviton Z-Wave RS232 Network**	
	Location	<User Defined> (Not Required)	
	Com Port	<Select>	COM1, 2, 3, etc.
<Discover Devices>			Click the **Discover Devices** button on the Communication Device
Door Locks	**Name**	<User Defined>	Discover Devices will set a default name of “Z-Wave Door Lock #2”, etc.
	Communication Device	<Auto Detect>	
	Door Lock ID	<Auto Detect>	This value is the Node ID of the Door Lock in the Z-Wave network.

COMMON MISTAKES

1. Placing the Z-Wave RS-232 Adapter out of range of other Z-Wave devices. Z-Wave devices create a wireless, self-healing mesh network, and should be placed where they are in range to communicate with multiple other devices for best results.
2. Improper Z-Wave setup. Ensure to fully program and test your z-wave network for proper operation **prior** to integration with **g!**.
3. Using Z-Wave devices as repeaters that don't support "beaming".