Latch R // Runbook
v.1.1 August 2023

Table of Contents

- Product Overview
- Best Practices and Field Notes
- For Install and Service
  - Tools
  - Permissions (Confirm Access)
- Latch Specification Guide
- Onboarding
  - 1. Assign a device
  - 2. Assign or create a door
  - 3. Upgrade the Firmware of the device
  - 4. Configuration
  - 5. Test unlock
  - 6. Test lock
- Troubleshooting Workflow
  - 1. Confirm the Mobile device is functioning properly
  - 2. Check the Lens
  - 3. Update and Firmware Upgrade
  - 4. Issues with the Latch App or Latch Manager App
  - 5. Check Power
  - 6. Check for broken hardware / environmental impacts / third-party hardware
  - 7. Check Latch device functionality
  - 8. Confirm Relay Changes State
  - 9. Power Cycle the Device
- RMA Process
- Advanced Technical Support Guide
  - Input/Output (I/O) Troubleshooting
  - Weigand Troubleshooting
  - Ethernet & WiFi Troubleshooting
    - Troubleshooting WiFi Configuration
    - WiFi Signal Strength Chart
    - Port Filter/Blocked Test
  - Elevator Floor Access (EFA)
    - Requirements
    - Wiring Requirements

Programming the Latch R
Programming the Access Panel
Testing EFA
Approved 3rd party access control system
Firmware Upgrade Troubleshooting

Product Overview

The Latch R combines a reader, door controller, and management system into one simple product. The device directly connects to any electrified locking mechanism in addition to motion detectors and request-to-exit devices.

Latch R - webpage

Latch R - Installation guide

Best Practices and Field Notes

1. Use Provided Hardware
   a. Use the mounting screws that are provided with the hardware. If using different mounting screws, use #6 flat-head screws.
2. Preparation is Key
   a. To avoid mounting difficulties, verify or provide the appropriately sized hole and necessary depth for the wires and connection points.
3. Don’t Force It
   a. Use care when mounting the reader on the backplate to avoid damage.
4. Keep the Copper Covered
   a. Make sure unused wires on the reader pigtail have no exposed wire ends.
5. Use Appropriate Cabling for Power and Ethernet
   a. Braided 18 gauge, 2-conductor for power, and CAT6 for ethernet. DO NOT attempt to power the reader with CAT6 or twisted pair wire.

Field Notes

1. When Latch R is configured for WiFi, there must be a strong WiFi signal for the Latch R to function properly, ensure reliability, and provide an acceptable User experience. Be aware of the WiFi infrastructure prior to installation and ensure the location(s) of the installed readers are provided for appropriately. Please see the WiFi Troubleshooting guide below for signal strength recommendations as well as troubleshooting steps.
2. Make sure unused wires on the reader pigtail have no exposed wire ends. Failure to properly terminate and or cover exposed wire ends could damage the device.
3. If a door operator is being integrated, be mindful of the voltage/amperage that is passing through the Latch R relay and ensure it does not exceed the relay rating (1.5A, 24V DC, or 16V AC max).
4. Latch R Operating Power is 6W (0.5A @12VDC, 0.25A @24VDC) You may experience intermittent issues with the Latch R if there are multiple devices being powered by the same output on the power supply resulting in overconsumption of voltage and amperage. (i.e. Latch R, REX/motion, Lock, etc.)
5. Confirm that the Door Schedule is set to the desired timeframe (if the door schedule feature is being used).

   a. If a Latch R has a door schedule enabled, the relay could be in an open or closed state.
   b. This is important to know for anyone troubleshooting the relay.
6. Be aware of ADA Requirements.
7. All elevator integrations must include oversight from an elevator technician.

For Install and Service

Tools

Phillips #2 Screwdriver
Torx T-20 Security Screwdriver/Bit
Multimeter
Wire connectors
iOS Mobile Device

Permissions (Confirm Access)

a. Confirm the user has the correct access permissions

Latch Manager App

i. Device Management Permissions
ii. Unlock Access

Latch App

iii. Unit Unlock Access
iv. This is needed to perform a test call on the unit - note PM will have to set this up.

Latch Specification Guide

Onboarding

1. **Assign a device**
    a. Once you have installed the Latch device, you need to add and save the device's information:
        i. Open the Manager App.
        ii. Select the ‘New Door’ icon in the top right corner.
        iii. You’ll then be prompted to scan the QR Code on the Latch Device.
        iv. Scan the QR Code on the rear of the device.
        v. Select the desired Portfolio and Property Information of the property you are installing in.
2. **Assign or create a door**
    a. If you have pre-created a door in Latch Manager you can assign it by selecting 'Door Name.'
    b. If you have not pre-created the door you’ll need to create one. To do so:
        i. Enter the door or apartment name.
        ii. Select the door type. Learn more about door types.
            1. Latch R is most commonly used for communal, service, and building entrances.
3. **Upgrade the Firmware of the device**
    a. Select the latest firmware version.
    b. You’ll then be prompted to go through the upgrade process.
    c. Select ‘Start.’
    d. The Latch Device should then start upgrading. (Note: the upgrade on non-Geneva lens products like R1 & R2 can take about 10 minutes, do not step away from the device or navigate out of the Manager app).
    e. Once successful, select 'Next’ to move to configuration.
4. **Configuration**
    a. Once you have saved the device's information (see 'Adding a Device' above) navigate to the device list screen.
    b. Select the device you installed.
    c. Select 'Configure.'
    d. Select the appropriate relay configuration for the device.
        i. Normally open: Sets the Latch R relay to be normally open.
        ii. Normally closed: Sets the Latch R relay to be normally closed.
        iii. Panel: Select if you are connecting Latch R to an existing access control panel.

- e. If you are connecting to a panel, enter the Facility Code and Card ID for a card that unlocks the panel at all times and days.
- f. Select the re-lock time.
- g. If you have connected ethernet to the device, toggle it on.
  - i. If you require static ethernet configuration, toggle to static mode, and enter the subnet mask, gateway, and IP address.
  - ii. Save configuration.
  - iii. If you need to change the configuration of a Latch R:
    1. Navigate to the devices list.
    2. Select 'Configure.'
    3. Re-configure the settings and save.

5. Test unlock

- a. You will then be prompted to test unlock by tapping ‘Tap to unlock.’
- b. Check that the device is unlocked and the door opened.
- c. Select ‘Next.’
- d. Select ‘Finish.’

6. Test lock

- a. The door will relock after 5s, or 10s depending on device configuration.
- b. Make sure that the device re-locks as expected prior to closing and securing the door.

Troubleshooting Workflow

1. **Confirm the Mobile device is functioning properly**
    a. Confirm that the mobile device is being used to interface with the Latch device.
        i. Is compatible with Latch (supported models here)
        ii. Has strong and reliable cellular or WiFi service.
            1. The user's mobile device must have at least two bars of reception for wifi or cellular to ensure the best access and device performance.
            2. Without adequate cellular or wifi service to the user's mobile device:
                a. Updates and Firmware Upgrades will fail.
                b. Any changes to a user's access permission will fail to update as well leading to failed unlocks.
        iii. Has Bluetooth been enabled?
        iv. Isn’t in a protective case that may interfere with the performance.

2. **Check the Lens**
    a. Do the LEDs on the lens light up when the lens is touched?
        i. If not, follow the power troubleshooting steps.
    b. Are any LEDs lit continuously and/or pulsing
        i. LED feedback instances
            1. Denial of Service (DoS):
                a. The LED on the Latch Lens located in the “12 o’clock” position, when illuminated indicates **that another device is connected to the lens over BLE.** If the Latch device detects continuous attempts to connect via Bluetooth, it will automatically go into DoS mode after 50 failed attempts and BLE unlock will no longer be available.

                b. DoS mode is a feature that has been incorporated into the Latch Lens functionality to prevent unauthorized blocking of a Latch device via continuous Bluetooth connection attempts.

c. Once a lock is put into DoS mode, it remains in that state for 5 minutes, or until the device is reset or a user successfully authenticates using either an NFC card or a passcode.

d. After 5 minutes of inactivity, the device will resume normal advertising in order to prevent inadvertently extended lockouts.

2. Rate Limiting Mode (RLM):
    a. Rate limiting mode is indicated by the digits 5 and 6 flashing on the Lens.
    b. 20 consecutive NFC or Passcode failures put the device into rate limiting mode (RLM). While in this state, the device will not accept those types of accesses for 5 minutes. After 5 minutes, SOS mode starts where NFC and passcodes will be allowed thrice before entering RLM mode again if they continue to fail.
    c. Successive RLM entries will increase the blocking access time by 5 minutes up to 25.
    d. In order to exit Rate Limiting Mode, simply enter a correct Door Code, use a valid keycard, or perform a BLE unlock via the Latch App. If one of the authentication attempts results in a successful unlock the lock moves into normal mode, if not it moves back into RLM mode.

3. Update and Firmware Upgrade

a. Ensure the Latch device has been updated recently with the Latch App (instead of the Latch Manager App)
    i. Confirm the device has been updated
        1. Open the Latch App.
        2. Navigate to and select the door in question.
        3. Select the “Update” tab.

b. Ensure that the Latch Device has been upgraded to the latest version of the firmware.

4. Issues with the Latch App or Latch Manager App

a. Check for any updates that may be available for your Latch App (iOS and Android) and Manager App.
b. Toggle the mobile device's Bluetooth settings off, and then back on.
c. Power cycle the mobile device (turn it off, wait for 30 seconds, restart the device).
    i. If Android device, perform the Bluetooth cache clear and location services toggle.
d. Log out of and back into the Latch app.
e. Delete and reinstall the Latch app.
    i. Ensure your phone's Bluetooth and Location settings are on, as well as the Latch App Bluetooth and location settings.

5. Check Power

a. Does the reader show signs of power (LEDs illuminate upon touching the lens)
b. If the reader is non-responsive follow the steps below to check the power.
    i. Whenever possible, every effort should be made for the Latch R to be powered alone, independent of other devices.
        1. The exception is in stand-alone situations where the third-party locking hardware relies on the power and relay from Latch R.
            a. It is critical that the combination of third-party hardware and reader does not overreach on power consumption.
    ii. Confirm voltage and wiring meet requirements:
        1. Confirm that the correct voltage and current are getting to the reader.
        2. Using a multimeter, check the wires coming from the power supply to determine the amount of voltage and current.
            a. Set the multimeter to VDC and place the red meter probe on the (red) positive reader wire and the black lead on the (black) negative reader wire.
            b. 12 - 24VDC should be displayed on the multimeter screen.
                i. R1 utilizes .25A @ 12VDC or .12A @ 24VDC
                ii. R2 utilizes .5A @12VDC or .25A @ 24VDC
        3. If there is no voltage at the reader, check the power supply.
            a. If the power supply is powered and there is no voltage being output, troubleshoot the power supply. The power supply may need to be replaced.

b. Verify the cable gauge meets standards.
   i. 22AWG up to 50’
   ii. 20AWG up to 200’
   iii. 18AWG up to 500’

iii. If proper voltage is confirmed at the connection to the reader, continue on to check polarity.

c. Polarity:
   i. Polarity in electrical terms refers to the positive or negative conductors within a DC circuit. Electrical polarity (positive and negative) is the direction of current flow in an electrical circuit.
      1. Using a multimeter, determine if the polarity from the power supply is correct
      2. Place the red meter lead on the red power wire and the black meter lead on the black power wire. If the polarity is reversed, a negative symbol will display in front of the voltage (example: - 12 VDC)
      3. If the polarity is incorrect, the reader will not power on.
      4. Positive needs to go to the red wire of the reader.
      5. Negative needs to go to the black wire of the reader.

6. Check for broken hardware / environmental impacts / third-party hardware

i. Check for overall damage to the device.
ii. Are there any signs of force or any noticeable scratches, cracks, or breakage?
iii. Testing the reader by itself / in isolation is the best way to rule out third-party hardware.
iv. Take the reader to the location of the power source, power it alone, and test the functionality.

7. Check Latch device functionality

i. Does the device unlock when access is attempted?
ii. Normal unlock sequence.
   1. (Bluetooth) The user opens the app and clicks unlock (or the app automatically starts to unlock through proximity once the lock is open) OR (NFC) a card is brought up to the lens OR (Doorcode) a code is input.

        2. The center LEDs light up and then the circle of LEDS opens clockwise.
        3. The user should hear a beep from the reader and the third-party locking hardware should unlock.
    iii. Check Device Configuration in the App
        1. Confirm Latch R has been activated
            a. Add a device.
            b. Assign or create a door.
            c. Set up the device.
            d. Test unlock/lock.
            e. Configure device settings in the app.
                i. Detailed steps can be found in this Activation Steps support link.
        2. If the relay onboard the Latch R is being used, confirm the relay is configured for the desired state.
            a. If the relay is not set up correctly it may be assumed it is not working or there is a problem with the device when there is not.
            b. The relay can be programmed to be normally closed (N.C.) or normally open (N.O.)
                i. A normally closed state provides a closed circuit that opens when activated.
                    1. This is the desired state when using electric strikes and maglocks providing a fail-safe (unlocked without power) scenario.
                ii. A normally open state provides an open circuit that closes when activated
                    1. This is the desired state when using electric strikes providing a fail secure (locked without power) scenario.
            c. Confirm relay is configured properly relative to the locking hardware.

8. Confirm Relay Changes State

    a. Confirm that the Door Schedule feature is not enabled and causes the relay to be in an undesired state.

b. Remove the reader from its mount and locate the relay wires (Reader Installation Guide) blue (COM) and yellow (NO/NC).
    i. Using a multimeter, perform a continuity check.
    ii. Place one meter probe on the blue wire and one on the yellow wire.
    iii. While the probes are connected, perform an unlock, this test function is used to check if voltage properly passes through the reader relay.
        1. This should change the relay from an OPEN state to a CLOSED state, assuming the relay is configured to be NORMALLY OPEN.
    iv. Depending on the multimeter, it will display a 0 and may beep if there is a conductive path between the two probe tips (meaning, the resistance is very close to zero). The meter will not make a noise or display OL (low value/open loop) if there is no conductive path.
        1. Alternatively, if your relay is configured to be NORMALLY CLOSED, the multimeter may beep as soon as you touch the leads to the Blue and Yellow wires and then become silent for several seconds when you perform the unlock. This is changing the relay from a CLOSED state to an OPEN state.
    v. In the event, that the relay is tested at the reader and it does NOT change states, the device should be RMAd - see RMA steps below
    vi. Relay power specs:
    vii. 1.5A @ 24V DC or 16V AC max

9. Power Cycle the Device

i. If all attempts to troubleshoot the device are unsuccessful, recycle power to the Latch R by removing power to the device for at least 60 seconds.
ii. Ideally, this power cycle would occur at the power supply but can be done at the reader itself by disconnecting the red and black wires.
iii. A power cycle could resolve some minor issues **NOTE: Anytime a unit is power cycled - either power is disconnected and/or batteries are removed or replaced - the unit must be updated using the Latch App (instead of the Latch Manager App) once it has rebooted.**

RMA Process

Overview

In order to replace a defective device, receive a replacement unit, and return the defective unit to our QA team for evaluation, an RMA will need to be submitted through our RMA process.

Process Overview

1. Contact Latch Support with RMA details:
    a. support@latch.com
    b. +1 (888) 808-0670
2. Required Details
    a. Device Serial
    b. Associated Property Name
    c. Associated Door Name
    d. Issue Description / Symptoms
    e. Troubleshooting Steps Attempted
    f. Shipping Address (for a new device)
    g. Shipping Contact Name
    h. Shipping Contact Email
    i. Shipping Contact Phone Number

Advanced Technical Support Guide

***NOTE:** If the below troubleshooting steps do not resolve your issue, please reach out to Support@latch.com and our Support Team will be happy to assist you.*

Input/Output (I/O) Troubleshooting

Symptoms

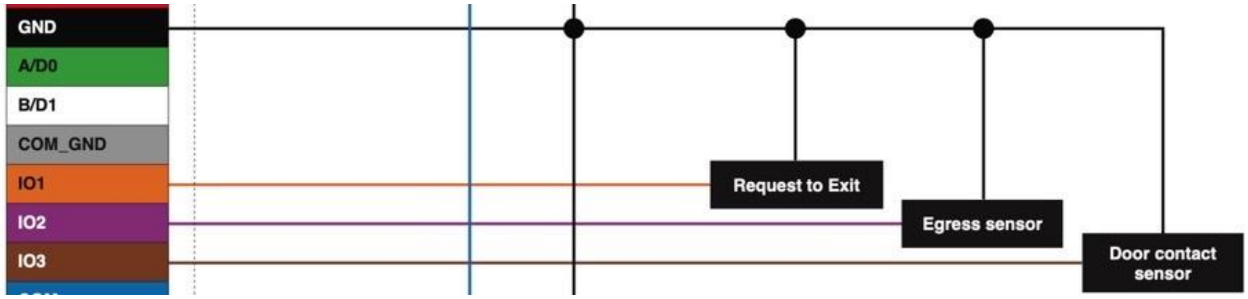
1. The device fails to properly and successfully Lock & Unlock
2. REX device not functioning as designed
3. Door monitoring is not functioning as designed

Input/Output Descriptions

- The Latch R has three configurable inputs/outputs, which can be connected to third-party hardware in the following settings:

1. IO1 Configuration States (for hardware that both senses and triggers unlock):
   - Unlock Only
   - Unlock + Egress Sensor
   - Disabled
   - IO1 can be configured as either Normally Open or Normally Closed
2. IO2 Configuration States(for hardware with only sensors):
   - Unlock Only
   - Egress Sensor

     Disabled
3. IO3 Configuration States
   - Unlock Only
   - Door Contact Sensor
   - Disabled
   - If IO3 is configured for a Door Contact Sensor, an automatic relock can be toggled on.



Troubleshooting I/O #1

- In the case of troubleshooting IOs and third-party hardware, there are many variables to be considered. Our primary goal is to determine that the Latch device is functioning as intended.

    NOTE: Termination resistors are not required when utilizing the I/Os on board the Latch R

- In the case that connected hardware is not functioning as intended and is connected to I/O #1:
    1. Confirm what the connected hardware is intended to do (unlock only, or unlock plus egress sensor).
    2. Confirm that the configuration in the Manager App matches what is needed on-site.
    3. Test the hardware with the opposite NO/NC configuration.
    4. Bypass the Latch reader, and attempt to test hardware removed from the Latch R.

Troubleshooting I/O #2

- In the case of troubleshooting IOs and third-party hardware, there are many variables to be considered. Our primary goal is to determine that the Latch device is functioning as intended.
- In the case that connected hardware is not functioning as intended and is connected to I/O #2:
    1. Confirm what the connected hardware is intended to do (Unlock or Egress Sensor)
    2. Confirm that the configuration in the Manager App matches what is needed

on-site.

3. Test the hardware with other configurations and note any changes.
4. Attempt to test hardware removed from the Latch R.

Troubleshooting I/O #3

- In the case of troubleshooting IOs and third-party hardware, there are many variables to be considered. Our primary goal is to determine that the Latch device is functioning as intended.
- In the case that connected hardware is not functioning as intended and is connected to I/O #3:
    1. Confirm what the connected hardware is intended to do (Unlock or Door Contact Sensor)
    2. Confirm that the configuration in the Manager App matches what is needed on-site.
    3. Test the hardware with other configurations and note any changes.
    4. Attempt to test hardware removed from the Latch R.

Weigand Troubleshooting

Symptoms

1. The device fails to properly and successfully lock & unlock.
2. Scanning a valid keycard does not yield a successful unlock.

Check Latch R Wiring & Configuration

1. Confirm Reader has been configured correctly
    a. Using the Manager App, navigate to the door you are working on.
    b. Select “Configure”
    c. Under “Relay Configuration,” select “Panel”
        i. This will enable the Wiegand capability.
2. Verify wiring configuration.
    a. First, confirm the reader terminations at the reader location, and then the access

control panel is both secure and correct.

i. See Latch R Install Guide

ii. Verify cables are connected to the Access Control panel - D1, D0, and Comm/Ground terminals, respectively.

3. If the issue persists, remove the reader and wire it directly to the reader port on the access control panel. If the problem is resolved then this points to possible wire damage.
    a. Check for any noticeable damage like skinned, broken, or cut wires
        i. Check continuity on each individual wire to confirm the wire is not broken
    b. Confirm wire specs: **(Shielded - Insulated)**
        i. 22AWG up to 50’
        ii. 20AWG up to 200’
        iii. 18AWG up to 500

Check Access Control Software & Hardware

1. Check access control software and hardware.
    a. Verify the panel has been configured for the correct Wiegand bit format.
        i. Does it support Wiegand 26-bit format?
    b. Confirm that the 3rd party access control panel has been programmed with the correct facility code.
        i. NOTE: The facility code is specific to the type of keycard being used.
2. Check Wiegand data wires.
    a. Confirm Wiegand data wires are terminated correctly at the access control panels reader connection.
        i. Green is DATA 0.
        ii. White is DATA 1.
        iii. Gray is ground.
            1. Ensure the communication ground is connected to the common ground terminal.
            2. DO NOT connect the reader's communication ground to the reader’s power ground.
            3. Connecting the communication ground to the reader power ground may result in Wiegand data garbling/interference.

Multimeter Testing

1. Check Power and Wiegand output
    a. Using a multimeter check the output voltage at the power output of the reader port for 12 VDC or 24 VDC, whichever is being used.
        i. This is the dedicated reader power.
    b. Wiegand communication
        i. When no data is being sent, both DATA 0 and DATA 1 are pulled up to the "high" voltage level, usually ~5 VDC.
        ii. Wiegand communication uses a binary code of 1’s and 0’s. When a 0 is sent the DATA 0 wire is pulled to a low voltage while the DATA1 wire stays at a high voltage. When a 1 is sent the DATA1 wire is pulled to a low voltage while DATA0 stays at a high voltage.
        iii. The range should be between 4.5 VDC and 5.5 VDC.
        iv. Below 4.5 VDC would indicate a problem. If reader power is adequate then the reader port may be bad. Resolving this would mean moving the reader to a working open reader port or replacing the access control hardware that contains that reader port.
    c. Using a meter, check VDC between DATA 0 and Wiegand ground and DATA 1 and Wiegand ground.
        i. ~5 VDC should be present on DATA 0 and DATA1.
    d. If these tests fail, unplug the reader from the panel reader port located on the access control panel and retest. At this point, with the reader unplugged, if the above tests fail, configure a known working panel reader port and see if this resolves the issue.
    e. If the above tests fail with no reader connected this will be likely due to a bad reader port.
        i. It may be that the access control panel/blade needs to be replaced if the reader port is bad.

Ethernet & WiFi Troubleshooting

Symptoms

1. Failure notification when configuring the device for the network.
2. Access is not getting synced over the network when added/removed.

3. Access and photo logs not getting uplinked over the network.

Note: Latch R device has a bandwidth requirement of 10/100 Mbps. Keep in mind that the network must have sufficient bandwidth to support all connected devices.

Ethernet / Wifi Configuration Timeout Troubleshooting

1. Confirm that the network configuration is correct.
    a. Open the Latch Manager App.
    b. Navigate to the door you are working on.
    c. Select "Configure".
    d. Verify Reader Network configuration aligns with property network infrastructure/configuration.
        i. i.e. WiFi or Ethernet.
2. Confirm the network device that you are trying to connect to is active.
    a. Ethernet switch / WiFi has power and is detectable from mobile devices.
3. If you are still experiencing issues with connectivity, please continue troubleshooting with the following slides.
4. Ensure *Spanning Tree Protocol* is disabled for the Ethernet switch (if managed) if not necessary.

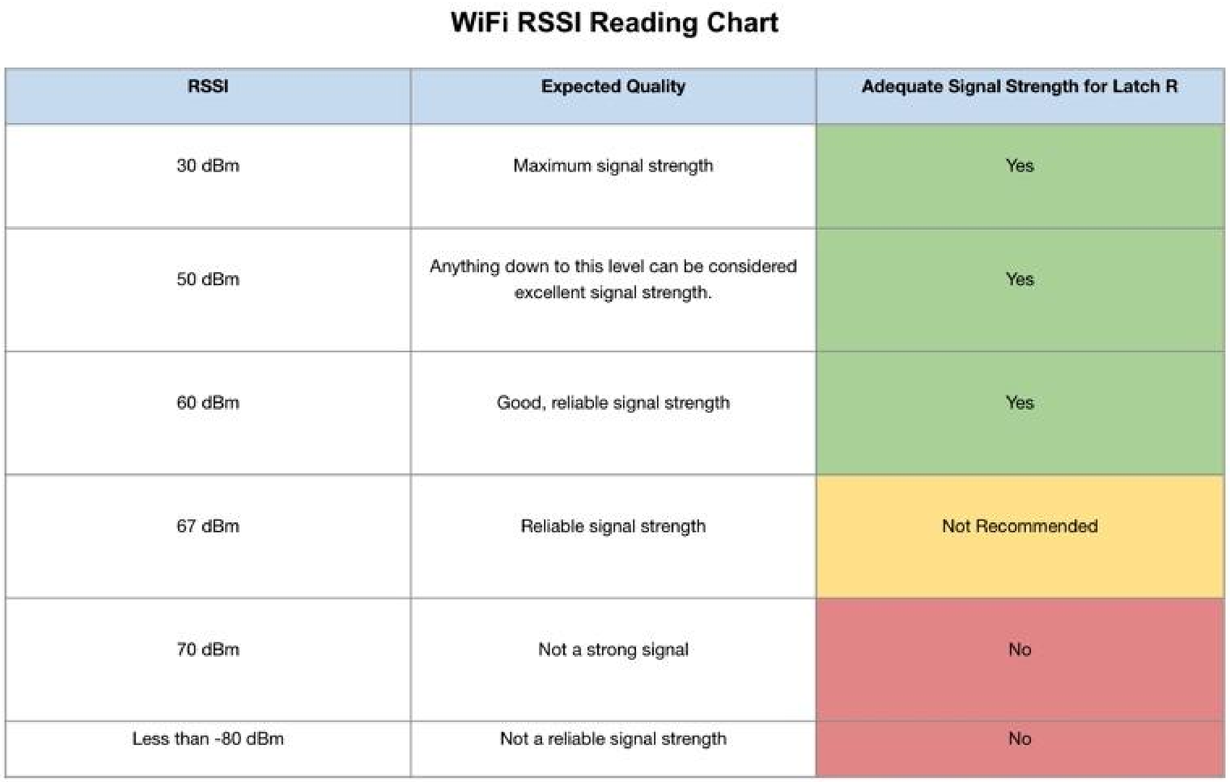
Troubleshooting WiFi Configuration

In any case, where saving a reader's network configuration results in a "Timeout" error and the device is connected via WiFi:

1. Confirm that the Reader is on the latest firmware version.
    a. In the Latch Manager app, navigate to the door.
    b. Select "Upgrade Firmware."
    c. Wait for the firmware upgrade to successfully completed.
2. Confirm that Reader has been configured for WiFi.
    a. In the Latch Manager app, navigate to the door.
    b. Select "Configure."
    c. Find "WiFi Settings."
    d. Under "WiFi Settings," confirm that the WiFi enabled switch is toggled ON (green)

3. Confirm the correct WiFi network password.
    a. Must be verified with on-site contact.
4. Confirm if the network is 2.4 GHz frequency.
    a. Must be verified with on-site contact.
    b. If possible, make the 2.4GHz connection isolated (i.e., not shared with 5GHz)
        i. Some APs use the same wireless settings for both bands.
    c. Ensure transmit power is the highest possible on the 2.4GHz band (i.e., set to 'maximum' or 'highest').
    d. If possible, ensure the 2.4GHz band is configured for ***only*** 802.11 b/g/n.
    e. If possible, determine the best channel (with minimal traffic) and isolate that channel for the 2.4GHz band.
        i. Typically, the best recommended channels for the 2.4GHz band are 1, 6, or 11.
        ii. Running a Wireless Diagnostics tool can help determine the best channel
            1. For Android, you can use the Wifi Analyzer app.
    f. Channel width for the 2.4GHz band should be set to 20 MHz (not 40 MHz).
5. Confirm Reader is within range of the WiFi network
    a. Download the Airport Utility app to your mobile device.
        i. This app allows you to see how close you are to the WiFi network you are trying to connect to.
        ii. Does not allow you to see the signal strength of the Reader.
    b. With the phone next to the Reader use the Airport Utility apps WiFi scan.
    c. The network the device is trying to connect to should populate in the scan with an RSSI reading.
        i. If the network you are trying to connect to does NOT populate in the scan, you are out of range or something is blocking the signal.
6. Traffic on port 8883 needs to be allowed.
7. Additional Troubleshooting Steps
    a. Disable AP roaming features (if any).

WiFi Signal Strength Chart



WiFi RSSI Reading Chart

RSSI	Expected Quality	Adequate Signal Strength for Latch R
30 dBm	Maximum signal strength	Yes
50 dBm	Anything down to this level can be considered excellent signal strength.	Yes
60 dBm	Good, reliable signal strength	Yes
67 dBm	Reliable signal strength	Not Recommended
70 dBm	Not a strong signal	No
Less than -80 dBm	Not a reliable signal strength	No

Troubleshooting Ethernet Configuration

In any case, where saving a reader’s network configuration results in a “Timeout” error and the device is connected via Ethernet:

1. Confirm the Reader has the latest firmware.
    a. In the Latch Manager App, navigate to the door.
    b. Select “Upgrade Firmware.”
    c. Wait for the firmware upgrade to successfully complete.
2. Confirm that Reader has been configured for ethernet.
    a. In the Latch Manager app, navigate to the door.
    b. Select “Configure.”

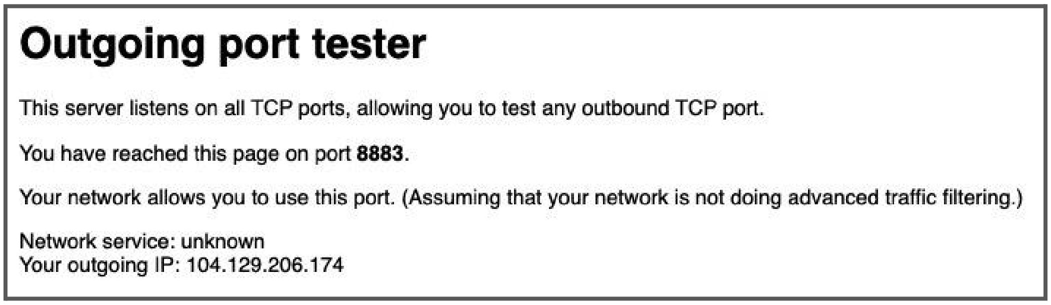
   c. Find “Ethernet Settings.”
   d. Under “Ethernet Settings,” confirm that the ‘Ethernet enabled’ switch is toggled ON (green).
3. Confirm the use of DHCP or Static IP Address
   a. This must be verified with on-site contact.
   b. IP Address: a unique string of numbers separated by periods that identifies each computer or device using the Internet Protocol to communicate over a network.
   c. Dynamic Host Configuration Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected.
   d. A Static IP address is an IP address that is manually configured into the device. This address does not change unless manually changed.
4. Check the ethernet cable.
   a. Confirm it is plugged in and the connection is secure.
   b. Check for any damage or hard bends in the cable.
5. Confirm network switch/router is working and configured.
   a. Does the router or switch have power?
   b. Traffic on port 8883 needs to be allowed.
      i. See the Port Filter/Blocked Test section below.
   c. Check that the port used for the Reader in the AP/router is configured for auto-negotiation.
6. If not necessary, disable STP/RSTP.

Port Filter/Blocked Test

- There are 2 options to determine if the AWS port that the Latch R uses is being filtered by the client's firewall:

1. Use the site: http://portquiz.net:8883/ if you are able to reach the page using the link that the port is not being filtered by the firewall. (*see photo*)
   a. Keep in mind:
      i. The firewall can still be blacklisting the AWS domain directly (use option 2 to confirm).
      ii. If you are not able to load the page the browser might be blocking non-standard web surfing ports.

        1. Try using a different browser or double-check with option 2.
2. Using the Nmap command to determine if the port is filtered or if the device can connect to the port.
    a. Use the following command:
        i. *nmap -p 8883 a2u1nmoy7g4pj2-ats.iot.us-east-2.amazonaws.com*
    b. The port should now show open.



Outgoing port tester

This server listens on all TCP ports, allowing you to test any outbound TCP port.

You have reached this page on port **8883**.

Your network allows you to use this port. (Assuming that your network is not doing advanced traffic filtering.)

Network service: unknown
Your outgoing IP: 104.129.206.174

FAQ

1. As of Firmware version 4.2.3, Latch R now supports 10/100 Half and Full-Duplex for Ethernet
    1. Prior to FW v4.2.3 Latch R only supported Half-Duplex for Ethernet
    2. Ethernet network switches/APs should have the associated port configured for auto-negotiation (default typically).
2. Why can't the lock (re)connect to WiFi/Eth?
    1. There are a number of reasons why reconnection fails. ***Most*** of the time it is due to poor signal strength from the AP; typically due to low power configured for the 2.4GHz band or because it is too far away.
3. Why can't I configure the lock for WiFi or Ethernet?
    1. This is usually due to a failing connection to the Network ***during*** the configuration process.
    2. The step that fails the most often is the LAN connection.
        i. Could be a bad/weak signal, bad cable, etc…
4. How does the lock handle reconnection? (How long does it retry, etc.)

1. We try to reconnect every 10 seconds for Ethernet and every 30 seconds for WiFi. After 20 minutes we piggyback a device reset on the next unlock. But we should still be actively trying to reconnect at those same intervals.

Elevator Floor Access (EFA)

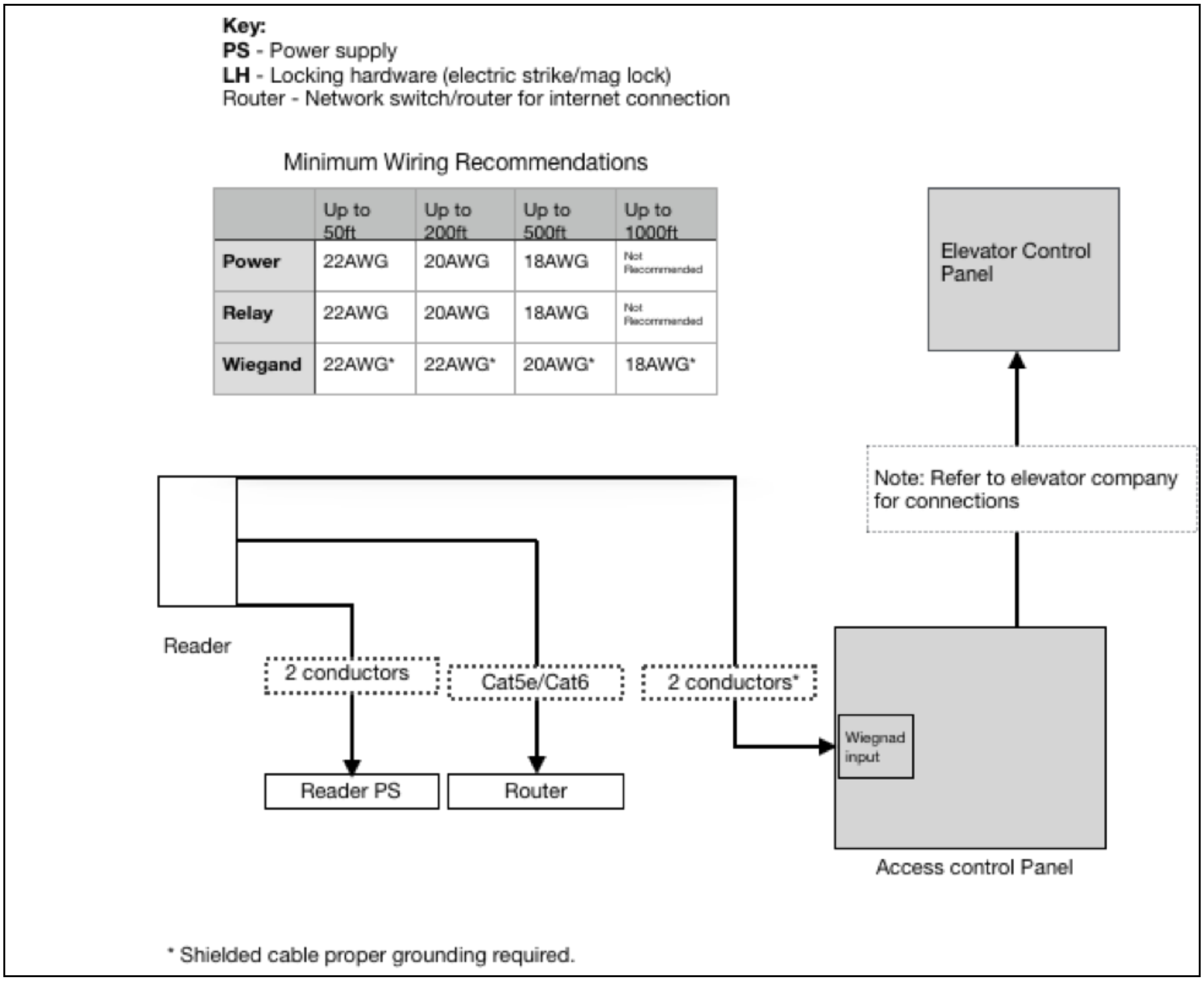
Before integrating an EFA system, please reach out to
Latch Support for assistance at support@latch.com.

EFA allows a credential to be required to reach certain floors, increasing security.

Requirements

- Floor Group Table: The Property Manager must work with Latch to set up floor access ahead of installation. Latch will then generate a Floor Group Table to be programmed into the access control panel being used for elevators. This will be displayed in the Manager App after the R is activated.
- Third-party access controller: The panel must be able to receive a 26-bit Wiegand credential. If the property requires scheduling or floors to be unlocked during certain hours, this needs to be supported by the access controller. The installer must be comfortable working with the access controller and it must be on Latch's approved list. For installers wishing to use access controllers not on this list Latch will minimally support the installation/configuration of the panel.
    - See the "Weigand Troubleshooting" section for additional information.
- **Internet:** Internet must be provided to the Rs. If an R is installed inside a cab, access to the internet must be provided via Ethernet through transceivers with a coax cable running in the traveling cable.

Wiring Requirements



Key:
PS - Power supply
LH - Locking hardware (electric strike/mag lock)
Router - Network switch/router for internet connection

Minimum Wiring Recommendations

	Up to 50ft	Up to 200ft	Up to 500ft	Up to 1000ft
Power	22AWG	20AWG	18AWG	Not Recommended
Relay	22AWG	20AWG	18AWG	Not Recommended
Wiegand	22AWG*	22AWG*	20AWG*	18AWG*

Note: Refer to elevator company for connections

* Shielded cable proper grounding required.

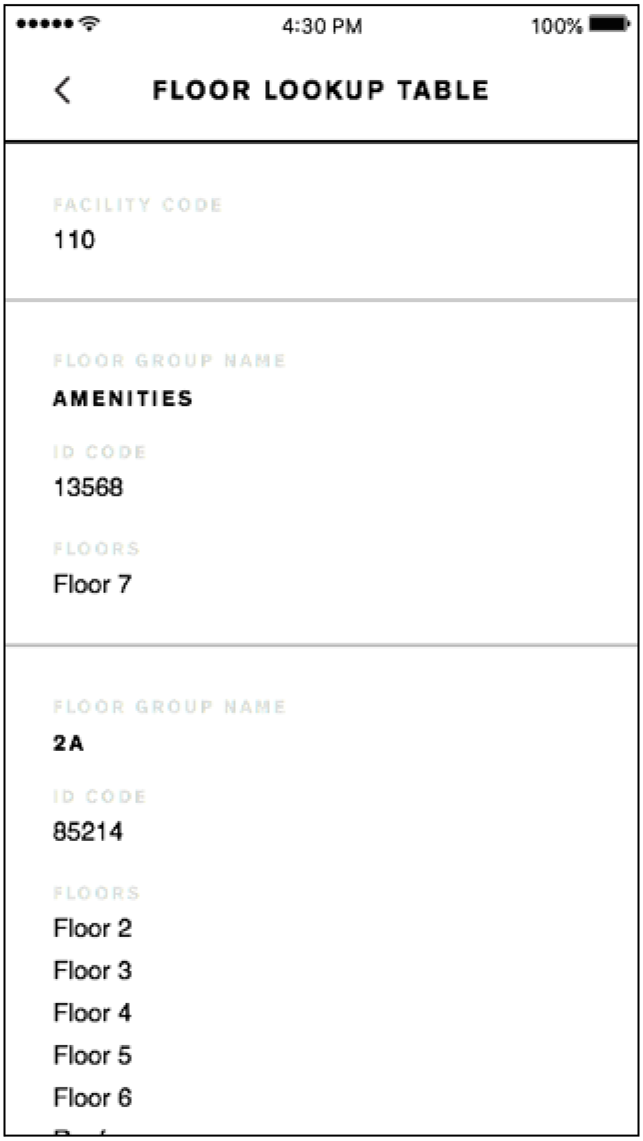
Programming the Latch R

- Activating the Latch R
  - During the activation process make sure to select FW Version 3.1x.xx
- Configuration
  - Internet is mandatory for all EFA installations.
  - Go to the Device Detail page after the activation process.
  - Go to the Settings page.
  - Configure Ethernet or WiFi.

  - Save changes.

Programming the Access Panel

- Floor Groups that mirror the Latch Cloud must be created in the panel. Refer to the Floor Lookup Table on the Device Detail page in the Manager App.
- The Floor Lookup Table contains the following:
  - Floor Group Name: This corresponds with the User Name field in most panels.
  - Facility Code and ID Code: Put together this is the Wiegand code.
  - Floors: The floors that belong to this Floor Group.



FLOOR LOOKUP TABLE

FACILITY CODE
110

FLOOR GROUP NAME
AMENITIES

ID CODE
13568

FLOORS
Floor 7

FLOOR GROUP NAME
2A

ID CODE
85214

FLOORS
Floor 2
Floor 3
Floor 4
Floor 5
Floor 6

Example of a Floor Lookup Table

Testing EFA

1. Prior to the day of installation, the Property Manager must create an account for each Floor Group, assign each account a different Floor Group, and give access to each of the accounts to the Integrator.
2. Before presenting a credential, test the elevator by making sure that all of the necessary floors are locked.
3. Present the credential for the first Floor Group.
   a. Confirm that all of the necessary floors are unlocked.
   b. Example: If the first Floor Group has access to floors 2 and 3, verify that floors 2 and 3 are unlocked.
4. Continue this process for each Floor Group, including the Daily Doorcode Floor Group.
5. After testing is complete, the Property Manager should delete each of the accounts created for testing.

Approved 3rd party access control system

Regular Dispatch
a. Brivo
   i. ACS6000
b. Keyscan
   i. EC1500
   ii. EC2500
c. Software House
   i. Istar Edge
   ii. Istar Ultra
   iii. Istar Pro

2. Destination Dispatch
   a. Braxos
      i. Schindler

Firmware Upgrade Troubleshooting

Symptoms

- During the Firmware Upgrade process on a Latch R device, you may receive a red error screen appearing on the Latch Manager app. This can happen either during the initial activation process or during a routine Firmware Upgrade after installation. This indicates that the firmware upgrade process failed.

Basic Firmware Upgrade Failure Troubleshooting

1. Delete the Latch Manager app from your mobile device, and re-download it to ensure you are on the latest version.
2. Power cycle iOS device (turn it off, wait for 30 seconds, restart the device).
3. Update the Device using the Latch App.
    a. Open the Latch App > My Doors > Select Door > Update > Press the “Update” button when close to the door/device.
    b. Detailed instructions for updating can be found in this Support Article.
4. Confirm the serial number from the device hardware.
5. While attempting the firmware upgrade, you should be physically within 3-6 feet of the device.
6. Confirm mobile device has sufficient cellular/WiFi network connectivity.
7. Firmware upgrades should be attempted at least 3 times.
8. If no success, continue on to additional troubleshooting.

Additional FW Updating Troubleshooting

1. Verify if I/O cables are shielded/tied if not in use. Grounded if in use
    a. Ungrounded/unshielded I/O cables can cause pick up erroneous voltage causing failures during FW upgrades.
2. Check if Lens and Home System are broadcasting
    a. Using the nRF connect app available through the app store, set the Max.RSSI filter to -40 dBm and allow it to scan.
    b. While scanning, be near the Latch device you’re scanning, the device should populate in the scan window.
    c. This nRF tool is helpful in collecting additional information that could lead to a more accurate diagnosis.
        i. Example: After replacing batteries the Lens is still unresponsive but the Home System is broadcasting indicating there IS power.