



SHELTER[™]
Cloud-Based Software User Guide

©2022 dormakaba USA Inc.
All rights reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of dormakaba USA Inc. The software described in this document is furnished under a license agreement or nondisclosure agreement.

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. Please call dormakaba USA Inc. at (317) 365-2407 if you see any errors or have any questions. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means electronic or mechanical, including photocopying, recording, information storage, and retrieval systems, for any purpose, without the express written permission of dormakaba USA Inc.

This document is distributed as is, without warranty of any kind, either express or implied, respecting the contents of this book, including but not limited to implied warranties for the publication's quality, performance, merchantability, or fitness for any particular purpose. Neither dormakaba USA Inc., nor its dealers or distributors shall be liable to the user or any other person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this publication.

BEST and SHELTER are some of the trademarks of dormakaba USA Inc.

A85383 Rev F Jan 2022

Table of Contents

1	Overview	
----------	-----------------	--

2	Getting Started	
	System setup and commissioning	2
	Gateway network setup	2
	Registering for a Shelter cloud-based software account	4
	Gateway account registration	4
	Token generation	4
	Registering with token	5
	Gateway licensing	5

3	Enrolling Gateway Devices	
	Enable gateway enrollment	6
	Enroll repeater	6
	Enroll lock	7
	Enroll fob	7
	Disable gateway enrollment.	7

4	Shelter Cloud-Based Software	
	Home	8
	Device management—viewing/modifying devices	8
	Gateway	9
	Locks	10
	Lock status.	11
	Repeaters	11

Fobs	12
Groups	13
Task scheduler.	14
Self-test	14
Transaction history	14
User management	15
Notification management	16
Help	17

5 Device Management

Gateway	18
Ports and connections	18
Power	18
Installation considerations	19
LEDs	20
Gateway web page	20
Offline mode option	23
Lock firmware updates	23
Lock	25
Mechanical operation.	25
Power and batteries	25
Tamper detection	26
LEDs and sounder	27
Factory reset	27
Enrollment	27
Configuration.	27
Site survey	27
Self-test	28

Table of Contents

Mechanical consideration	28
Fob	29
Buttons	29
Enrollment	29
Factory reset	29
Operation	29
LEDs	30
Testing	30
Battery	31
Repeater	31
Power	31
Installation considerations	32
Enrollment	32
Factory reset	33
Inputs	33
Outputs (relay boards)	34
Compatibility with other systems	34
<hr/>	
6 Installation Validation	
Verify enrollment	35
Verify firmware over the air upgrade	35
Performance notes	35
<hr/>	
7 Training/Testing/Use/Drills	
Notes and information	37
<hr/>	
8 Warranty	
Warranty information	38

1 Overview

Shelter is a wireless lockdown solution that consists of locks, fobs, gateways, and repeaters. The Shelter lock is designed to operate as a standard mechanical classroom function lock for daily use. In emergency situations, the Shelter lock can be wirelessly locked down and will behave as a storeroom function lock. Any key that can normally access the lock will be able to retract the latch. The Shelter lock always provides free egress. With the Shelter cloud-based software platform, you will be able to access the platform and customize it to the needs of your building and your security protocol.

The Shelter solution was not designed to serve as an overall electronic access control system to lock and unlock doors on a regular basis. dormakaba USA Inc. shall not be held liable for misuse of the Shelter solution.

2 Getting Started

System setup and commissioning

It is recommended that the locks, repeaters, and fobs are left unpowered until you are ready to set up your system. When ready to initially set up your system:

- Ensure your gateways and repeaters are properly placed to give optimum wireless coverage
- Ensure repeater mode is set correctly per your site plan—e.g., repeater or end node; see **Repeater Enrollment** section

Gateway network setup

An internet connection is required to set up and configure the Shelter solution. However, once the entire system is configured, an internet connection is not required to initiate or clear a lockdown. (See **Offline Mode Option** section.)

The gateway will obtain an IP address via DHCP or STATIC through the LAN port; however, you will need to connect the gateway locally to obtain the DHCP IP address or set the STATIC IP address.

For the gateway to be capable of a Shelter cloud-based connection, outbound ports 80 and 443 must be open allowing the gateway to communicate with the sites <https://networkedge-conductor.link-labs.com> and networkAsset-conductor.link-labs.com

- Connect public internet to ethernet LAN port of the gateway

- Connect a computer to the ethernet local port of the gateway
- Apply power to gateway
- Set computer IP address to access gateway: 192.168.3.1/255.255.255.0/192.168.3.3

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192.168.3.1

Subnet mask: 255.255.255.0

Default gateway: 192.168.3.3

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Validate settings upon exit

Advanced...

OK Cancel

- Navigate browser to the local gateway page <http://192.168.3.3>
- Login:
Gateway user name: **admin**

Gateway password: **password**

This password can be changed in the gateway administrator account settings.

Note: For security purposes, it is recommended to change the password upon first log in.

- Navigate to the bottom of the gateway main page to find the wired network DHCP IP address

- You can now connect the computer back to the area network and use the gateway DHCP wired network IP address—e.g., <http://10.149.24.51>
- Save this IP address to access the gateway web page later through the area network LAN connection
- IP address: _____._____._____._____
- In the future, this IP address can be obtained from the Shelter cloud-based software if it should change
- To set a static IP, change the IP address configuration method to static and fill in the static IP fields from your network administration; when complete, press submit

Note: The gateway will communicate directly to the cloud through the internet. The ports 80 and 443 will need bi-directional communication to the following locations:

Port - 80,443 – Conductor Connections

- access-conductor.link-labs.com
- ec2-54-164-136-215.compute-1.amazonaws.com (54.164.136.215)
- ec2-54-236-81-98.compute-1.amazonaws.com (54.236.81.98)
- networkasset-conductor.link-labs.com
- ec2-52-86-79-116.compute-1.amazonaws.com (52.86.79.116)
- ec2-54-209-121-112.compute-1.amazonaws.com (54.209.121.112)
- clientedge-conductor.link-labs.com
- ec2-54-209-158-182.compute-1.amazonaws.com (54.209.158.182)
- ec2-54-174-117-67.compute-1.amazonaws.com (54.174.117.67)
- conductor.link-labs.com
- ec2-52-45-219-168.compute-1.amazonaws.com (52.45.219.168)
- ec2-54-156-206-13.compute-1.amazonaws.com (54.156.206.13)
- ec2-54-173-84-2.compute-1.amazonaws.com (54.173.84.2)
- ec2-52-86-190-186.compute-1.amazonaws.com (52.86.190.186)

Ports – 80,443 – Salt Connection

- 52.41.145.100
- ec2-52-41-145-100.us-west-2.compute.amazonaws.com (52.41.145.100)
- ec2-52-41-145-100.us-west-2.compute.amazonaws.com (52.41.145.100)
- *Don't forget exceptions in Web Filters

Port – 443 – Data Transfer

- link-labs.com
- 104.25.56.116 (104.25.56.116)

Ports – 80 Pu

- a2-17-42-64.deploy.static.akamaitechnologies.com (2.17.42.64)
- a2-17-42-83.deploy.static.akamaitechnologies.com (2.17.42.83)

Registering for a Shelter cloud-based software account

Visit <http://www.shelter.bestaccess.com> to register/create a Shelter cloud-based software account.

Note: If the gateway is desired to be kept off the internet. (See **Offline Mode Option** section.)

BEST SHELTER
SIMPLY SECURING SAFE SPACES

[Register/Create an Account](#)

Username [Forgot Username](#)

Password [Forgot Password](#)

Submit

Follow the directions as prompted by the website. You will be asked to provide: name, address, email address, and other basic information. This information should correspond to the person you wish to be your system administrator. The administrator can create additional users after registration. These users are for accessing Shelter cloud-based software, not users who are assigned fobs.

Create a User Account

Your account details

Company

Email

First Name

Username

Choose Password

Verify Email

Last Name

Re-enter Password

A strong password must be used. The password must be at least 8 characters long, contain (1) number, (1) uppercase, (1) lowercase letter, and (1) special character.

Password Hint

Facility Name

Street Address

City

Zip/Postal Code

School District

State

Terms & Conditions

Please check this box to confirm your agreement to the terms and conditions, privacy policy and refund policies.

Sign up Progress

Account details

Terms & Conditions, privacy and return

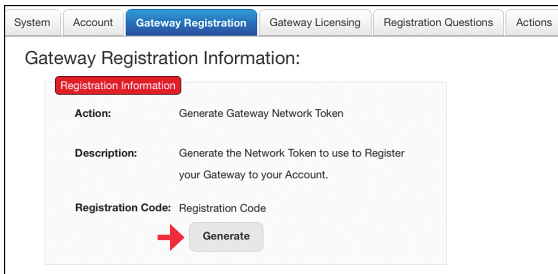
After you have registered, you should receive an email to the email address you provided during registration with the link to your organization's landing page. Please keep a copy of this link in your files or browser. Enter the username and password you created during registration.

Gateway account registration

A registration token is required prior to registering your account.

Token generation

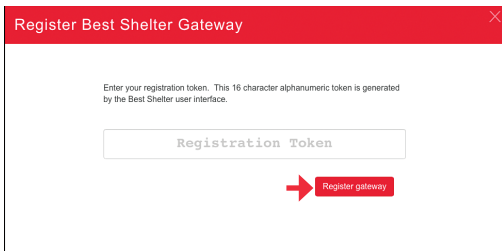
- Follow the new link in the email you have received to log in to the Shelter cloud-based software
- On the home page, navigate to the **Gateway Registration** tab



- Press the **Generate** button to create the network token to use to register your gateway to your account
- A token should be generated for each gateway that will be registered into the Shelter solution gateway account
- Copy this token to your clipboard

Registering with token

- Navigate to the gateway DHCP or static wired network IP address
- Use the IP address recorded earlier under gateway network setup



- Paste token and select **Register Gateway** button
- Wait about one minute and verify that the registration status reads, 'Registered'



Once devices are enrolled, which is explained in the next section, the gateway should not be re-registered or the devices will need to be re-enrolled.

Gateway licensing

Should a Customer desire to continue to use the services after the one year free trial period, the Customer will be required to purchase a Shelter gateway cloud-based subscription service from a dormakaba USA Inc. authorized reseller. (See the Shelter cloud-based service subscription agreement under help.)

Email warnings about license expiration will be sent to the site administrator as well as pop-ups upon login to the Shelter cloud-based software. These warnings will start as early as three months prior to gateway license expiration dates. For reference, these dates can always be found on the home page under the **Gateway Licensing** tab.

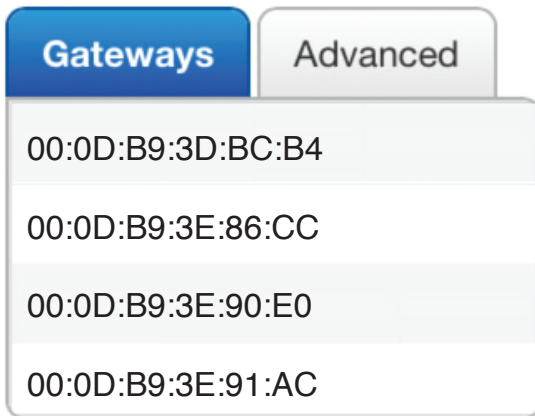
Name	Address	Registration Time	License Expiration Date	License Suspension Date	License Status
Middle School	\$10190-0-0b7773077	2/1/2018 9:33:27 AM EST	2/1/2019 9:33:27 AM EST	1/1/2018 9:33:27 AM EST	Suspended
Elementary School	\$10190-0-0b1111c11	5/1/2018 9:33:27 AM EDT	5/1/2019 9:33:27 AM EDT	4/1/2018 9:33:27 AM EDT	Expired
High School	\$10190-0-0b2222c22	5/1/2019 9:33:27 AM EDT	5/1/2019 9:33:27 AM EDT	4/1/2019 9:33:27 AM EDT	Valid
Administrative Building	\$10190-0-0b3333c33	5/4/2019 1:53:18 PM EDT	5/4/2018 1:53:18 PM EDT	4/4/2019 1:53:18 PM EDT	Valid

3 Enrolling Gateway Devices

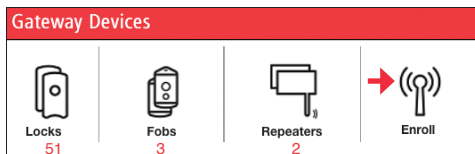
Enable gateway enrollment

From the home page, www.shelter.bestaccess.com, double-click on the gateway. The gateway MAC can be found on the top of the gateway web page.

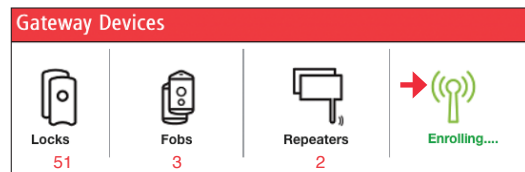
Note: A public internet connection is required for the gateway to enroll devices. (See **Offline Mode Option** section.)



- Click on the enroll icon



- The enroll icon will switch to 'green' enrolling for two hours unless the enroll icon is clicked again

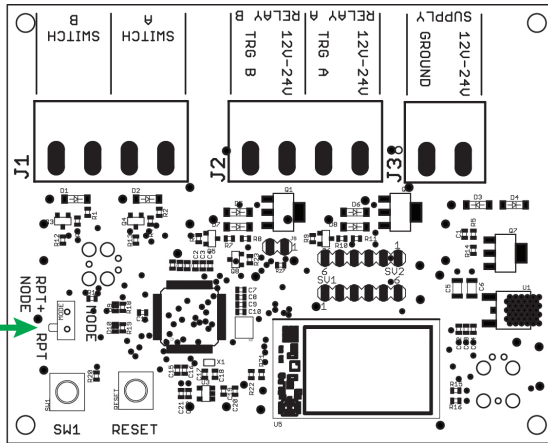


- Repeaters must be enrolled before locks
- It is recommended that a site map is used to note the locations where devices are installed; this will allow friendly names to be added later after enrollment is successful; a map is also very important for troubleshooting
- Multiple devices can be enrolled while enrollment is enabled; however, it is recommended that the Shelter cloud-based software is periodically checked to confirm devices are enrolling successfully
- If enrollment is failing, reference the **Site Survey** section under **Lock Device Management** to confirm signal strength is adequate

Note: No more than three devices can be enrolled at the same time.


Enroll repeater


- Enroll repeaters first in your system
- Place mode switch to correct position
- Ensure repeater mode is set correctly per your site plan





- Power repeater
- Navigate to the **Device** tabs in the lower left-hand corner of that gateway's details page

Gateway Devices


Locks
51


Fobs
3


Repeaters
2


Enrolling...

→

Locks

Fobs

Repeaters

Refresh

	Timestamp	Message Type
1932 -17	4/27/2019 3:10:27 PM EDT	
1939 - Office - Conf	4/27/2019 3:21:45 PM EDT	
193D - 22 - 5th Grade	4/27/2019 3:22:09 PM EDT	

- Confirm new repeater MAC is in the device list

Enroll lock

- Insert batteries and install directly onto door mounting bracket before the LED sequence ends
- Navigate to the **Device** tabs in the lower left-hand corner of that gateway's details page
- Confirm new lock MAC is in the device list

Note: Locks may not enroll if they are less than 10 feet from a gateway or repeater antenna.

If locks must be placed within 10 feet of a gateway or repeater antenna, enroll the lock outside this range first and then place on the door.

Enroll fob

- Insert batteries into fob
- Navigate to the **Device** tabs in the lower left-hand corner of that gateway's details page
- Confirm new fob MAC is in the device list

Disable gateway enrollment

- Click on the 'green' enroll icon
- Enroll icon will switch back to 'black' enroll state

4 Shelter Cloud-Based Software

Home

Upon logging into the Shelter cloud-based software, you'll see the Shelter dashboard with account details organized in tabs across the top and system configuration controls along the left. Through these tabs and controls, you can easily configure and modify the system to meet your needs. You can manage devices, device groups, and users.

Note: If the gateway is desired to be kept off the internet, please see **Offline Mode Option** section.

Devices include gateways, locks, repeaters, and fobs—the physical components that comprise the security network in your facility. Users are those who have been provided access to the software in order to modify the configuration, initiate all-clear after a lockdown event, or manage event data captured in the dashboard, like audit trails or notifications.

On the dashboard, you'll notice a map with icons on it. The icons represent the gateways installed throughout your facility or multiple locations. Click on any icon to see the gateway's MAC address, facility name, and the active devices configured to respond to it.

You can also find all of the gateways enrolled in your system by referencing the table below the map. When you click on a gateway, you'll see the most recent activity for the gateway.

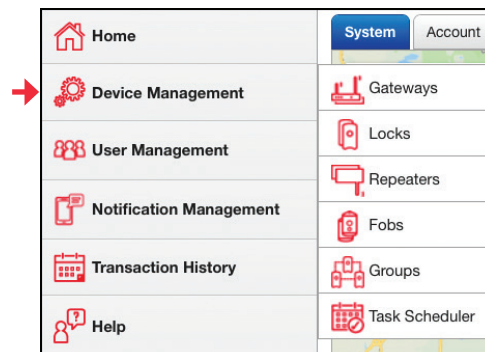
Device management—viewing/modifying devices

Device Management allows you to view and modify the following Shelter devices:

- Gateways
- Locks
- Repeaters
- Fobs

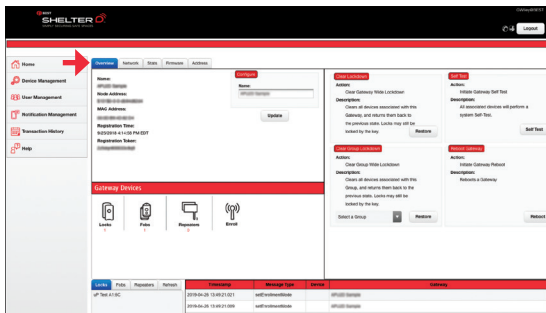
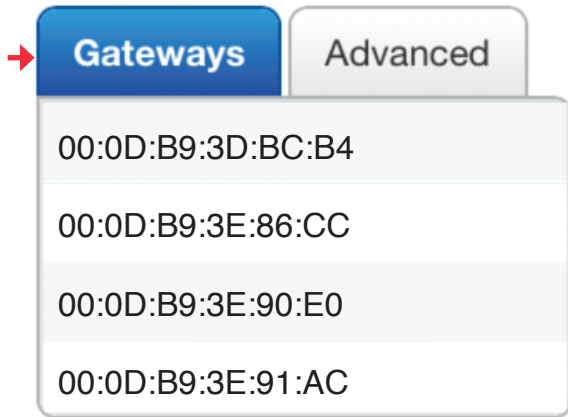
Shelter devices can be renamed under the **Configuration** tab.

Also under **Device Management**, you can configure and customize door groups and schedule tasks.



Gateway

From the **Gateways** tab, found in the lower left corner, you can 'double-click' the gateway you wish to view or modify.



Information under the main **Overview** tab includes:

- Name – 'friendly' name assigned to gateway
- MAC address
- Registration time – date/time gateway registered
- Downlink channel – current gateway channel
- Registration token
- Number of locks enrolled in the gateway

- Number of fobs enrolled in the gateway
- Number of repeaters enrolled in the gateway

Actions under the **Overview** tab include:

- Self-test – manually execute self-test for all associated devices
- Clear lockdown – for all associated devices
- Clear group lockdown – clearing by selected group
- Reboot gateway – initiate a software reboot of the Shelter gateway
- Lock icon – click to navigate to lock page for only this gateway
- Fob icon – click to navigate to fob page for only this gateway
- Repeater icon – click to navigate to repeater page for only this gateway
- Enrollment icon – click to engage enrollment

Information under the **Network** tab includes:

- IP address
- Connection: type

Information under the **Stats** tab includes:

- Advanced information

Information under the **Firmware** tab includes:

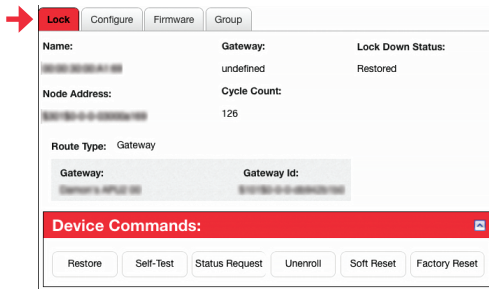
- Firmware packages installed on the gateway

Information under the **Address** tab includes:

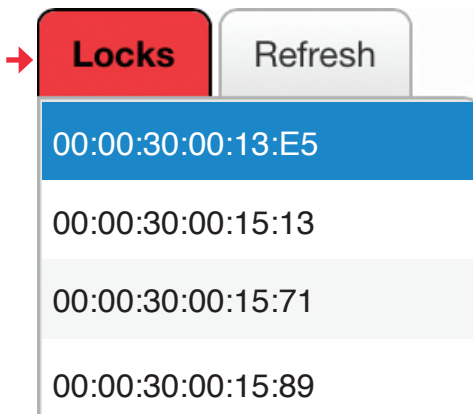
- Physical address where the gateway is located that will update the map

Locks

From the **Locks** tab, found in the upper left corner in **Device Management**, you can navigate to the lock page. This will show all locks in the organization.



From here, you can select the lock you wish to view or modify in the **Locks** tab found in the lower left corner.



Information under the main **Locks** tab includes:

- Name – 'friendly' name assigned to lock
- Lockdown status – lock/unlock state
- Last lockdown time – last time a lockdown was executed
- Gateway – current gateway controlling lock

- Enrollment time – first time lock enrolled into system
- Last modified – last time lock configuration changed
- Cycle count – number of times lock motor has run
- Route type
- Route name

Configuration options include:

- Sounder – enable/disable
- LED – enable/disable
- Lock name – where you can assign a 'friendly' name to the lock
- Status update interval – time between status messages

Note: A more frequent status rate will result in a reduction in lock battery life. Also, configuration changes will not take effect until the lock reports its next status.

Additional information includes:

- Battery strength – percentage of battery remaining
- Battery life – estimated days of battery life
- Signal strength – RSSI communication value
- Connected to – route of communication
- Last self-test result – pass/fail result
- Last self-test time – time of last self-test
- Most recent transaction, if any

Actions under the **Locks** tab include:

- Restore – clear lockdown
- Self-test – manually execute self-test
- Factory reset – manually execute factory reset
- Un-enroll – removes lock from system
- Status request – will request a status message from the individual lock

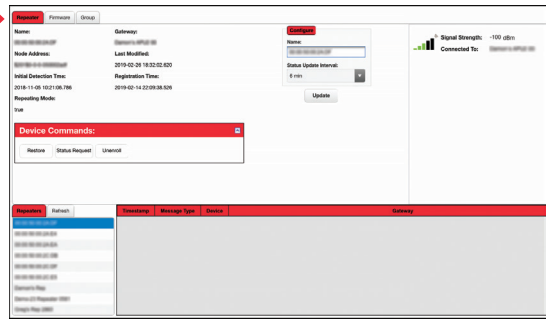
- Soft reset – will reset the firmware running in the lock →

Information under the **Firmware** tab includes:

- Firmware packages installed on the lock

Information under the **Groups** tab includes:

- Group assignments that control the lock



Lock Status

From the **Locks** tab, found in the upper left corner in device management, selecting the **Status** tab rather the **Locks** tab will display all lock statuses on one page.

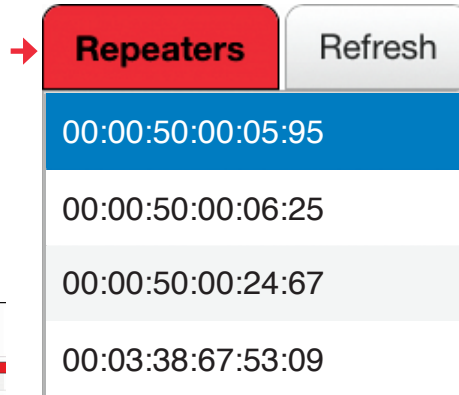
Information includes:

- Additional information also found on lock page

Actions include:

- Downloading the page information
- Printing the page
- Refreshing the page

From here, you can select the repeater you wish to view or modify in the **Repeaters** tab found in the lower left corner.



Lock Status
Displays the battery and signal strength status of all locks within your organization.
NOTE: This signal strength status updates are dependent upon each individual lock's update interval.

Device Name	Lockdown Status	Battery Voltage	Battery Voltage	Signal Strength	Signal Strength	Last Status Time	Gateway	Action
A-7 1083 Marlin	Reasoned	3.02		-99		November 13, 2018 9:04:16 PM EST	Danora's APUS 00	Gateway
00 00 00 00 A1 04	Reasoned	3.51		-82		April 26, 2019 1:04:30 PM EDT	Danora's APUS 00	Gateway
C10 1489 Marlin	Reasoned	4.85		-64		April 26, 2019 1:04:48 PM EDT	Danora's APUS 00	Gateway
B15 1412 Marlin	Reasoned	4.89		-62		April 26, 2019 1:05:14 PM EDT	Danora's APUS 00	Gateway
02 1063 11	Reasoned	4.89		-99		April 11, 2019 2:40:27 PM EDT	undefined	Gateway
A8 1086	Reasoned	4.82		-65		April 26, 2019 11:11:42 AM EDT	Danora's APUS 00	Gateway
C-15 1485 Marlin	Reasoned	4.92		-47		April 26, 2019 12:03:44 AM EDT	Danora's APUS 00	Gateway
A11 1074 Marlin	Reasoned	4.93		-67		April 26, 2019 12:47:02 PM EDT	Danora's APUS 00	Gateway
C17 1479	Reasoned	4.94		-77		April 26, 2019 9:25:40 AM EDT	Danora's APUS 00	Gateway
C-16 1476 Marlin	Reasoned	4.94		-64		April 26, 2019 9:28:58 AM EDT	Danora's APUS 00	Gateway
Rep C5 1461	Reasoned	4.97		-99		October 5, 2018 10:04:23 AM EDT	Danora's APUS 00	Gateway
B-3 1068	Reasoned	4.99		-66		April 26, 2019 8:03:48 AM EDT	Danora's APUS 00	Gateway
B10 1164	Reasoned	5.00		-89		April 26, 2019 1:04:38 PM EDT	Danora's APUS 00	Gateway

Repeaters

From the **Repeaters** tab, found in the upper left corner in **Device Management**, you can navigate to the repeater page. This will show all repeaters in the organization.

Information under the main **Repeaters** tab includes:

- Name – 'friendly' name assigned to repeater
- Registration time – date/time repeater registered
- Gateway – current gateway repeater is enrolled to
- Last modified – last time repeater configuration changed
- Downlink channel – current repeater channel
- Initial detection time – time of first detection

- Repeating mode – true for repeating, false for end node only mode
- Lockdown status – lock/unlock state

Configuration options include:

- Repeater name – where you can assign a 'friendly' name to the repeater
- Status update interval – time between status messages

Additional information includes:

- Signal strength – RSSI communication value
- Most recent transaction, if any
- Connected to – gateway repeater is connected to

Actions under the **Repeaters** tab include:

- Restore – clear lockdown
- Status request – will request a status message from the individual repeater
- Un-enroll – removes repeater from the system

Information under the **Firmware** tab includes:

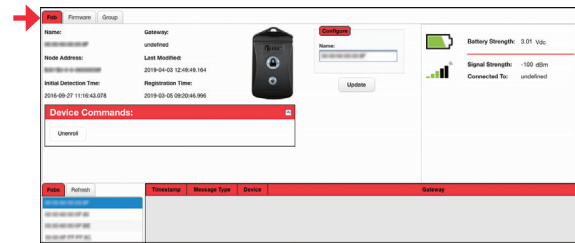
- Firmware packages installed on the repeater

Information under the **Groups** tab includes:

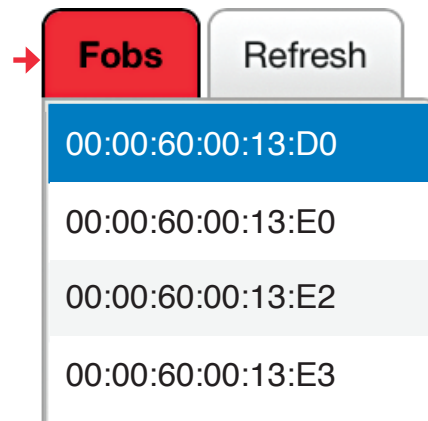
- Group assignments for the repeater

Fobs

From the **Fobs** tab, found in the upper left corner in **Device Management**, you can navigate to the fob page. This will show all fobs in the organization.



From here, you can select the fob you wish to view or modify in the **Fobs** tab found in the lower left corner.



Information under the main **Fobs** tab includes:

- Name – 'friendly' name assigned to fob
- Registration time – date/time fob registered
- Gateway – current gateway fob connected to
- Last modified – last time fob configuration changed

Configuration options include:

- Button statistics – number of button presses since last battery change
- Fob name – where you can assign a 'friendly' name to the fob

Additional information includes:

- Battery strength – percentage of battery remaining
- Most recent transaction, if any

Information under the **Firmware** tab includes:

- Firmware package installed on the fob

Information under the **Groups** tab includes:

- Group assignments for the fob

Actions under the **Fobs** tab include:

- Un-enroll – removes fob from the system

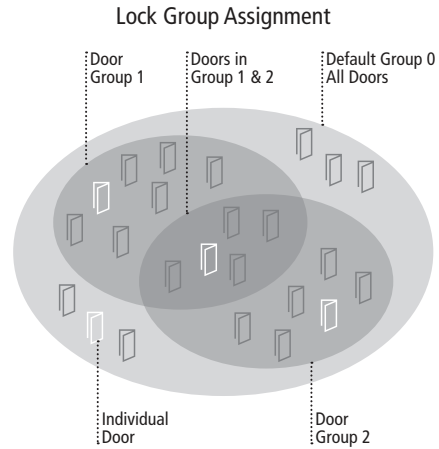
Groups

Groups or door groups are created to separate sections of the building to be controlled by fobs or repeater inputs. Doors can be assigned to multiple groups if more than one fob or repeater output needs to control that door. Groups can be assigned 'friendly' names like 'Building A North' to easily identify in the system.

- Locks and repeater output relays can belong to door groups; they can belong to multiple door groups
- All locks and repeaters belong to default group 0
- Fobs and repeater switch inputs can control door groups or individual devices; each fob or switch input can only control a single door group or individual device
- Door groups can be controlled by as many fobs or switch inputs as are in the system
- Default door group 0 can be controlled by fobs a, b, c, d, etc.

Note: Group assignments for locks will not take effect until after the next lock status communication occurs.

Note: Fobs and repeaters by default do not control any groups.



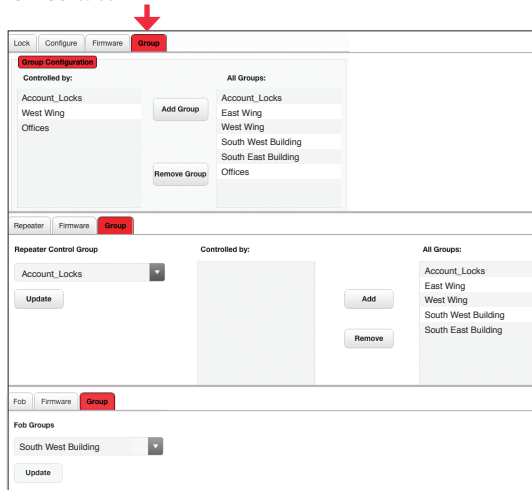
Groups can be added, modified, or deleted on the **Groups** tab. Groups are assigned to individual gateways and devices enrolled into gateways—64 max per gateway.

➔ **Groups**

GatewayName	GroupId	GroupName
\$101\$0-0-0-db93e9600	0	Account_Locks
\$101\$0-0-0-db93e9600	1	East Wing
\$101\$0-0-0-db93e9600	2	West Wing
\$101\$0-0-0-db93e9600	3	South West Building
\$101\$0-0-0-db93e9600	4	South East Building
\$101\$0-0-0-db93e9600	5	Offices

On

Group assignments can be made on the individual **Device** tabs.



Task scheduler

You can use **Task Scheduler** to create and manage self-tests that your system will carry out automatically at the times you specify.

Self-test

Under **Device Management**, select task scheduler to create a task. Options under **Task Scheduler** include:

- Create task
- Modify task
- Delete task

When creating a task, you will need to provide task information and schedule information.

- Choose a gateway from the drop-down list that you want to execute task.

- Under **Advanced Settings**, check enabled to enable the task.

Transaction history

Transaction History displays historical transaction events from the system devices from a time period selected.

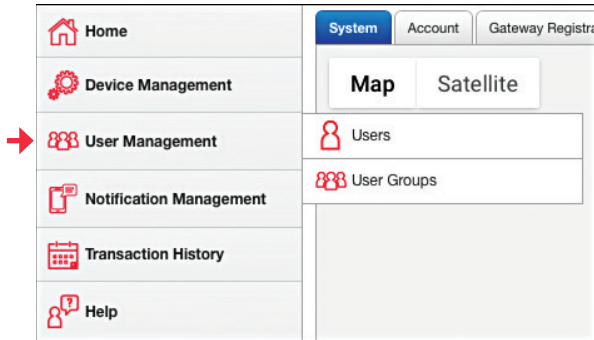
Under **Transactions**, you will need to provide the max number of records you want to retrieve, the start/end time, and choose the gateway from the drop-down list.

You can also print or export the results that are returned.

User management

Options under **User Management** include:

- Users
- User groups



Under **Users**, you can add users to the system—maximum of five—that need access to the Shelter cloud-based software. Options under **Users** include:

- Add
- Modify
- Delete

Username	Full Name	Description	Status	Last Login
bestsupport	Best Support	dormakaba	✓	1969-12-31 19:00:00.000

Add Modify Delete Total User Count: 1

When adding a user, you will need to first select a user group and then provide security information and address information.

Under **User Groups**, you can specify which group the user belongs to.

Options under **User Groups** include:

- Administrator user groups
- Standard user group

Administrator User Groups can perform any action in the Shelter cloud-based software including device actions, user management, notification management, etc.

Standard user groups only have viewing capability and cannot modify any settings in the system.

Notification management

Notification Management allows you to specify which users and what types of notification messages are received.

Settings include:

- Name the group
- Select a notification event

To create a notification group, add a name to the group and enter either a phone number or email address for that name. Continue to add multiple names to the group, and then select the notification events for that group. Check the **Enabled** box to enable the group and press create.

Notification Management
New Notification Group Information

Name: Battery Notification Group
Created By: marketing_01
Description: Notify of Low Battery on device

User Notification Addresses

Name	Email	Phone

Name:
 Email Address Phone Numbers

Notification Events

Fob Notifications:
 Critical Battery
 Lockdown Button Pressed
 Self Test Button Pressed

Lock Notifications:
 Critical Battery
 Lockdown Event
 Lockdown Hardware Failure
 Self Test Failure
 Tamper Activated
 Tamper Deactivated
 Communication Offline

Gateway Notifications:
 Communication Offline

Repeater Notifications:
 Lockdown Event
 Lockdown Switch Activated
 Lockdown Restore Switch Activated
 Communication Offline

Enabled

Notification Groups		
Name	Description	Enabled
Fob & Repeater and Notification Group	All Event Notification Group	<input checked="" type="checkbox"/>
Lock Notification Group	All Event Notification Group	<input type="checkbox"/>
Gateway Group	All Event Notification Group	<input checked="" type="checkbox"/>
Maintenance Group	All Event Notification Group	<input checked="" type="checkbox"/>

Total Notification Group Count: 4

Fob notifications

- Critical battery – indicates the fob's battery needs to be replaced
- **Lockdown** button pressed – indicates the fob that signaled a lockdown event
- **Self-Test** button pressed – indicates the fob that self-tested using the **Self-Test** button

Lock notifications

- Critical battery – indicates the lock batteries need to be replaced; lock will lock down at critical battery
- Lockdown event – indicates the system had a lockdown event and suggests checking status of all devices
- Lockdown hardware failure – indicates the lock has a motor abnormality
- Self-test failure – indicates the lock has failed self-test and should be checked for its indicated failure
- Tamper activated – indicates a tamper event and the lock should be checked
- Tamper deactivated – indicates tamper event has been resolved
- Communication offline – indicates the lock has not sent status for over 40 hours; lock should be checked

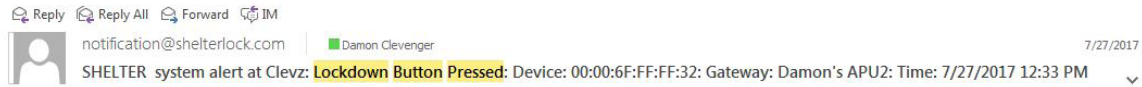
Gateway notifications

- Communication offline – indicates the gateway has not sent status in 25 minutes; system should be checked

Repeater notifications

- Lockdown event – indicates the system had a lockdown event and suggests checking status of all devices
- Lockdown switch activated – indicates the repeater has activated lockdown via its switch
- Lockdown restored switch activated – indicates the repeater has activated restore via its switch
- Communication offline – indicates the repeater has not sent status in one hour; system should be checked

Notification example – **Lockdown** button pressed:



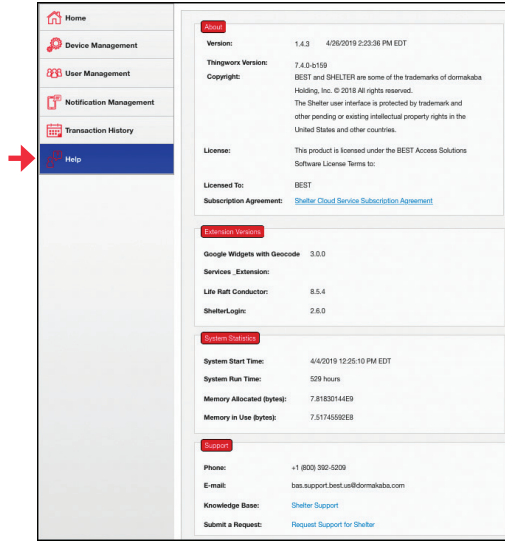
SHELTER system alert at Clevz: **Lockdown Button Pressed**: Device: 00:00:6F:FF:FF:32: Gateway: Damon's APU2: Time: 7/27/2017 12:33 PM

Clevz - company/organization

Lockdown button pressed - 00:00:6F:FF:FF:32 (Name of the fob—this fob was not assigned a friendly name so the default MAC address is used.) This notification informs the user of the fob that signaled the lockdown.

Help

Support information can be found under the **Help** button.



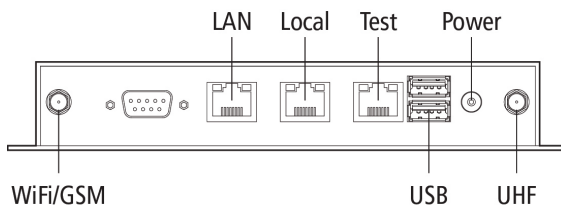
Gateway: device - Damon's APU2 (Portal gateway name is helpful if you have multiple portals or facilities in the same organization.)

5 Device Management

Gateway

The gateway is the center of the communication system for the Shelter solution. This is the component that is registered with and provides information to the Shelter cloud-based software via the internet. The gateway is on a 900MHz platform giving our system very reliable, long-range connectivity.

Ports and connections



- WiFi/GSM – reserved for future antenna connections
- LAN – DHCP or static network connection
- Local – local 192.168.3.3 network connection
- Test – reserved for future use
- USB – reserved for future use
- Power – 12VDC 2A minimum supply (2.5mm ID, 5.5mm OD plug)
- UHF – 900MHz device communication antenna connection; do not power the gateway without attaching this antenna

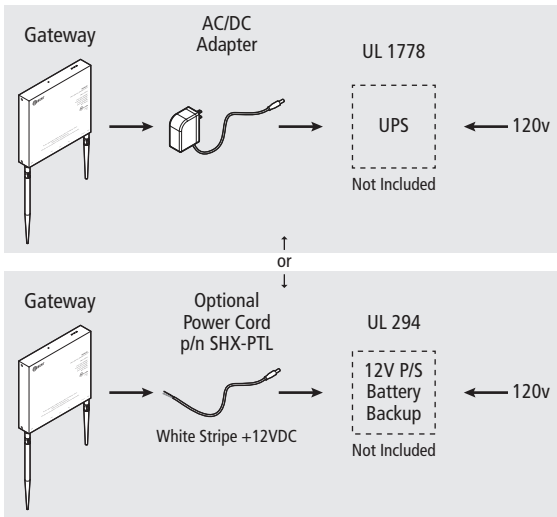
Power

Connect to 12VDC 2A minimum power supply.

Power connection options:

- Connection with included AC/DC power adapter where power adapter is plugged into an uninterrupted power supply; it is recommended to use UPS - UL 1778 power supply
- The Shelter solution relies upon the gateway and repeater components to be hard-wired to a power supply in order to receive a signal from the fob and transmit the signal to the Shelter lock or for the repeater relays to function properly
- It is strongly recommended that the gateway and repeater have a battery backup in place
- In the event of a power loss at the gateway or repeater, the Shelter solution may not function properly
- Connection with optional power pigtail (p/n SHX-PTL) to a power supply that contains a battery backup; it is recommended to use a UL 294 certified power supply

Note: Maximum recommended wire run is 200 ft with 18AWG wire.

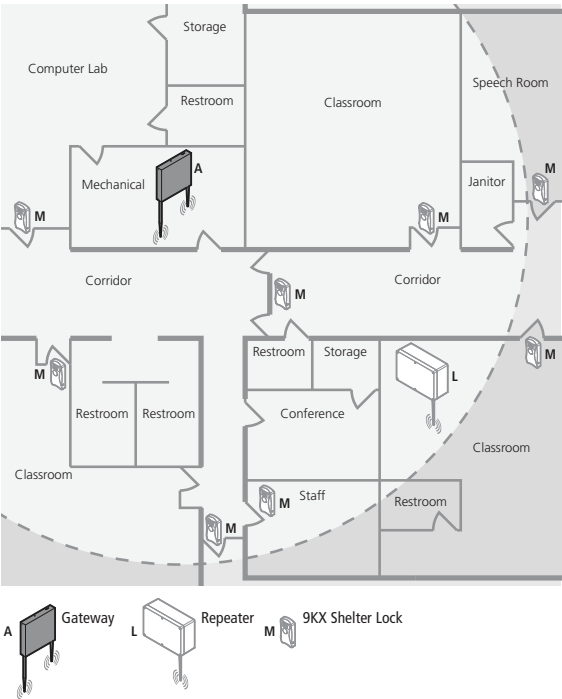


Note: White stripe +12VDC

Note: Maximum recommended wire run is 200 ft with 18AWG wire.

Installation considerations

- Gateway should be installed as high off the floor as possible
- Care should be taken to avoid placing gateway antennas within one ft of large metallic objects—structural members, electrical cabinets, etc.—to minimize signal degradation
- Placing gateway on an open metallic shelf or cabinet top is acceptable as long as antennas are configured at right angles—see Shelter gateway installation instructions section #3, alternative orientations—and antennas are clear of large metallic objects within a one ft radius
- Installation location should provide a minimum of eight inches of separation between the gateway antenna and persons during operation to ensure FCC RF exposure guidelines are met
- Installation in locations that produce poor site survey results may require the installation of an optional omni-directional antenna kit (p/n SHX-OMNI)
- When enrolling devices, if a new location is required for the gateway be sure to press the **Save Configuration** button before removing power or device enrollments may be lost
- Create a site plan to determine the area you want to secure and where to install the gateway
- The gateway should be installed in a centralized location near a network connection and within 200 ft of the power supply
- Gateways should be installed in a climate controlled and secure area
- All wiring or hardware should be in a secure area and not exposed to potential tampering
- A fob is typically capable of sending a signal up to 200 ft away to reach a gateway or repeater
- A Shelter lock is typically capable of receiving a signal up to 400 ft away from a gateway or repeater
- A repeater is typically capable of receiving a signal up to 400 ft away from a gateway
- A repeater may be required to maximize coverage and extend the range



Gateway web page

The Shelter solution is offered with a gateway cloud-based service to set up, configure, test, and monitor the Shelter solution. While the use of the gateway cloud-based service is recommended to get the best use out of your Shelter solution, it is not required. Users can log on to their gateway via a local network connection to perform minimal configuration and management of the Shelter solution. Not all features and functions of the software are available via the local gateway.

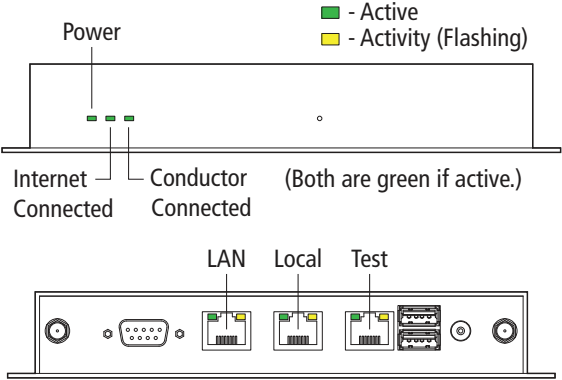
Critical functions like the following will be available on the local gateway web page:

- Lock group creation
- Lock group associations
- Unlock all locks
- Unlock individual locks
- Traffic inspection to see that locks are sending status
- Gateway firmware updates—web page only
- Clearing downlink channel—web page only

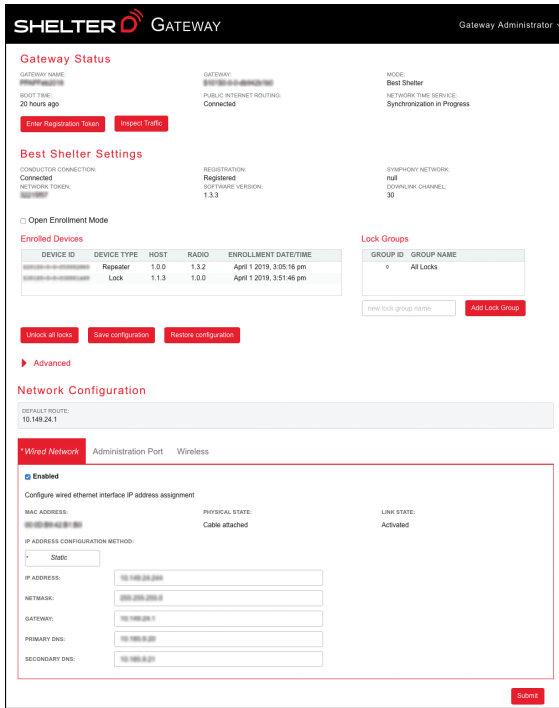
- If the Shelter cloud-based software is not being used and new devices need to be added, see **Offline Mode Option** section
- The gateway web page can be reached via local ethernet connection at 192.168.3.3 or the LAN connection via DHCP; this is the IP address recorded earlier under gateway network setup

LEDs

Guide to LED's found on the gateway:



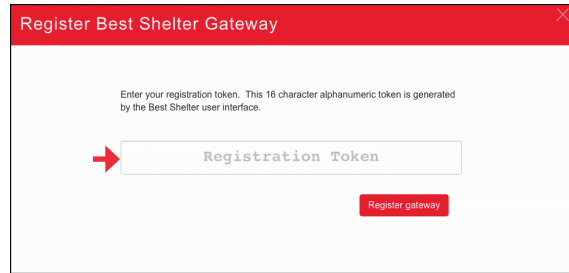
Note: Gateways labeled P/N LL1A07LFT029 will only display power LED no matter the connection status.



- Mode
- Network time service

Actions under the **Enter Registration Token** button include:

- Register gateway to the Shelter cloud-based account using this 16 character alphanumeric token



Information found under the **Inspect Traffic** button includes:

- View live traffic in raw data form from devices

Shelter settings:

Once the gateway is registered, the conductor connection will say connected, and the registration will say registered. If the state is not connected and not registered, devices will not enroll and will not be available for configuration in the Shelter cloud-based software.

Information under **Shelter** settings includes:

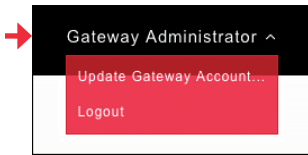
- Conductor connection
- Network token
- Registration
- Software version
- Symphony network

If the public internet routing state is not connected:

- New devices will not be able to enroll unless using offline mode

Actions under the **Gateway Administrator** drop-down tab include:

- Update gateway account – allows password change
- Logout – log out of the gateway page



Information under **Gateway** status includes:

- Gateway name
- Boot time
- Gateway MAC
- Public internet routing – shows connected when a public internet connection is available

- Existing devices connected to the gateway will not be available for configuration in the Shelter cloud-based software

Enrollment failures include:

- If a device fails to enroll, the gateway open enrollment mode may not be checked
- If a device fails to enroll, the gateway public internet routing may not be connected or the conductor connection may not be registered; see **Offline Mode Option** section
- If a device fails to enroll, a factory reset and/or power cycle may be necessary
- If a device fails to enroll, the communication signal may be too weak; perform a site survey of the location where enrollment failed; a repeater may be required near this location

Open Enrollment Mode check box includes:

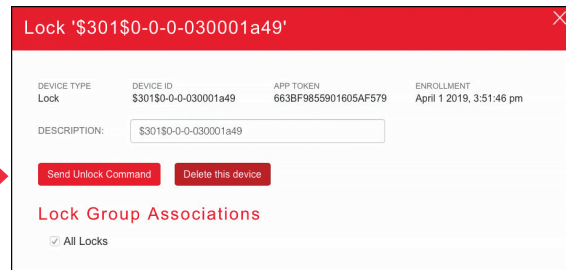
- Check to enable enrollment of devices

Information under **Enrolled Devices** includes:

- Current devices enrolled
- Time when the device was enrolled
- Firmware versions of the device

Actions when clicking on a device under **Enrolled Devices** include:

- Send unlock command – sends unlock command to this device only
- Delete this device – deletes the device from the enrolled devices
- Lock group associations – check the groups that need to be associated with the device

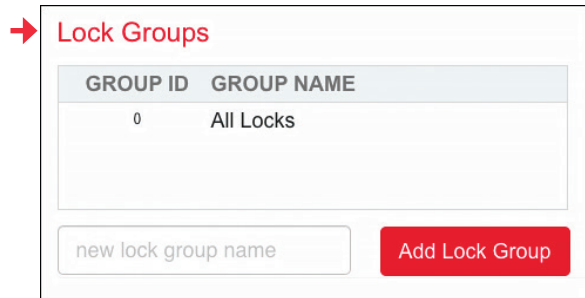


Information under **Lock Groups** includes:

- Shows available lock groups to assign to devices

Actions under the **Add Lock Groups** button include:

- Click to create a new lock group—64 max per gateway



Unlock All Locks button function includes:

- Unlocks all locks and places repeater relays in normal state

Save Configuration button function includes:

- Saves current device configurations locally and to the Shelter cloud-based service if registered
- The configurations will automatically be saved every five minutes if the button is not pressed; if the restore configuration is pressed, it will override the current configuration if it has not been saved

Restore Configuration button function includes:

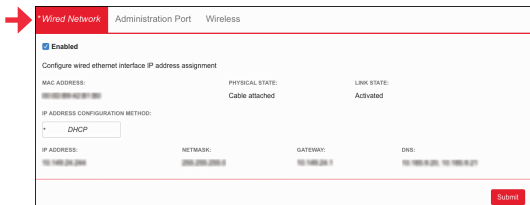
- Restores the configuration from the Shelter cloud-based service

Advanced tab information includes:

- Shows package installation versions and active processes

Network Configuration information includes:

- Wired network – shows the MAC address and DHCP IP address for the LAN connection
- Administration port – shows the MAC address and fixed IP address for the local connection
- Wireless – reserved for future use



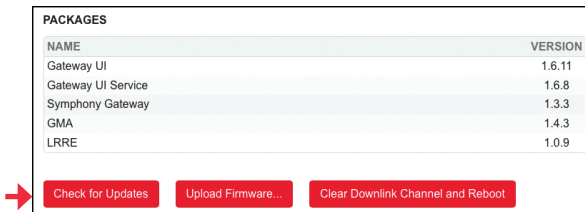
Click the **Advanced** link

- The **Check for Updates** button is for updating gateway software

WARNING: Pressing this may require firmware updates for the devices. Contact technical support to check device and gateway compatibility.

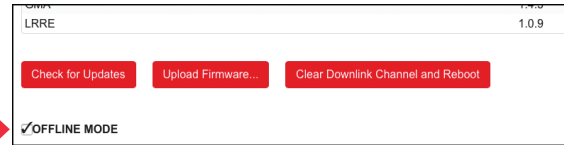
- The **Clear Downlink Channel and Reboot** button is to choose a new downlink channel if the environment has changed where the initial channel selected becomes less than optimal

WARNING: Devices may need to be reset if the downlink channel changes.



Offline mode option

Offline mode is used for sites that choose not to connect their gateway to the public internet.



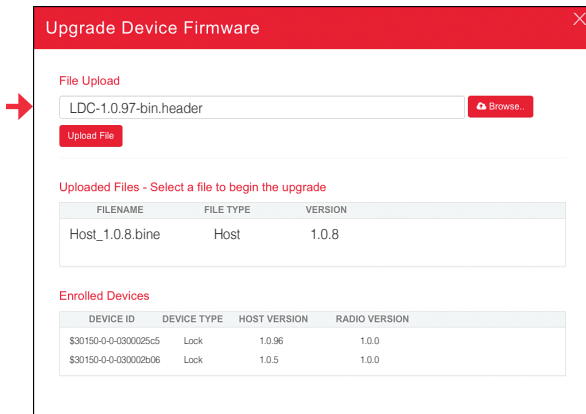
- It allows devices to be enrolled without the public and conductor internet connections
- When in offline mode transactions, device status, self-test, notifications, and control of devices will not be possible through the Shelter cloud-based software
- Devices enrolled in offline mode will not show up as available devices in the Shelter cloud-based software; this is true even if the **Offline Mode** box is unchecked at a later date
- Devices enrolled in offline mode will need to be re-enrolled if the gateway is placed back in online mode

Lock firmware updates

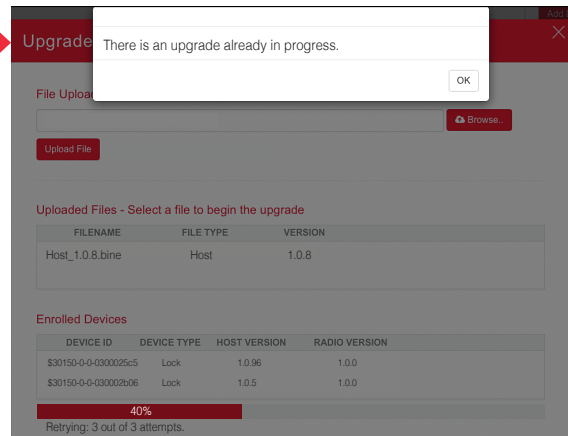
Only locks with firmware version 1.1.0 and newer are capable of wireless firmware updates.

- Click the **Upload Firmware** button
- Choose a file with a .bine extension; it will show incorrect file type if the wrong file type is selected

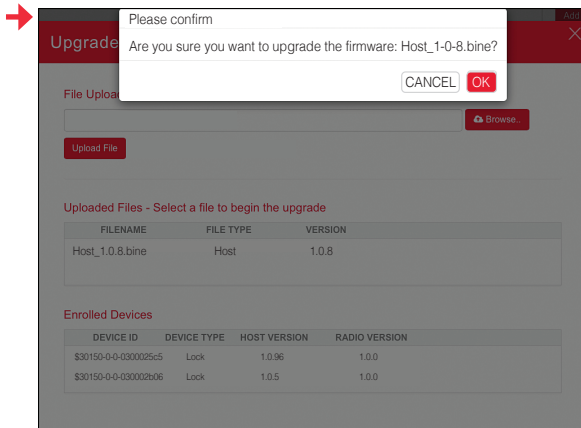
- Select the file



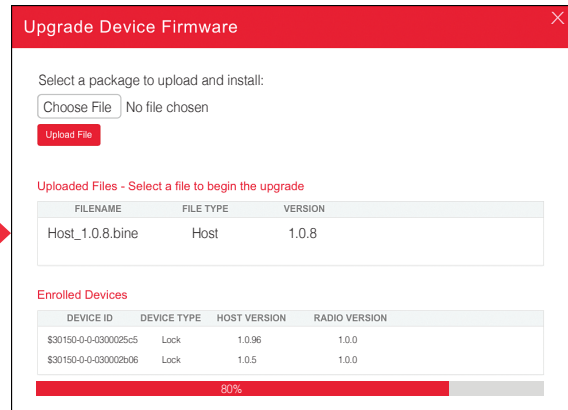
- It will display upgrade in progress if already running



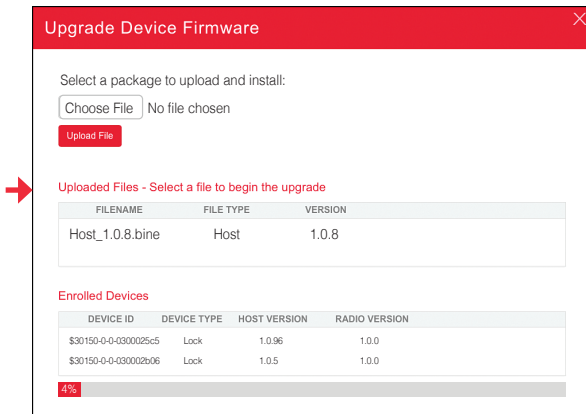
- Confirm the upgrade



- Let the lock upgrade run; all locks that require the update will update at the same time



- Let the upgrade process retry if necessary; no action required



Lock

The Shelter locks are based on the 9K cylindrical lock and the 45H mortise lock platforms. It is battery powered and communicates via 900MHz securely with the gateway. The lock operates mechanically with a key in both lock-down and standard modes.

Mechanical operation

- Classroom – in standard mode, lock and unlock with the key on outside
- Storeroom – in lockdown mode, the key retracts latch; outside lever always locked

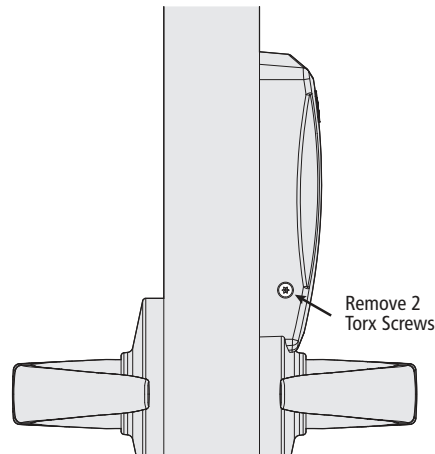
Power and batteries

- Battery life can be viewed in the **Additional Information** section of the lock in the Shelter cloud-based software
- The Shelter lock operates on four AA batteries

- Use AA alkaline batteries rated for 2850mAh; battery life will decrease if the batteries do not meet this specification
- Only use alkaline batteries, and do not mix with other types of rechargeable or lithium batteries
- Only use fresh batteries, and do not mix new and used cells as this would result in invalid remaining battery life of the lock
- When the battery becomes critical and while it still can operate the motor, the motor will lock the Shelter chassis leaving the Shelter lock in storeroom mode

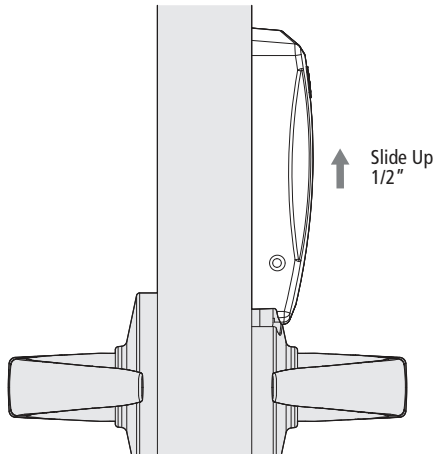
Enclosure removal:

- Remove the two security screws on either side of the enclosure

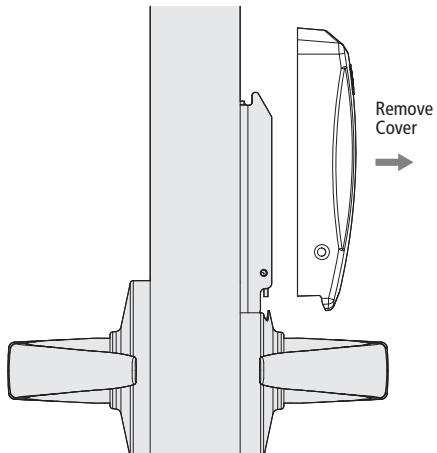


- Pull directly up on the black plastic enclosure until it starts to move; it will only need to travel roughly half an inch

WARNING: The enclosure has the possibility to cause internal damage if you continue moving upwards; remove slow and controlled. If you feel the enclosure has some resistance to continue traveling upwards or has bottomed out, do not continue to force it upwards; remove slow and controlled.



- Pull the enclosure directly away from the door

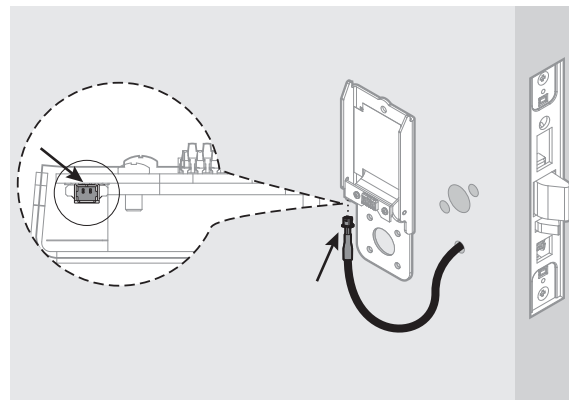
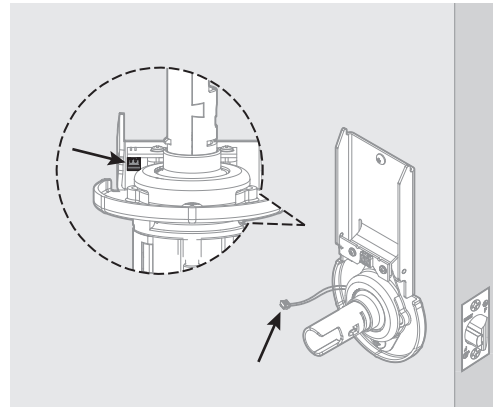


Tamper detection

- When the electronics enclosure is removed, the sounder and LED will indicate this action and a transaction will be sent to the Shelter cloud-based software
- When the electronics enclosure is re-installed, the sounder and LED will indicate this and normal functionality will resume; if this indication does not occur, inspection of the electronic's connections is required

Motor connection:

- Do not pull on motor wires
- The motor connector should not be removed without removing the transfer board as it is a locking connector



LEDs and sounder

Event	Sounder	LED
Power Up	lock/unlock sounder actions will occur following the previous stored state	cycles through all LED colors
Tamper Detection	8 short	8 short yellow
Tamper Clear	3 short	3 short cyan
Lockdown	10 short	solid red while locking; continuous short red for 1 minute; 2 short every 1 minute for 60 minutes; 2 short every 5 minutes until restore
Restore	5 short	solid green while unlocking; 5 short green
Low Battery	1 long every 5 minutes	1 long red every 5 minutes
Firmware Update	n/a	blue flashing
Delay before Lockdown	n/a	yellow continuous
Survey Mode Start	2 short	2 short cyan
Self-Test	1 special	blue-green-red-white
Motor Error	2 long	2 long red
Factory Reset	continuous every 1/2 second	yellow continuous
Enrollment Success	4 short	4 short blue

Factory reset

- Use a flathead screwdriver to short PCB contacts marked 'deep reset' while removing and reinstalling a battery—power cycle:
 - Continue to hold screwdriver in place until sounder begins to beep continuously
 - Cycle power again to complete deep reset
- Factory reset removes gateway enrollment from the lock and restores settings to factory default

Enrollment

- Locks will attempt to enroll to any gateway with enrollment mode enabled when powered up
- If enrollment fails, the unit may need a factory reset to restart the process

Configuration

- Each Shelter lock and repeater can be programmed to include an additional delay anywhere from 1 to 60 seconds after the receipt of a signal—over and above the 10-20 second typical response time
- Shelter LED/sound configuration: LED and sound configuration options can be disabled from the Shelter solution
- **Note:** If these options are disabled, the user will not have any visual or sound confirmation that the Shelter lock received a lockdown signal.

Site survey

- Every Shelter lock electronics module can be used to conduct a site survey
- Power cycle the lock and DO NOT install onto mounting bracket; you will see the site survey start indication

- Shelter locks can enter site survey mode even if they are not enrolled into a gateway
- To exit site survey, either reinstall the electronics on the mounting bracket and wait 12 minutes for this mode to timeout or power cycle and reinstall on the mounting bracket
- When not enrolled, the site survey will automatically switch to the strongest gateway or repeater signal; you may see a white LED during the switch
- When enrolled, the site survey will not switch from the gateway or repeater enrolled through if it can still communicate with it
- User may have to walk slowly or wait for the lock to detect the strongest signal
- The LED indication updates approximately every 15 seconds
- If the site survey starts yellow (-119 to -110) or lower at the door, slowly walk the lock enclosure toward a gateway or repeater to see where it turns green
- If the site survey is indicating yellow (-119 to -110) or lower, the signal MAY NOT be strong enough to reliably communicate; green (-109 to -100) or better is recommended for the best results

Site survey LED signal strength indications:

LED Color	Signal Strength (RSSI)
Blue	-89 or higher
Light Blue	-99 to -90
Green	-109 to -100
Yellow	-119 to -110
Orange	-125 to -120
Red	-126 or lower
White	Disconnected

Self-test

- The Shelter lock self-test can be executed on a schedule or manually
- The self-test triggers the Shelter lock to perform diagnostics:
 - Lock and unlock to detect motor failures
 - LED test
 - Sound test
- Results are returned to the gateway and updated in the Shelter cloud-based software
- Notifications can be set to alert configured users of the system with results of the self-tests

Mechanical consideration

Open door:

- The Shelter solution does not come with a door closer solution
- All doors must remain in a closed position for the locking mechanism to work
- If a door is open when a lockdown is initiated, it will still revert to a locked position but will need to be manually closed to restrict the area

Right of egress:

- The Shelter solution has been designed to prevent entry into a room when a threat is present; however, the inside lever of the Shelter lock will not lock which will allow for a right of egress at all times
 - You will always be able to exit a room, even during a lockdown

Mechanical key:

- Even during lockdown mode, a mechanical key will still be able to operate the latchbolt and open a door

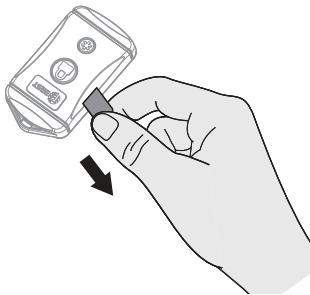
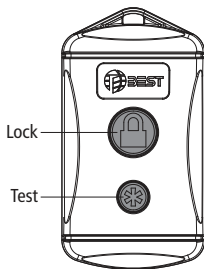
- End users are encouraged to maintain security and control of mechanical keys at all times

Fob

A fob provides a handheld wireless method of sending a lockdown command to a lock/repeater or a group of locks/repeaters. It has a typical range of 200 ft from a gateway or repeater. Building construction can affect this range.

Buttons

The fob has two buttons. The **Lock** button initiates a lockdown and the **Test** button initiates a test of the fob functionality.



Enrollment

- Do not pull the battery tab from the fob until the gateway enrollment mode is enabled, and the fob is in range of the gateway

- When the battery tab is pulled, the enrollment process will start
- If the battery tab was already pulled, the battery can be removed and re-installed to re-start the enrollment process
- At the start of enrollment, the bottom small button flashes green for several seconds, and then the top large button flashes green for several seconds
- If the fob fails to enroll, a factory reset may be required

Successful enrollment:

- Button flashing stops when enrollment is successful

Failed enrollment:

- If the fob can hear the gateway but cannot enroll, the small LED will continue to flash green
- If the fob cannot hear the gateway, the large button will continue to flash red

Factory reset

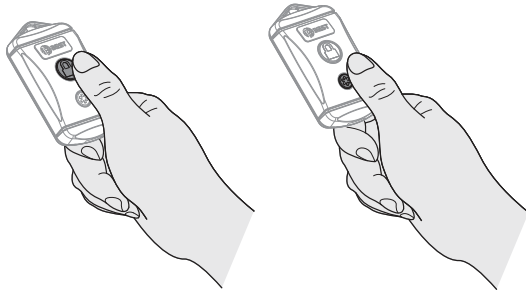
- To factory reset the fob, hold in the large button while inserting the battery, and continue to hold until the large button green LED flashes
- When the green LED flashes, the factory reset is complete and the enrollment process will re-start

Operation

- Remove the cover



When pressing the **Lock** or **Test** button, the fob should be oriented in your hand as shown:



Note: Do not operate the fob from inside a pocket as the signal will not be optimal.

Lock button:

- Press and hold **Lock** button up to two seconds to initiate a lockdown. **Lock** button will flash red, then green, indicating a lockdown was initiated, and a signal was sent
- If after pressing the **Lock** button it does not flash green, the signal from the fob was not properly sent; the fob signal may be out of range of the Shelter solution or may be experiencing interference
- The Shelter solution was designed with a Shelter lock that has a visual LED indicator that will turn red and an alarm that will sound when a lockdown has been completed
- **NOTE:** If the Shelter lock LED indicator does not turn red or the alarm does not sound, your lock may NOT be in lockdown mode.

Test button:

- To test fob functionality, press and hold **Test** button up to two seconds
- **Test** button flashes red, then green, indicating successful connection

LEDs

The **Lock** and **Test** buttons have LED indicators within them that will illuminate when either button is held for two seconds.

When the battery is low, the large button will flash red every 30 seconds.

Testing

- It is highly recommended to test a facility with the maximum amount of fob users at the same time to ensure proper performance of the Shelter solution
- If delays or performance impacts occur, please contact your dormakaba USA Inc. representative for recommendations
- The fob should be tested by pressing the **Test** button in all areas of the Shelter solution where the fob functionality is desired
- During any drills, the fob should be tested
- Fobs should be regularly tested to ensure proper performance of the fob and lock
- Battery life needs to be monitored and managed

Battery

- CR2450 is the battery type required for the job
- Typical battery life is two–three years but may vary depending on usage



Repeater

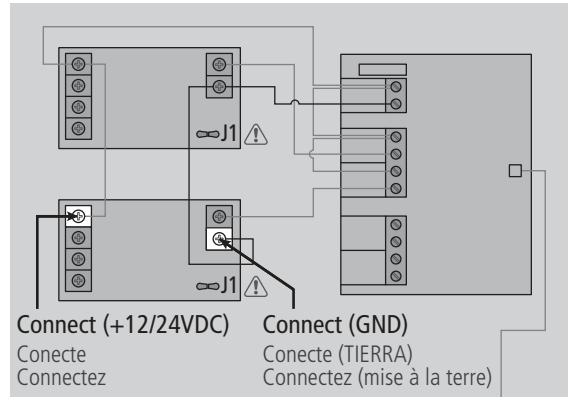
A repeater is a device that helps expand the signal from the gateway. A gateway has a range of around 400 ft in each direction. However, this distance may vary depending on building construction. If a lock is farther away than 400 ft, a repeater would be used to take the wireless signal from the gateway and increase it another 400 ft. A repeater also has input and output relays to allow for easy integration into existing systems.


Power

- 12-24VDC power supply with a minimum of 0.75A

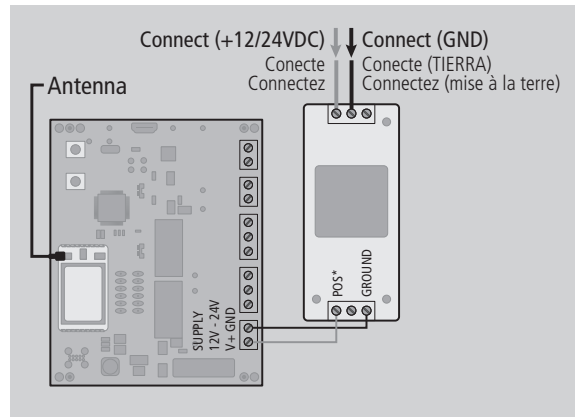
Note: Maximum recommended wire run is 200 ft with 18AWG wire.

- Connection to a power supply that contains a battery backup
- It is recommended to use a UL294 certified power supply



 **Note:** Cut J1 resistor on the Altronix relay boards for 24VDC

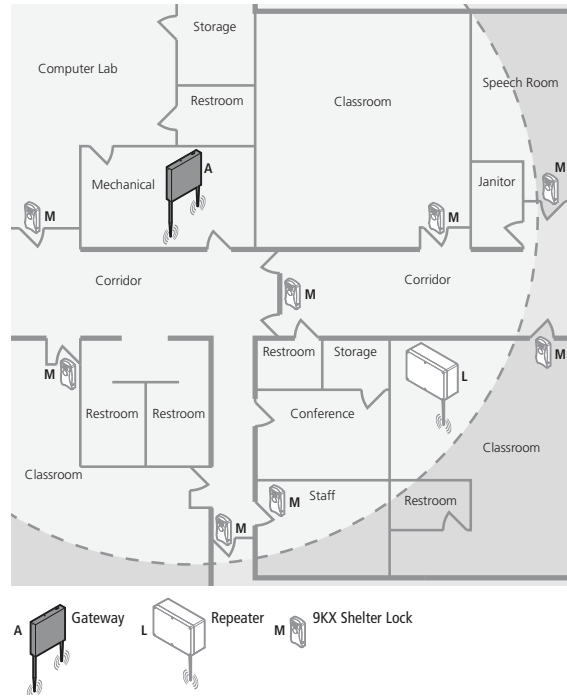
Revision A wiring diagram



Revision G and later wiring diagram

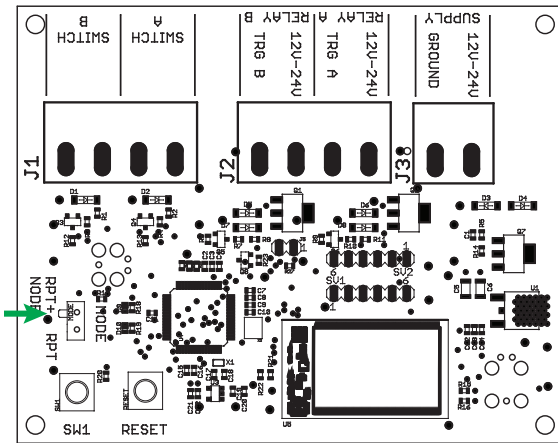
Installation considerations

- Repeater should be installed as high off the floor as possible
- Care should be taken to avoid placing repeater antennas within one ft of large metallic objects —structural members, electrical cabinets, etc.— to minimize signal degradation
- The antenna orientation must be vertical either facing up or down
- Installation location should provide a minimum of eight inches of separation between the gateway antenna and persons during operation to ensure FCC RF exposure guidelines are met
- Installation in locations that produce poor site survey results may require the installation of optional omni-directional antenna kit (p/n SHX-OMNI)
- If the repeater installation location is outdoors, an optional pole mount kit (SHX-PLE) is available
- Installation of the repeater in an outside environment should be installed with the recommended water tight seal or connections
- Create a site plan to determine the area you want to secure and where to install the repeater
- The repeater should be installed within the 400 ft nominal transmit range of the gateway
- It should also be located within 200 ft of power supply and any additional devices you wish to control
- Additional repeaters may be required to extend range or full coverage of building



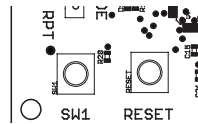
Enrollment

- Select the mode of operation before enrolling the repeater



- Switch the mode switch to RPT ON to allow the repeater to extend the range of the gateway
- Switch the mode switch to RPT OFF to allow the repeater to just control the inputs and outputs
- Ensure the gateway enrollment mode is enabled
- Powering the repeater for the first time will start the enrollment process
- The three LEDs on the repeater board will alternate sequentially during the enrollment process
 - With RPT mode enabled, the center and right LED will continuously flash after successful enrollment
 - With RPT mode disabled, only the right LED will continuously flash after successful enrollment
- If enrollment fails, the repeater may need to be factory reset or power cycled

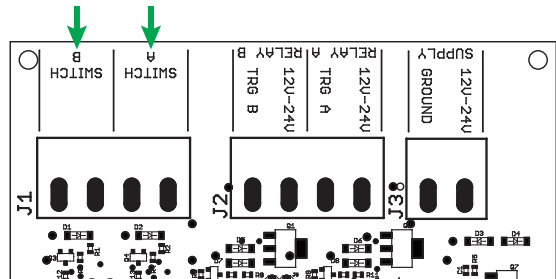
Factory reset



- Press the **Deep Reset** button and hold while pressing the **Reset** button momentarily
- Continue to hold the **Deep Reset** button until all three LEDs flash three times
- The enrollment process will re-start at this time

Inputs

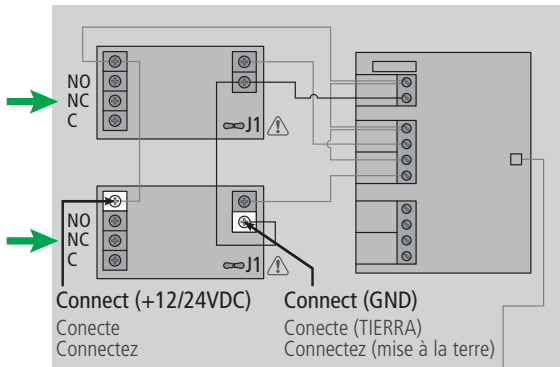
- Input switch A will operate at a lockdown input
- Input switch B will operate at a restore input



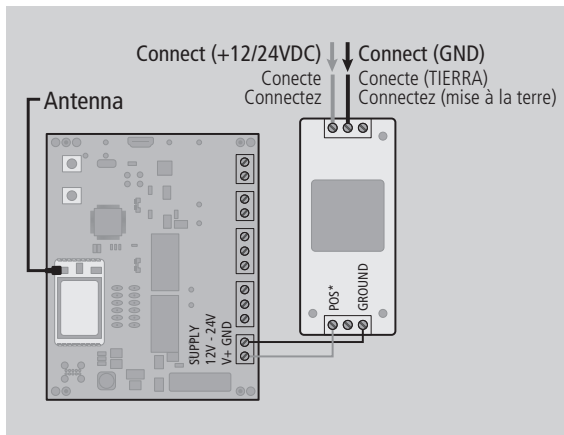
- Both inputs require a dry contact to trigger, and they do not allow voltage input

Outputs—relay boards

- Both relays operate at the same time during a lockdown and restore event



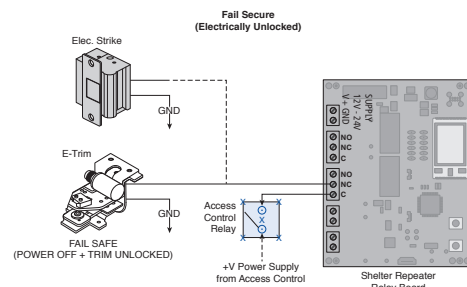
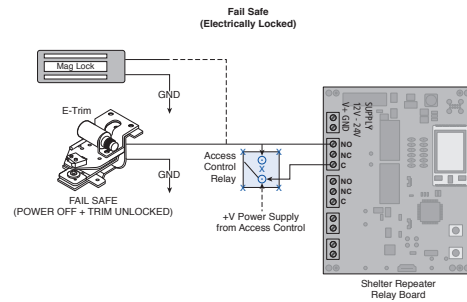
Revision A repeater outputs



Revision G and later repeater outputs

- Both relays are form C with both normally open and normally closed contacts
- Both relays are rated at 24VDC @ 1AMP

Common examples of relay connections:



- Contact your local integrator to determine recommended connections

Compatibility with other systems

While the Shelter solution network components including the Shelter lock, fob, and repeater may be capable of being configured via input and output relays to allow the fob to initiate a signal to any third-party access control system or alarm system allowing communication with first responders, dormakaba USA Inc. has not tested these systems and cannot guarantee the accuracy or performance of the Shelter solution components with third-party products. dormakaba USA Inc. recommends that you work with your third-party integrator to determine compatibility and performance of the system. dormakaba USA Inc. shall have no liability or obligation for additional products or services provided or delivered by a third-party.

6 Installation Validation

Verify enrollment

Once all devices are enrolled verify the following:

- Locks have reported a firmware version
- Locks are reporting status at the status update interval that was configured
- Each fob should be tested that it is configured properly for specified lock groups
 - Start with a mechanically unlocked door 'unlocked by key'
 - Perform the lockdown with the fob
 - Ensure all doors in that lock group have been locked
 - On the gateway device management page, press the restore button
 - Ensure all doors in that lock group have been unlocked
- After lockdown/restore commands testing is complete, verify each lock responded with locklog messages
- On the gateway device management page, press the self-test button
- Confirm for each lock under **Lock Device Management**
 - Signal strength
 - Battery level
 - Last self-test result
- Repeater inputs are functioning if wired to switches
- Repeater output relay devices are functioning as intended, alarms, exit devices, etc.
- Ensure all created user accounts can log in
- Test all notification events occur as configured
- Test that battery backups are functioning for the repeaters and gateway
- Verify all locks can be locked/unlocked by key

Verify firmware over the air upgrade

Once all locks have successfully taken an over the air upgrade, the same steps for verifying enrollment should be taken to verify the upgrade.

Performance notes

- The distance of signal may vary depending upon building construction
- Proper testing of all fobs is recommended to ensure signals are being properly sent and received to the gateway and to understand the scope of where a lockdown can be initiated both inside and outside of a building
- Signals cannot be guaranteed at the exact time a lockdown is initiated
- Frequent self-tests are recommended to ensure proper performance of the system

- All wireless devices should be installed with consideration given to nearby metal objects; performance could be impacted
- Typical lockdown response time is 10 to 20 seconds from the initiation of a signal
- Typical lockdown clear response time is 10 to 20 seconds from the initiation of a signal; however, certain conditions could impact this delay

7 Training/Testing/Use/Drills

Notes and information:

- Frequent testing of the Shelter solution is strongly recommended, including scheduled self-testing via the gateway cloud-based service
- Any changes to building construction or layout should be followed up with proper testing
- Any further addition of wireless devices to the building should be followed up with the proper testing
- Any changes in staff or personnel who are holders of a fob should be followed up with proper testing and training
- Any changes in products connected or integrated with the Shelter solution should be followed with proper testing
- Once a door is locked, it can still be manually opened on the inside to allow entry for those individuals who were not able to access the area prior to the lockdown
- Users should have appropriate training and security plans in place to secure persons who are not able to enter an area prior to the lockdown being implemented
- Testing of the Shelter solution without the gateway cloud-based service will be a manual effort and not allow you to test all functions or capabilities
- Final testing may result in the need for additional products, including gateways, repeaters, fobs, etc.
- dormakaba USA Inc. site survey tools may provide an initial recommendation on products needed; however, each end user is responsible for working with their own facility management, distributor, or third-party integrator to determine final products required to ensure the proper performance of their Shelter solution
- dormakaba USA Inc. does not guarantee the accuracy of any site surveys
- As conditions to the end user's environment change, additional equipment may be required. dormakaba USA Inc. is not responsible for providing additional equipment as end user's conditions or environment change

8 Warranty

Warranty Information

What is Covered: dormakaba USA Inc. warrants that the Products manufactured by dormakaba USA Inc., identified below, and sold under its trade names "BEST" and "SHELTER" are free of defects in materials and workmanship as outlined below. The sole and exclusive liability of dormakaba under this warranty is limited to the repair or replacement of any Product or component part covered by the warranty at the sole discretion of dormakaba.

Who is Covered: This warranty is extended only to the Seller's distributors of Products and the end user who purchases Products for purposes other than resale (collectively, "Purchaser").

Hardware Warranty Period:

The following products shall be warranted for three (3) years from the date of sale:

- 9KX Electro-mechanical Cylindrical Lock
- 45HX Electro-mechanical Mortise Lock

The following products shall be warranted for one (1) year from the date of sale:

- Shelter Gateways, Shelter Repeaters and Repeater Accessories, Shelter FOBs

Finishes shall be warranted for three (3) years from the date of sale excluding US10B/613 "Oil Rubbed Bronze" finish.

Warranty Claims: Any Products believed to be defective as covered by this warranty may not be returned without

prior written Returned Materials Authorization (RMA) from dormakaba Customer Service 1-855-365-2407 covering specific items and quantities within thirty (30) days from the discovery of the alleged defect(s). dormakaba will inform the purchaser where to ship said Product(s), shipping charges prepaid by you, for examination. In the event such examination reveals a defect covered by this warranty; dormakaba will, at its sole option, repair or replace the Product, and return it or its replacement to the purchaser, with charges only for shipping.

Exclusions: This warranty specifically excludes, and dormakaba shall not be held responsible for the following:

- a) COSTS ASSOCIATED WITH INSTALLING, REMOVING OR REINSTALLATION OF THE PRODUCT.
- b) Damage caused by Product malfunction or failure attributable to acts of God.
- c) Improper use or installation.
- d) Poor or no maintenance or routine testing.
- e) Work performed by someone other than an Authorized dormakaba technician.
- f) Failure to follow dormakaba's operating instructions, quick use guide, or environmental specifications.
- g) Incorrect application, modification, vandalism, erosion or corrosion, shipping and/or handling, improper storage, accident, misuse, abuse or any other cause not within the control of dormakaba.
- h) This warranty is void if any modification is made to the

warranty product, regardless of whether the modification causes or contributes to the alleged defect. All modifications are made at the risk and expense of the party making the modifications.

- i) dormakaba shall not be liable for any repairs, replacements, or adjustments to the product or any costs of labor performed by the Purchaser or others without dormakaba's prior written approval.
- j) dormakaba provides no warranty or guarantee that the Shelter 9KX Cylindrical Lock, Shelter FOB, Shelter Gateway or Shelter repeaters or repeater accessories will function properly or be mechanically compatible with products not manufactured by dormakaba, including any third party access control systems, third party monitoring systems, etc.
- k) The US10B/613 finish is considered to be a living finish that will change over time with use and age and is expressly excluded from this warranty. The finish changes that occur are indicative of normal wear and tear and reflect the essence of a living finish. The finish changes are not considered manufacturing defects and are not covered by this warranty.
- l) This warranty does not cover any post sales technical support under the following circumstances:
 - a. Failure to provide a network connection if deemed necessary by dormakaba
 - b. Technical support for network configuration
 - c. Technical support for software installed on computer hardware or computer operating system that is no longer commercially available for purchase.
 - d. Technical support for unsupported internet browsers
- m) It is Customer's responsibility to obtain all necessary use permits, licenses, etc. required by the local jurisdiction for installation of any Shelter components.
- n) If any Governmental agency requires any changes in

the Shelter solution originally installed, Customer agrees to pay for such changes.

Third Party Warranty: Except as otherwise provided above, dormakaba makes no warranty, express or implied, with regard to third party hardware or software and expressly disclaims the implied warranties or conditions of merchantability or merchantable quality, fitness for a particular purpose, title, infringement and those arising by statute or otherwise in law. Customer's sole recourse for warranty claims is with the manufacturer of the Product. However, dormakaba agrees to pass through any third party warranty that dormakaba receives from the manufacturer of the Products to Purchaser. The extent of any third party warranty details, terms and conditions, remedies and procedures may be expressly stated on, or packaged with, or otherwise accompanying the Products.

For the purpose of this Warranty, the Shelter solution shall include the Shelter 9KX Cylindrical Lock, Shelter FOB, Shelter Gateway, Shelter Repeaters and any Shelter Repeater accessories.

LIMITATION OF WARRANTIES:

THIS WARRANTY IS GIVEN EXPRESSLY AND IN PLACE OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, REPRESENTATIONS, OR WARRANTIES NOT SPECIFIED HEREIN.

DORMAKABA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE SHELTER SOLUTION MAY NOT BE COMPROMISED, OR THAT THE SHELTER SOLUTION WILL IN ALL CASES BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE, OR PROVIDE THE PROTECTION FOR WHICH IT IS INTENDED.

LIMITATION OF LIABILITY

THE SHELTER SOLUTION MAY BE USED TO ACCESS AND TRANSFER INFORMATION OVER THE INTERNET. DORMAKABA DOES NOT OPERATE OR CONTROL THE

INTERNET AND EXPRESSLY DISCLAIMS ANY AND ALL LIABILITY ASSOCIATED WITH ANY OF THE FOLLOWING: (A) VIRUSES, WORMS, TROJAN HORSES, OR OTHER UNDESIRABLE DATA OR SOFTWARE; OR (B) UNAUTHORIZED USERS (E.G., HACKERS) OR ATTEMPTS TO OBTAIN ACCESS TO AND DAMAGE CUSTOMER'S DATA, WEBSITES, COMPUTERS, OR NETWORKS. DORMAKABA SHALL NOT BE RESPONSIBLE FOR SUCH ACTIVITIES. CUSTOMERS ARE SOLELY RESPONSIBLE FOR THE SECURITY AND INTEGRITY OF THEIR DATA AND SYSTEMS.

THE SHELTER SOLUTION IS A PRODUCT DESIGNED TO REDUCE THE RISK OF ENTRY INTO A LOCKED AREA. DORMAKABA SHALL NOT BE HELD LIABLE FOR LOSSES WHICH MAY OCCUR IN CASES OF MALFUNCTION OR NONFUNCTION OF ANY SHELTER PRODUCT,

LOSSES RESULTING FROM FAILURE TO WARN OR INADEQUATE TRAINING; EVEN IF DUE TO DORMAKABA'S NEGLIGENCE OR FAILURE OF PERFORMANCE

DORMAKABA IS NOT AN INSURER. INSURANCE COVERING PERSONAL INJURY, PROPERTY LOSS, AND DAMAGE TO AND ON CUSTOMER'S PREMISES MUST BE OBTAINED AND/OR MAINTAINED BY CUSTOMER. CUSTOMER UNDERSTANDS THAT IT IS CUSTOMER'S DUTY TO PURCHASE SUCH INSURANCE.

THE WARRANTY PROVIDED HEREIN SHALL CONFER NO RIGHTS ON THE PART OF ANY PERSON OR ENTITY THAT IS NOT A PARTY HERETO, WHETHER AS A THIRD-PARTY BENEFICIARY OR OTHERWISE.

IT IS AGREED THAT IT IS IMPRACTICAL AND EXTREMELY DIFFICULT TO FIX ACTUAL DAMAGES WHICH MAY ARISE IN SITUATIONS WHERE THERE MAY BE A FAILURE OF THE SHELTER SOLUTION. THEREFORE, IF LIABILITY IS IMPOSED ON DORMAKABA, ITS EMPLOYEES, AGENTS OR REPRESENTATIVES, FOR PROPERTY DAMAGE OR PERSONAL INJURY, SUCH LIABILITY SHALL BE LIMITED TO AN AMOUNT EQUAL TO THE PURCHASE PRICE OF THE PRODUCTS COVERED BY THIS WARRANTY OR \$10,000 WHICHEVER IS LESS. THIS SUM SHALL BE PAID AND RECEIVED EITHER (I)

AS LIQUIDATED DAMAGES AND NOT AS A PENALTY, OR (II) AS A LIMITATION OF LIABILITY APPROVED AND AGREED UPON BY THE PARTIES. THE PAYMENT OF THIS AMOUNT SHALL BE DORMAKABA'S SOLE AND EXCLUSIVE LIABILITY REGARDLESS OF WHETHER LOSS OR DAMAGE IS CAUSED BY THE PERFORMANCE OR NONPERFORMANCE OF OBLIGATIONS OF DORMAKABA UNDER THIS WARRANTY OR BY NEGLIGENCE, ACTIVE OR OTHERWISE, OF DORMAKABA, ITS EMPLOYEES, AGENTS OR REPRESENTATIVES.

NO SUIT OR ACTION SHALL BE BROUGHT AGAINST DORMAKABA MORE THAN ONE (1) YEAR AFTER THE ACCRUAL OF THE CAUSE OF ACTION ARISES.

DORMAKABA SHALL NOT, IN ANY EVENT, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL OR PUNITIVE DAMAGES SUFFERED BY PURCHASER OR ANYONE CLAIMING BY, THROUGH OR UNDER PURCHASER, AS A RESULT OF THE CONDITION OF THIS PRODUCT, OR ANY PART OR PORTION THEREOF.

SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS OR PROHIBIT THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY IN YOUR STATE.

THIS WARRANTY IS GOVERNED BY THE LAW OF THE STATE OF INDIANA WITHOUT REGARD TO ITS CONFLICTS OF LAW PRINCIPLES. DORMAKABA AND PURCHASER AGREE THAT THE UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS SHALL NOT APPLY TO SALE OF THE PRODUCTS COVERED BY THIS WARRANTY.

CUSTOMER RETAINS THE SOLE RESPONSIBILITY FOR THE LIFE AND SAFETY OF ALL PERSONS IN ITS PREMISES, AND FOR PROTECTING AGAINST LOSSES TO HIS/HER OWN PROPERTY OR THE PROPERTY OF OTHERS IN ITS PREMISES, CUSTOMER AGREES TO INDEMNIFY AND SAVE HARMLESS DORMAKABA, ITS EMPLOYEES,

AGENTS, OR REPRESENTATIVES FROM AND AGAINST ALL CLAIMS, LAWSUITS, DAMAGES AND LOSSES, WHETHER IN CONTRACT LAW, TORT LAW (INCLUDING NEGLIGENCE, PRODUCT LIABILITY AND STRICT LIABILITY, OR ANY OTHER THEORY OF LAW), IN ANY WAY RELATING TO THIS WARRANTY OR THE USE OR OWNERSHIP OF THE SHELTER SOLUTION, OR THE IMPROPER OPERATION OF THE SHELTER SOLUTION, WHETHER DUE TO MALFUNCTIONING OR NONFUNCTIONING OF THE SHELTER SOLUTION OR THE NEGLIGENT PERFORMANCE OR NONPERFORMANCE BY DORMAKABA, INCLUDING BUT NOT LIMITED TO PERSONAL INJURY OR PROPERTY DAMAGE.

DORMAKABA SHALL NOT BE LIABLE FOR ANY FINE OR PENALTY ASSESSED BY ANY MUNICIPALITY, FIRE, OR POLICE DEPARTMENT AS A RESULT OF ANY FALSE ALARM COMMUNICATED BY THE SHELTER SOLUTION. CUSTOMER SHALL BE RESPONSIBLE FOR CREDITING DORMAKABA THE FULL AMOUNT OF ANY SUCH FINE OR PENALTY THAT IS ASSESSED AGAINST DORMAKABA FOR SUCH FALSE ALARM ISSUED BY CUSTOMER.