dormakaba

CenconX Series Keypads

CenconX

System User Guide

CX003.0524 - 10/**2024**
Original document

EN

Table of Contents

1 Introduction

This guide outlines general information for using and programming CenconX series keypads, safe locks, and various system components, including accessories and software client. This guide assumes the installer has knowledge of electrical, mechanical, and computer concepts, as well as having familiarity with safe lock systems and associated components. For reliable and safe operation of the equipment, comply with all safety precautions outlined in this guide.

1.1 Approved Standards

The CenconX family of safe locks conform to the following approved standards:

- UL 2058 (High Security Electronic Locks)
- EN 1300:2018
- Model: CENX – FCC ID: 2ASNP-CENX, IC ID: 24793-CENX

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Changes or modifications not expressly approved by dormakaba USA Inc. could void the user's authority to operate the equipment.

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage.
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CET APPAREIL EST CONFORME À LA NORME RSS INDUSTRIE CANADA EXEMPT DE LICENCE. Son fonctionnement est soumis aux deux conditions suivantes:(1) Cet appareil ne doit pas provoquer

d'interférenceset(2) Cet appareil doit accepter toute interférence, y compris les interferences pouvant causer un mauvais fonctionnement du dispositif. Cet appareil numérique de la classe [B] respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

1.2 Electrical Precautions

Ensure alkaline batteries (where applicable) are new and in good condition; leaking batteries can cause damage to components and can also cause serious bodily harm. Do not apply power (where applicable) before completing all steps of the installation; doing so may damage the components. Ensure all power supplies are plugged into grounded electrical receptacles that comply with local building code(s). When AC mains power is required the power supply shall be installed in accordance with NFPA 70 and any applicable electrical codes.

1.3 Environmental Specifications

Operating & Storage Temperature Range: For UL compliance, this product was verified for operation at 32

122 °F (0 50 °C)

Relative Humidity Range: 0 95% non-condensing

1.4 Tools

dormakaba USA Inc. recommends having the following tools on hand to install CenconX safe locks and their components:

- Digital voltmeter
- Wire cutters and needle nose pliers
- Set of screwdrivers
- Drill and drill bits
- Automatic saw (band saw, hand saw)
- US or Metric taps
- File or equivalent tool
- All installation/hardware documentation for quick reference

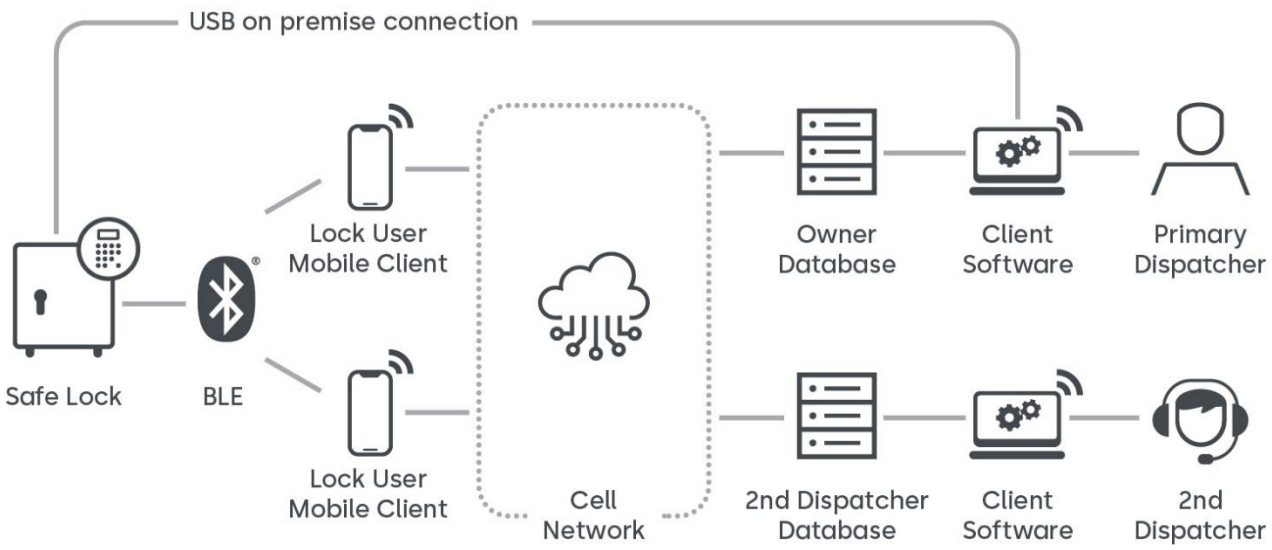
Consult the CenconX Installation Guide (Doc# CX004.0524) for further details on the specific parts and tools required for installation.

2 Typical System Layout

The following sub-sections review safe lock system components with related diagrams. Refer to each product's individual documentation for more detailed information on hardware installation and proper device usage.

The following diagram (Figure 1) shows a complete CenconX system layout for a single lock system with primary and secondary dispatcher. Please note that your system may not include all components shown.

Figure 1 – CenconX Authorization & Verification Framework



In the CenconX system, Lock Users use credentials to access and open safe locks through one or more of the following methods:

- Entering a valid credential using the CenconX keypad.
- Utilizing a wireless BLE credential at a CenconX keypad. This credential is managed using the Software backend database and dispatched to a Mobile device running the Mobile Client Application.

When setting up your CenconX system, you have the ability to configure a single client/database setup for a single Owner (Primary Dispatcher), or you can introduce a second client/database to allow for a Secondary Dispatcher to have some control over system management and access.

2.1 Safe Lock Hardware

The CenconX system components have been tested as compatible with the CenconX system and should not be substituted. Consult each component's individual documentation for proper mounting, connectivity, and installation. The safe itself must be appropriate for the lock hardware to provide maximum security; certain makes and models of safes may not be appropriate for this CenconX safe lock system. If unsure, consult with dormakaba USA Inc. Sales or Support for further information.

2.2 System Components

Each system may differ depending on customer requirements. The following sub-sections cover the full suite of the CenconX safe lock system.

2.2.1 Keypad

The CenconX Keypad is the user interface for the entire system. All Keypads are available in both Tamper Evident and Serviceable options, which will impact how the keypad is physically mounted. Refer to the CenconX Installation Guide (Document # CX004.0524) for more information.

2.2.2 Safe Lock

The safe lock is either a dead bolt or a swing bolt that locks and unlocks when the Keypad receives correct user credentials. Refer to the CenconX Installation Guide (Document # CX004.0524) for more information.

2.2.3 AC Adapter

The AC Adapter can be used to power the System where batteries alone would not be appropriate. Refer to the AC Adapter Installation Guide (Document # 7037.0320) for more information. (Item/Order # 701107, "AC-Power Supply Multi-Adapter")

2.2.4 Battery Box

The Battery Box can serve as the secondary power source to the CenconX System. Refer to the Battery Box Installation Guide (Document #7035.0421) for more information. The Battery Box is not UL evaluated. (Item/Order # 704055, "Battery Box")

2.2.5 Alarm Box

The Alarm Box is a hard-wired external alarm device. If used, the Alarm Box must be plugged into the BAT port of the primary lock. The Alarm Box allows for a remote disable input that can block the open command to the lock if asserted. Refer to the Alarm Box Installation Guide (Document #7036.0320) for more information. The Alarm Box is not UL evaluated. (Item/Order # 704045, "Alarm Box")

2.2.6 Reset Box (coming soon)

The Reset Box offers the capability to remove users and reset the Master Combination. To reset the lock, the lock must be disconnected from any power source (AC Power or Battery) and powered from the Reset Box only. The Reset Box must be connected to the BAT port on the back of the CenconX safe lock. The Reset Box has a green LED that will light when the reset function is performed. If a lock is already reset, applying the Reset Box will not light the LED.

Refer to the Reset Box User Guide (Document #~~7039.0521~~) for more information. The Reset Box is not UL evaluated. (Item/Order # ?????, "Reset Box")

2.2.7 Power Considerations

The system common power across all components. As long as 9V DC power is supplied to the system, the system will work as intended. It is unnecessary to apply multiple sources of power to some or all components.

Some considerations to follow:

- The standard-profile Keypad models require two 9V batteries to be inserted into the tray.
- The low-profile Keypad models require a Battery Box or Power Adapter accessory for power. These keypads include an emergency battery connection to apply power from outside of the safe container.
- A Battery Box accessory is available to be attached inside the secure container to grant power to the system.
- A Alarm Box can be connected to the primary lock to provide power to the system. This Alarm Box must be physically located in the secure side of the container.
- An AC/DC Power Adapter accessory can be used to apply line power to the system.

- When resetting a lock via the Reset Box, a 9V battery must be inserted into the Reset Box to apply power for the short duration usage.

2.3 Getting Started

This section outlines typical use of a CenconX System with a single or multi-user setup with references to various sections found through this document.

Follow these steps to get started implementing a System:

1. **Identifying System Requirements (System Planning Stage)**
    a. Identify Required System Components – Review Section 2.2 "System Components" for installation procedures regarding each component of a System.
    b. Identify System type – Review Section 3.1 Understanding the CenconX System to understand the difference between the single database setup and the dual database setup to determine which one is right for you.
    c. Identify Required User Types and Privileges – Read Section 3.2 "CenconX System User Types" , 3.2.1.8 Lock User Permissions – System User Functions, and 3.2.2.5 Software User Permissions – System User Functions for an overview how each user is authorized to use the system.
2. **Configure the System**
    a. Install/Commission/Activate – Read Section 3.6 Installing, Commissioning, and System Activation for instructions on performing this step.
3. **Customize the System**
    a. Set Date and Time – Read Section 3.8 Change Time/Date/DST for instructions on setting or re-setting the Time.
    b. Configure other System Functions – Instructions for configuring custom options are provided in Section 3.5 System Functions and elsewhere throughout the document.
4. **Running/Maintaining the System)**
    a. Refer to Section 4 Keypad replacement for information pertaining to replacement of defective CenconX keypads.
    b. Refer to Section 3.9 Battery Levels for information about system power and knowing when to replace your device's batteries.
    c. Refer to Section 3.11.2 Reset a Lock to learn how to revert a lock to its default/factory settings.
    d. Refer to Section 3.10 View Audits to learn how to view and retrieve audits (see also Appendix A: List of Audits)

3 How to Use the System

This section outlines how to use the installed system and how to execute specified functions. Please note that your installation may not include everything outlined in this section.

3.1 Understanding the CenconX System

CenconX is a keyless OTC safe lock solution consisting of three primary components:

- The CenconX keypad/lock system
- The dormakaba Safe Locks mobile app
- The dormakaba Apexx Series Software

3.1.1 System Description

The CenconX system it a combined hardware and software solution that grants administrators control over the setup and configuration of CenconX safe locks and the control and management of CenconX lock systems and the individuals who use them.

Users of various types can be granted access to CenconX Lock systems through the use of One Time Codes (OTCs) or Personal Identification Numbers (PINs). OTCs and PINs can be assigned and dispatched to users via Apexx Series Software who use them to gain access to the CenconX lock system by entering them on a CenconX keypad or a mobile application installed on their smart phone.

In addition to lock configuration, user and device (lock, keypad, mobile device) management, and code dispatching, Apexx Series Software also allows users to pull audits and create audit reports, create and manage lock access schedules, as well as a whole array of other system management tools. Refer to Apexx Series Software's built-in help menu for detailed descriptions of all software features and how to use them.

3.1.2 Primary Dispatcher vs. Secondary Dispatcher

As previously mentioned, when setting up your CenconX system, you have the ability to configure a single client/database setup for a single Owner (Primary Dispatcher), or you can introduce a second client/database to allow for a Secondary Dispatcher to have some control over system management and access.

Primary and Secondary Dispatcher roles vary slightly in what abilities they have with regard to system management. For more details, refer to the following sections in this document:

- 3.2.2.3 Software Users - Dispatcher
- 3.2.2.5 Software User Permissions – System User Functions
- 3.3.1 Lock Access Modes

3.2 CenconX System User Types

In CenconX, there are three types of users who utilize and/or control various aspects of the lock system:

- Lock Users
- Mobile Application Users
- Software Users

Their functions and abilities regarding the roles they play in the lock system are described in the subsections that follow.

3.2.1 Lock User Types

There are four types of Lock users, each with different capabilities. The sub-sections outlined below cover each Lock User Type and their respective functions.

3.2.1.1 Lock User Type - Admin

The Administrator (Admin) User is the most powerful of the Lock Users, responsible for aspects of the lock system such as installation, Lock User setup/creation, and system configuration.

- There will always be 1 Admin (aka Master) User per safe lock.
- The Admin User ID is 00
- the Admin user ID can never be disabled.
- The Admin user cannot open a lock directly, though the Admin has the ability to create other Lock Users (Managers and Standard Users) who have the ability to open locks.
- Admins are involved in the initial installation and setup of a lock
- Admins have advanced user capabilities such as the ability to reset locks and reinstall keypads.
- Admins have the ability to change the combinations of users of all types, including their own.

Refer to the Lock User Permissions Chart for a more detailed breakdown of the Admin User's abilities.

3.2.1.2 Lock User Type - Manager

As the name suggests, Managers are involved in the management of the lock system and its users.

- A safe lock can have up to 2 Manager Users
- The Manager User IDs are 01 and 02
- Managers have more privileges than normal Lock Users (Static & OTC Users), but not as many as the Administrator.
- Unlike the Administrator, Managers can open locks

Refer to the Lock User Permissions Chart for a more detailed breakdown of Manager User's abilities.

3.2.1.3 Lock User Type – Static Pin User *coming soon*

Static Pin Users are one of the two Standard User types (the other being OTC Users) that are subordinate to both the Admin and Manager User types.

Static PIN Users are assigned fixed combinations that can be used to access the safe lock system.

- Static PIN Users can be assigned various abilities, including the ability to open locks or view audits at the keypad.
- Static User PINs are fixed at 6-digits long

Refer to the Lock User Permissions Chart for a more detailed breakdown of the Static Pin User's abilities.

Note: Static Users are only available in the Primary Dispatcher (Owner) database.

3.2.1.4 Lock User Type – One Time Code User

One Time Code Users are one of the two Standard User types that are subordinate to both the Admin and Manager User types.

OTC (One Time Code) users receive single-use opening codes valid for one use on an associated lock. The dispatching of these codes and the user-lock associations are controlled by Software Users.

- A safe lock can have an unlimited number of OTC users
- Regardless of the number of OTC users, only a maximum of 50 one-time-codes can be assigned/dispatched to users at any given time
- If the System is configured with a Secondary Dispatcher, the 50 one-time-codes is distributed evenly between the Owner and Dispatcher (25 each)
- An OTC user can be dispatched, at most, 3 one-time-codes for a particular lock without them being expired or consumed.

Refer to the Lock User System Functions Chart (Table *2*) for a more detailed breakdown of the OTC User's abilities.

3.2.1.5 Lock User Permissions – Access Lock

A user may be granted permission to open the lock. This capability allows the user to open the lock when they present the proper credential(s). Access restrictions such as Time Delay, are enforced unless override privileges are granted.

3.2.1.6 Lock User Permissions – Audit Lock

A user can be granted permission to retrieve audits. This user can retrieve audits by connecting the system to a PC and utilizing the Apexx Series Software, or review audit information from the Keypad menus.

If using a mobile device, audits will be retrieved from the lock and sent to the software backend whenever the mobile device is used to operate the lock.

3.2.1.7 Lock User Permissions – Time Delay Override with Combination

A user may be granted permission to Override Time Delay. This will allow the user to open the lock without waiting for the time delay period to expire. If the system is in Dual User Mode and one user has this privilege, the Time Delay will be overridden.

The Table below shows the permitted mix of capabilities a user may perform. The configuration software and lock firmware shall enforce this capability mix. The numbers in the table represent the states of each user privilege (1 = enabled, 0 = disabled)

Table 1 - User Capabilities

TDO w/Combo	Audits	Access	User Capabilities
0	1	0	• Can retrieve audits only • Cannot open the lock
0	0	1	• Can open the lock only
0	1	1	• Can open the lock • Can retrieve audits
1	0	1	• Can open the lock • Can override the Time Delay with their credential(s) • Cannot retrieve audits
1	1	1	• Can open the lock • Can retrieve audits • Can override the Time Delay with their credential(s)

3.2.1.8 Lock User Permissions – System User Functions

The Table below shows the list of System User Functions available for each Lock User type.

Table 2 - Lock User System Functions

Functions	Admin (ID = 00)	Manager (ID = 01 or 02)	Static PIN User (ID = 03 - 49) *COMING SOON*	OTC User	No Authentication required
Commission Keypad/Lock	N/A	N/A	N/A	N/A	**Yes**
Reset Lock via Keypad	**Yes**	No	No	No	No
Reinstall Keypad	**Yes**	No	No	No	No
Configure Lock Access Schedule	No	No	No	No	No
View Lock Access Schedule	No	No	No	No	No
Configure Lock Holiday Schedule	No	No	No	No	No
View Lock Holiday Schedules	No	No	No	No	No
Set Time Format	**Yes**	**Yes**	No	No	No
Set Date Format	**Yes**	**Yes**	No	No	No
Daylight Saving Time (DST) Enable/Disable	**Yes**	**Yes** (if permitted)	No	No	No
Set Date/Time on Lock	**Yes**	**Yes** (if permitted)	No	No	No
View Audits on Keypad	**Yes**	**Yes**	**Yes** (requires Access Privilege)	No	No
Retrieve Audits to PC	**Yes**	**Yes**	**Yes** (requires Access Privilege)	No	No
Activate PC Link	**Yes**	**Yes**	**Yes** (requires Access Privilege)	No	No
Assign Lock Access Schedule	No	No	No	No	No

Functions	Admin (ID = 00)	Manager (ID = 01 or 02)	Static PIN User (ID = 03 - 49) *COMING SOON*	OTC User	No Authentication required
Enable/Disable Dual User Mode	No	No	No	No	No
Enable/Disable Dual User Mode Applies to Managers	No	No	No	No	No
Enable/Disable Dual Credential Mode	No	No	No	No	No
Enable/Disable Dual Credential Mode applies to Managers	No	No	No	No	No
Get System Information	**Yes**	**Yes**	**Yes**	**Yes**	No
Add/Delete/Disable/Enable Users	No	No	No	No	No
Assign Lock Access for a User	No	No	No	No	No
Add/Delete Manager (in lock)	No	No	No	No	No
Enable Time Delay Override Feature (per lock)	No	No	No	No	No
Add/Remove Time Delay Override Privilege for a Manager/User	No	No	No	No	No
Set Time Delay: Delay Period & Open Period Time (per lock)	No	No	No	No	No
Set Manager Combination (Manager in lock)	No	No	No	No	No
Open Lock	No	**Yes**	**Yes**	**Yes**	No
Change Own Lock User Combination	**Yes**	**Yes**	**Yes**	No	No

Functions	Admin (ID = 00)	Manager (ID = 01 or 02)	Static PIN User (ID = 03 - 49) *COMING SOON*	OTC User	No Authentication required
Time Delay: Delay Period Counting – up/down/none	No	No	No	No	No
Time Delay: Open Period Counting – up/down/none	No	No	No	No	No
Cancel Time Delay (cancel lock opening)	**Yes**	**Yes**	**Yes**	No	No
Set Duress Combo Enable/Disable per System	No	No	No	No	No
Change Admin (in lock) Combination	**Yes**	No	No	No	No
Open Lock with Override Time Delay w/ Combination	No	**Yes**	**Yes** (requires Access Privilege)	No	No
Set Keypad Backlight On/Off	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Set Buzzer On/Off	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Set Language on keypad	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Force PIN Change on 1st use	No	No	No	No	No
Accept Firmware Update	**Yes**	**Yes**	No	No	No
Configure Remote Input Signal	No	No	No	No	No
Show last Close Codes	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

3.2.2 Software Users

Software Users use Apexx Series Software to perform system administrative tasks, such as controlling/changing system settings and providing and configuring system access.

Software Users fall into the following categories:

- Administrator
- Manager
- Dispatcher
- Auditor

3.2.2.1 Software Users - Admin

- The Admin has full control over users of all user types (Software and Lock Users)
- Can create, delete, and/or update Lock Users using the software interface
- Can create specialized groups of locks within the software

Refer to the Software User System Functions Chart (Table *3*) for a more detailed breakdown of the Admin User's abilities.

3.2.2.2 Software Users - Manager

- Can manage Dispatchers and Audit-only Users.
- Can create routes for OTC users within the software
- Can create, delete, and/or update Lock Users using the software interface

Refer to the Software User System Functions Chart (Table *3*) for a more detailed breakdown of the Manager User's abilities.

3.2.2.3 Software Users - Dispatcher

- The Dispatcher is able to provide one-time-codes to users, but has a limited capacity to do so.
    - If the System is configured with a Secondary Dispatcher, the 50 one-time-codes is distributed evenly between the Primary Dispatcher and the Secondary Dispatcher (25 each)
- An Admin has the ability to assign Dispatchers to one or more Lock Groups. This would define which locks the Dispatcher would be able to dispatch one-time-codes for.

Refer to the Software User System Functions Chart (Table *3*) for a more detailed breakdown of the Dispatcher User's abilities.

3.2.2.4 Software Users – Audit Only User

- Can only view Audit reports

Refer to the Software User System Functions Chart (Table *3*) for a more detailed breakdown of the Audit Only User's abilities.

3.2.2.5 Software User Permissions – System User Functions

Table *3* shows the list of System User Functions available for each Software User type.

Table 3 - Software User System Functions

Functions	**SW User – Primary Dispatcher Tenant** **Roles:** admin, dispatcher, manager, auditor	**SW User – Secondary Dispatcher Tenant** **Roles:** admin, manager, auditor, dispatcher	**SW User via "PC application for FW update over USB"** FW update works differently for uncommissioned (no ID and PIN authorization) vs. commissioned (require authentication with valid ID and PIN)	**SW User – "Special installer software"** Special software works differently for uncommissioned vs. commissioned locks
Commission Keypad/Lock	No	No	No	No
Reset Lock via keypad	No	No	No	No
Reinstall Keypad	No	No	No	No
Configure Lock Access Schedule	• **admin** • **manager**	No	No	No
View Lock Access Schedule	• **admin** • **manager**	• **admin** • **manager**	No	No
Configure Lock Holiday Schedule	• **admin** • **manager**	No	No	No
View Lock Holiday Schedules	• **admin** • **manager**	• **admin** • **manager**	No	No
Set Time Format	• **admin** • **manager**	No	No	**Yes**
Set Date Format	• **admin** • **manager**	No	No	**Yes**
Daylight Saving Time (DST) Enable/Disable	• **admin** • **manager**	No	No	**Yes**
Set Date/Time on lock	• **admin** • **manager**	• **admin** • **manager**	No	**Yes**
Retrieve Audits to PC	• **admin** • **manager**	• **admin** • **manager**	No	No
Assign Lock Access Schedule	• **admin** • **manager**	No	No	No

Functions	SW User – **Primary Dispatcher Tenant** **Roles:** admin, dispatcher, manager, auditor	SW User – **Secondary Dispatcher Tenant** **Roles:** admin, manager, auditor, dispatcher	SW User via "PC application for FW update over USB" FW update works differently for uncommissioned (no ID and PIN authorization) vs. commissioned (require authentication with valid ID and PIN)	SW User – **"Special installer software"** Special software works differently for uncommissioned vs. commissioned locks
Enable/Disable Dual User Mode	• **admin** • **manager**	No	No	No
Enable/Disable Dual User Mode Applies to Managers	• **admin** • **manager**	No	No	No
Enable/Disable Dual Credential Mode	• **admin** • **manager**	No	No	No
Enable/Disable Dual Credential Mode Applies to Managers	• **admin** • **manager**	No	No	No
Get System Information	• **admin** • **manager** • **dispatcher**	• **admin** • **manager** • **dispatcher**	**Yes**	**Yes**
Add/Delete/Disable/Enable Users	• **admin** • **manager**	No	No	No
Assign Lock Access for a User	• **admin** • **manager**	No	No	No
Add/Delete Manager (in lock)	• **admin** • **manager**	No	No	No
Enable Time Delay Override Feature (per lock)	• **admin** • **manager**	No	No	No
Add/Remove Time Delay Override Privilege for a Manager/User	• **admin** • **manager**	No	No	No
Set Time Delay: Delay Period & Open Period Time (per lock)	• **admin** • **manager**	No	No	No

Functions	**SW User – Primary Dispatcher Tenant** **Roles:** admin, dispatcher, manager, auditor	**SW User – Secondary Dispatcher Tenant** **Roles:** admin, manager, auditor, dispatcher	**SW User via "PC application for FW update over USB"** FW update works differently for uncommissioned (no ID and PIN authorization) vs. commissioned (require authentication with valid ID and PIN)	**SW User – "Special installer software"** Special software works differently for uncommissioned vs. commissioned locks
Set Manager Combination (manager in lock)	• **admin** • **manager**	No	No	No
Open Lock	No	No	No	No
Time Delay: Delay Period Counting – up/down/none	• **admin** • **manager**	No	No	No
Time Delay: Open Period Counting – up/down/none	• **admin** • **manager**	No	No	No
Cancel Time Delay (cancel lock opening)	No	No	No	No
Set Duress Combo Enable/Disable per System	• **admin** • **manager**	No	No	No
Change Admin (in lock) Combination	• **admin** • **manager**	No	No	No
Open Lock with Override Time Delay w/ Combination	No	No	No	No
Configure Input/Output settings for lock	• **admin** • **manager**	No	No	**Yes**
Dispatch OTC to lock/user (and optionally mobile device)	• **admin** • **manager** • **dispatcher**	• **admin** • **manager** • **dispatcher**	No	No
Send FW files to keypad/lock	• **admin** • **manager**	• **admin** • **manager**	**Yes**	**Yes**

Functions	**SW User – Primary Dispatcher Tenant** **Roles:** admin, dispatcher, manager, auditor	**SW User – Secondary Dispatcher Tenant** **Roles:** admin, manager, auditor, dispatcher	**SW User via "PC application for FW update over USB"** FW update works differently for uncommissioned (no ID and PIN authorization) vs. commissioned (require authentication with valid ID and PIN)	**SW User – "Special installer software"** Special software works differently for uncommissioned vs. commissioned locks
Dispatch Activate with or without Open command	• **admin**	• **admin**	No	No
Dispatch Sync to a mobile device/lock	• **admin** • **manager** • **dispatcher**	• **admin** • **manager** • **dispatcher**	No	No
Transfer Ownership	• **admin**	No	No	No
Enter Close Code for prior Open dispatch	• **admin** • **manager** • **dispatcher**	• **admin** • **manager** • **dispatcher**	No	No
Force Close of an open Dispatch	• **admin** • **manager**	• **admin** • **manager**	No	No
Create/Edit/Delete Lock Users	• **admin** • **manager**	• **admin** • **manager**	No	No
Accept Mobile Device registry	• **admin** • **manager**	• **admin** • **manager**	No	No
Create Lock entries in database	• **admin** • **manager**	No	No	No
Create Secondary Dispatcher tenant	• **admin**	No	No	No
Send updated info from Primary Dispatcher database to Secondary Dispatcher database	• **admin**	N/A	No	No
Import info into Secondary Dispatcher database	N/A	• **admin**	No	No

Functions	**SW User – Primary Dispatcher Tenant** **Roles:** admin, dispatcher, manager, auditor	**SW User – Secondary Dispatcher Tenant** **Roles:** admin, manager, auditor, dispatcher	**SW User via "PC application for FW update over USB"** FW update works differently for uncommissioned (no ID and PIN authorization) vs. commissioned (require authentication with valid ID and PIN)	**SW User – "Special installer software"** Special software works differently for uncommissioned vs. commissioned locks
Cancel or Remove Secondary Dispatcher tenant	• **admin**	No	No	No
Create/Edit/Delete SW user	• **admin**	• **admin** • **manager**	No	No
Create/Edit/Delete Route of locks	• **admin** • **manager** • **dispatcher**	• **admin** • **manager** • **dispatcher**	No	No
Display retrieved audits from locks	• **admin** • **manager** • **dispatcher** • **auditor**	• **admin** • **manager** • **dispatcher** • **auditor**	No	No
Display SW audits or logs	• **admin** • **manager** • **dispatcher** • **auditor**	• **admin** • **manager** • **dispatcher** • **auditor**	No	No
Set Lock User/Mobile application user ability to self-dispatch OTC	• **admin** • **manager**	• **admin** • **manager**	No	No

3.2.3 Mobile Application Users

Mobile Application Users use credentials on their mobile devices to gain access to the CenconX lock system. These credentials are managed in the system by Software Users and can be accessed by Mobile App users on their mobile devices.

- Mobile App users are assigned lock access and various privileges using Apexx Series Software (this is done by Software Users)
- Mobile App Users are Lock Users, but not all Lock Users are Mobile App Users.
- Mobile Users also play a key role with respect to auditing the lock system.

3.3 CenconX System User Modes

The User Mode is a system setting that determines how many Users and what class of user can gain access to the Keypad and applies to all locks connected to the System.

Note: The User Mode can only be set by authorized Software users.

3.3.1 Lock Access Modes

Different User Modes are available to users in the Primary and Secondary Dispatcher databases. See Table *4* and Table *5* for details.

Table 4 - User Mode Lock Access (Primary Dispatcher Database)

Mode	Lock Access	Notes
Single (Dual Mode OFF)	1 OTC User or 1 Static User or 1 Manager	Single user is the default User Mode for safe locks
Dual (OTC + OTC)	2 OTC Users or 1 Manager	Requires 2 One Time Code Users (or 1 Manager) to authenticate. Duress can be activated with either of the user's combinations.
Dual (Static + Static)	2 Static Users or 1 Manager	Requires 2 Static User IDs to authenticate. Duress can be activated with either of the user's combinations.
Dual (Static + OTC)	(1 Static User + 1 OTC User) Or 1 Manager	Requires 1 Static User and 1 One Time Code User IDs to authenticate. Duress can be activated with either of the user's combinations.

Table 5 - User Mode Lock Access (Secondary Dispatcher Database)

Mode	Lock Access	Notes
Single (Dual Mode OFF)	1 Access User or 1 Manager	Single user is the default User Mode for safe locks
Dual (OTC + OTC)	2 OTC Users or 1 Manager	Requires 2 One Time Code Users (or 1 Manager) to authenticate. Duress can be activated with either of the user's combinations.

3.3.2 Wrong Try Penalty

The Wrong Try Penalty occurs when a User inputs a credential incorrectly 4 times in a row. The penalty period is for 5 minutes, within that time no safe lock connected to the Keypad will open. All menu access and command inputs on the Keypad will also be locked for 5 minutes. Once the 5-minute penalty is over, 2 consecutive incorrect credential inputs will initiate another 5-minute penalty. The Wrong Try Penalty does not expire. This penalty cycle will not be cleared until the lock is successfully opened.

During the penalty period, the keypad will produce 2 short low beeps and 2 short **RED** flashes that will repeat every 10 seconds to signify the penalty is in effect. The time will count down on the screen. During this penalty the Keypad will respond to any key press with 2 short low beeps and 2 **RED** flashes. When the Wrong Try Penalty is over, the LED will flash **GREEN** twice and the keypad will produce 2 high beeps.

Note: If power to the Keypad is interrupted and restored during a Wrong Try Penalty, the penalty period will resume with same time remaining.

During the Wrong Try Penalty period, system operations and lock access via mobile devices will also be locked to users.

3.3.3 Schedules

Schedules are a 7-day time periods consisting of user defined Locking Periods during which access to particular lock(s) becomes restricted.

Software Users can create Lock Access Schedules to set specified time periods for valid lock system access. Once these schedules are created, they can be applied to one or more lock systems. Each lock can have only 1 access schedule applied for all users (One Time Code and Static PIN).

3.3.4 Time Delay

Note: This feature only applies to Static users and is configurable only through the software client.

During a Time Delay, the safe lock cannot be opened until the delay period expires. The Time Delay period ranges from 00 (Disabled) to 99 minutes and is set through the Apexx Software client. Once the Time Delay period is complete, the Confirmation Window period starts. During the confirmation period, the user can re-authenticate to open the lock.

- Keypads will provide continuous feedback to signify the Delay Period and Confirmation Window.
- The Keypad will beep and flash a **RED** LED once every 10 seconds during the Time Delay period.
- The Keypad will then beep and flash a **GREEN** LED once every 10 seconds during the Confirmation Window, signifying the safe lock can now be opened.
- The Confirmation Window is configurable from 1 to 60 minutes.
- The CenconX Keypad provides on-screen feedback during the Delay Period and Confirmation Window. Authorized users have the ability to configure how this feedback is displayed.
- There are multiple ways to override the Time Delay period, if enabled. If Time Delay is enabled for a lock, each valid User ID with a Combination will trigger the start of the time delay period if the intent is to open the lock.
- If Dual User mode is enabled, and a One Time Code User enters their credentials first, the Time Delay will not be applied.

3.3.5 Duress Mode

Note: Duress Mode (Silent Alarm) is not UL evaluated.

Duress Mode functions as a silent alarm that creates an external signal if a Duress Combination is entered. A Duress Combination is the User's combination with the last digit entered one number higher or lower. For instance, a User Combination of 1-2-3-4-5-6-7-8 will use a Duress Combination of either 1-2-3-4-5-6-7-7 or 1-2-3-4-5-6-7-9. When the Duress Combination is entered, a silent alarm will signal, and the lock will open.

Note: Combinations ending in 0 would use 1 or 9. Combinations ending in 9 will use 0 or 8.

- Duress Mode can be turned on/off per lock via Software
- Duress can be triggered by entering a Duress Combination using the CenconX keypad or through the mobile app.
- At the keypad, Duress for One Time Code users will be instigated by pressing the <return key> (←) a single time after the one-time-code is entered. Pressing the <return key> (←) twice after entering the one-time-code will be considered non-duress.
- Duress Mode (Silent Alarm) can also be used to trigger an external alarm system by using an Alarm Box. The Alarm signal will be output on the output line as a 1-second pulse (pulse high for one second)

3.3.6 Second Credential Support via Mobile Device

The CenconX system can be configured to require a secondary credential requirement for authentication. In addition to entering static PINs or one time codes at the keypad, mobile devices can be registered to users using the software backend which can allow for one time codes to be entered via a Mobile Device that has the mobile application installed. Refer to section 3.12 Mobile App for more information on setting up and using the mobile application.

3.4 CenconX Keypad – Layout, Usage, and Settings

3.4.1 Keypad Layout & General Usage

Below is a list of buttons and their functions on the Keypad:

- Number Pad – Can be used for entering User combinations and specific optional functions on screen
- Pound Key (#) – Is used to return to a previous screen, or to wake up the Keypad without entering a number. Pressing the pound key twice will put the keypad in sleep mode.
- Up and Down Arrows (^v) – Navigate through the menu options with these
- Return Key (←) – Confirms a selection or complete a command sequence

3.4.1.1 Keypad – Sleep mode

After a brief period of inactivity, the CenconX keypad goes into sleep mode. While asleep, the keypad will not respond to any BLE communication and will therefore not be able to communicate with the Mobile app. To wake up a sleeping keypad, simply press any of its keys.

3.4.2 Keypad –Menu Settings

To enter the Main Menu, press any non-numeric button followed by your user credentials.

What the User sees on the Keypad menu depends on both the installation/commission state and on what user credentials are entered. There are four possible menu configurations:

- Pre-Commissioned menu
- Unauthenticated Menu
- Admin/Master Menu
- Manager Menu
- Static PIN User Menu (coming soon)

3.4.2.1 Keypad – Menu Settings – Pre-Commission Menu (Installer Checkout Mode)

Initially, before the lock and keypad are commissioned, the lock and keypad are connected and powered, but the system is not yet operational. This state is known as "Installer checkout mode".

At this state, the installer can press the number "1" key to open the lock. Pressing any other key will open the Pre-Commission Menu.

The Pre-Commission Menu will have the following options available:

- Commission
- Time/Date
    - Time Format
    - Date Format
    - Set Time/Date
    - Observe DST
- System
    - Sys Info
        - Keypad
        - Lock
    - Language
    - Backlight
    - Buzzer
    - FW Update
    - Diagnostic

3.4.2.2 Keypad – Menu Settings – Unauthenticated Menu (in Commissioned State)

Once the lock and keypad have been commissioned, the user can wake the keypad, then use various keys to access certain functions/features as outlined below:

Note: If you press any of the numeric keys to wakeup the keypad, this will be read as the first digit of a One Time Code value.

- Press the Up (^) arrow key to bring up the Language menu.
- Press the Down (v) arrow key to display the menu for an unauthenticated user (no PIN entry necessary). The Unauthenticated Menu will have the following options available:

    - System
        - Sys Info
            - Keypad
            - Lock
        - Language
    - Activate Secondary Dispatcher

- Press the <return key> (←) to begin the lock opening sequence for a Statin PIN User (coming soon)
- Press the Pound key (#) to change a user code.

3.4.2.3 Keypad – Menu Settings – Admin/Master Menu

After commissioning the system, the user can press the Pound key (#) then enter the correct Admin code to view the Admin/Master Menu. The following menu features/options will be available:

- Change Code
- Activate Primary Dispatcher
- Deactivate Primary Dispatcher
- Deactivate Secondary Dispatcher
- Time/Date
    - Time Format
    - Date Format
    - Set Time/Date
    - Observe DST
- Audits
- PC Link
- System
    - Sys Info
        - Keypad
        - Lock
    - Language
    - Backlight
    - Buzzer
    - Lock
    - FW Update

3.4.2.4 Keypad – Menu Settings – Manager Menu

After commissioning the system, the user can press the Pound key (#) then enter a correct Manager code to view the Manager Menu. The following menu features/options will be available:

- Open Lock
- Change Code
- Time/Date
  - Set Time/Date
  - Observe DST
- Audits
- PC Link
- System
  - Sys Info
    - Keypad
    - Lock
  - Language
  - Backlight
  - Buzzer
  - FW Update

3.4.2.4 Keypad – Menu Settings – Static PIN User Menu (coming soon)

After commissioning the system, the user can press the Pound key (#) then enter a correct Static PIN User code to view the Static PIN User Menu. The following menu features/options will be available:

- Open Lock
- Change Code
- Time/Date
  - Set Time/Date
  - Observe DST
- Audits
- PC Link
- System
  - Sys Info
    - Keypad
    - Lock
  - Language
  - Backlight
  - Buzzer

3.5 System Functions

The System menu allows the User to view and change various aspects, such as Buzzer, Backlight, etc. Below is a table that outlines Buzzer, LED, and Screen Messages in response to certain events.

Table 6 - Buzzer, LED, and Screen Messages

Event	Buzzer	LED	Screen Message(s)
System wakeup	Short high beep	Short **GREEN** flash	N/A
Key press	Short beep	Short **GREEN** or **RED** flash	High beep + **GREEN** flash = Valid Key Low Beep + **RED** flash = Invalid Key
Valid command response	3 short high beeps	3 short **GREEN** flashes	Success
Invalid command response	3 short low beeps	3 short **RED** flashes	Invalid Message
Wrong Try Penalty	2 short low beeps - every 10 seconds	2 short **RED** flashes – every 10 seconds	Wrong Try Penalty
Wrong Try Penalty ends	2 short high beeps	2 short **GREEN** flashes	
Time Delay Window	1 low beep – every 10 seconds	1 **RED** flash – every 10 seconds	Time Delay
Confirm window	1 high beep – every 10 seconds	1 **GREEN** flash – every 10 seconds	Confirmation Window
Low Battery	2 low beeps	2 **RED** flashes	Low Battery
Critical Low Battery	3 long low beeps	3 long **RED** flashes	Critical Low Battery

Event	Buzzer	LED	Screen Message(s)
Master Reset	3 short high beeps	3 short **GREEN** flashes	Reset Success
Power On – No lock connected	5 medium to low beeps	5 medium **RED** flashes	Connect Lock
Power On – Bad configuration	5 medium to low beeps	5 medium **RED** flashes	Bad Config
Power On/Wake Up – Lock Connected but Not Installed	1 medium low beep	Solid **RED** LED	Install Primary Lock
Power On – Keypad not compatible	1 long low beep	Continuous alternate flashing **RED** and **GREEN**	Wrong Keypad Model Cannot Install
Master reset	3 short high beeps	3 short **GREEN** flashes	Reset Success

3.5.1 System Info

The System Info screen provides information related to the Keypad and safe locks connected to the System, including Firmware version and Model number. **Note:** This information is only available to authorized users.

Follow these steps to navigate through the System Info menu:

1. Enter and Authorized User ID and Combination.
2. Navigate through the Main Menu and select "System".
3. Select "Sys Info" from the sub-menu.
4. Select between "Keypad" or "Lock".
5. If "Keypad" is selected, the following information is available on screen:
    - "Batt Status" – Displays battery level with a percentage
    - "FW version" – Shows the current firmware version on the Keypad
    - "Model" – Displays the Model # of the Keypad
    - "S/N Part 1" and "S/N Part 2" – Shows the serial number of the Keypad (divided between two screens)
6. If "Lock" is selected, the following information is available on screen:
    - "Close Codes" – shows the latest close code
    - "FW version" – Displays the current firmware version on the safe lock

- "S/N Part 1" and "S/N Part 2" – Shows the serial number of the safe lock (divided between two screens)
- "Port | Lock" – Represents the Port and Lock #s
- "Open Count" – Shows how many times the safe lock was opened

3.5.2 Backlight Mode

The Backlight illuminates whenever a key is pressed on the Keypad. By default, the Backlight setting is Off to conserve battery power (if applicable).

Follow these steps to toggle the Backlight Mode On and Off:

1. Enter an Authorized User ID and Combination.
2. Navigate through the Main Menu and select "System".
3. Select "Backlight" from the sub-menu.
4. Select between "On" and "Off" to Enable/Disable Backlight Mode.
5. "Success Mode updated" will appear on screen and the Keypad will beep three times and flash a **GREEN** LED once complete.

3.5.3 Buzzer Mode

The Buzzer provides sound to signal specific functional outcomes. The Buzzer Mode is active (on) by default.

Follow these steps to toggle the Buzzer Mode On and Off:

1. Enter an Authorized User ID and Combination.
2. Navigate through the Main Menu and select "System".
3. Select "Buzzer" from the sub-menu.
4. Select Between "On" and "Off" to Enable/Disable Buzzer Mode.
5. "Success Mode updated" will appear on screen and the Keypad will beep twice and flash a **GREEN** LED once complete.

WARNING: Once the Buzzer Mode has been turned off, there will be no audible signals for successful or unsuccessful commands.

3.5.4 Combination Length

The Combination (PIN) Lengths for Users in a CenconX System are as follows:

- One Time Code users use 9-digit PINs
- Static users use 6-digit PINs (entered in conjunction with their 2-digit User ID)

3.5.5 Force Change Combination (software only???)

The Force Change Combination setting is a security rule that, when enabled, forces Manager and Standard users to change their combination prior to first use.

- In new systems, Force Change Combination is turned off by default.
- This setting can be turned on/off by a Admin Software User.
- The Force Change Combination rule applies to newly added users and newly reset combinations.

Follow these steps to change the Force Change Combination Rule:

1. Enter an Authorized User ID and Combination.
2. Navigate through the Main Menu and select "System".
3. Select "Combination" from the sub-menu.

4. Select “Force Change Combination”.
5. Select “Yes” to enforce the rule, or “No” to ignore the rule.
6. “Success Updated” will appear onscreen, and the Keypad will beep three times and flash a **GREEN** LED once the setting has been changed.

3.5.6 Input and Output Signals

Input and Output Signals are available on CenconX locks that can configured to perform various system functions. Using the Input Signal will require the installation of a Battery/Alarm Box (Item/Order # 704045).

Depending on how it is configured, it will perform one of the following functions when this signal is asserted:

Input Signal

- **Ignored** - Input Signal will have no effect on how the system operates
- **Remote Disabled/Lockout** - When an open lock request is received for any lock, all requests to open will be blocked regardless of which target lock the user is attempting to open. This is the default setting.
- **Time Delay Override** - Time Delay for all locks in the system is cancelled and any lock may be opened immediately by a user. If one or more locks were in either the Delay Period or the Confirmation Window, Time Delay is canceled, and the lock can be opened immediately by a user, with open privilege, providing the correct credentials
- **Dual User Override** - Dual User requirements are ignored, allowing a single user to open a lock or access the menus

Output Signal

- **Ignored** – Output Signal will have no effect on how the system operates
- **Duress Alarm** – when a Duress Combination is entered, the output signal will send a 1 second pulse.
- **Bolt Switch State** – sends a signal indicating whether the bolt switch is secure or not

3.6 Installing, Commissioning, and System Activation

The system requires that a lock and keypad be connected through an Install or pairing activity. This can be done before or after the Keypad and Lock have been mounted to the safe. To facilitate test opening, physical fit placement, it is recommended that you physically mount the Keypad and Lock prior to setting up the system. Refer to the CenconX Installation Guide for detailed instruction on the physical mounting of the Lock and Keypad. (Document # CX004.0524)

NOTICE

- Prior to pairing/installing a lock to a keypad, the lock must be in a factory (reset) state
- Prior to commissioning the lock and keypad, the installer can press the number “1” key to open the lock. Pressing any other key will open the Pre-Commission Menu.
- It is recommended that the lock be open during the commissioning process
- The lock and keypad can be paired/installed either before or after they are physically mounted
- Refer to the CenconX Installation Guide for details on how to physically mount the lock and keypad and apply power.
- **Important!** The Commissioning of the lock/keypad involves the creation of the lock Admin user. Once created, the installer must give the Admin user PIN to the owner of the system backend database when the system is Activated.

3.6.1 Install and Commission a Lock and CenconX Keypad

Follow these steps to “INSTALL” (logically, electronically pair) a Safe Lock to a CenconX Keypad:

1. Connect the CenconX lock and keypad together as outlined in the CenconX Installation Guide
2. Power up the CenconX lock and keypad as outlined in the CenconX Installation Guide

3. If using an alarm box and external alarm, install and connect these according to instructions.
4. Press the "1" key on the keypad to verify that the lock opens and that the output signal is operational (recommended)

At this stage, you can use the keypad to access, view, and/or change a limited number of lock/keypad settings via the keypad menu. No credentials/authentication are required. These are as follows:

- Buzzer
- Keypad Backlight
- FW Update
- View FW levels of the lock or keypad
- View Serial Number (S/N) of lock or keypad

5. Press any of the keypad's keys to wake up the keypad.
6. In the keypad menu, select "Commission", then press the <return key> (←).
7. When prompted, the installer must use the keypad to enter the Admin PIN, then press the <return key> (←). Retain this PIN for later so the system database owner can setup the Admin User in the software.

3.6.2 Install and Commission a Lock and CenconX Keypad (Activation)

With the lock system now commissioned and operational, it must be connected to the Primary Dispatcher database. This process is known as Activation and can be achieved three different ways described in the following sections.

Some things to note regarding Activation:

- The Activation process can be performed either at the same time as commissioning or done later.
- Once activated, new configuration and/or static user data can be transmitted to the system via import/export process with the software database or via the mobile device.

3.6.2.1 Activation Method – Via Cable

1. Using Apexx Series software, the installer can connect a USB to the lock system's keypad and create an encrypted export file containing all the preliminary settings and configurations as well as specific lock secrets that could allow the mutual trust between this lock system and the Primary Dispatcher Database.
   Note: The installer will need to authenticate with the Admin's PIN at the lock in order to enable USB.
2. The installer provides this file to the Software Admin, who uses it to import the required information into the database.

3.6.2.2 Activation Method 2 (???)

1. The Software Admin manually enters the serial numbers of the lock(s) being activated into Apexx Series software.
2. The Software admin produces an export file, which is given to the installer.
3. Using the installer application, the installer connects to the keypad via USB and installs the required files to activate the system.
   Note: The installer will need to authenticate with the Admin's PIN at the lock in order to enable USB.

3.6.2.3 Activation Method – Via Mobile

1. The Software Admin manually enters the serial numbers of the lock(s) being activated into Apexx Series software.
2. The Software Admin can select a Mobile User and send the required installation files/information to their mobile device.
3. The Mobile User's device is used as a bridge to provide a connection between the database and the keypad/lock.

4. When on site, the installer/mobile device user wakes up the keypad, then authenticates with the Admin PIN to transfer the installation information.

3.6.2.4 Completing the Activation process

Regardless of the Activation method chosen, once the installation files/info is shared between the database and lock system and the Admin authenticates with their ID and PIN, the following steps must occur:

1. In the CenconX keypad menu, highlight "Activate Primary Dispatcher", then press the <return key> (←).
2. Select "Activate", then press the <return key> (←).
3. If using a mobile device to activate the system, select "Enter Claim Code", then press the <return key> (←).

At this point, a new randomized Admin/Master PIN will be created. This new PIN can be exported and then manually imported by the Software Admin into the software database, or if using a mobile device, the device can connect to the lock system to retrieve this information and share it with the database when the mobile device connects to the network.

3.7 Open a Lock

3.7.1 Open a Lock – CenconX Keypad

You can open a lock in the CenconX lock system by one of the following ways:

- Entering a Static ID and PIN at the keypad
- Entering a one-time-code at the keypad
- Using a mobile device with a one-time-code

NOTICE Before attempting to open a lock, observe the following:

- The lock must already be commissioned and activated in the database
- A Software User must create a Lock User in the software backend
- The Lock User must be assigned to the lock(s) you are attempting to open
- If using a Mobile device, ensure it is provisioned in the database and that the mobile device is assigned to the user who is attempting to open the lock

3.7.2 Open a Lock – Static ID and PIN

You can open a lock using a Static ID and PIN at the keypad by doing the following:

1. Wake up the CenconX keypad by pressing the <return key> (←).
2. Use the numeric keys to enter your Static User ID and PIN, then press the <return key> (←).
3. If in Dual User mode, you will be asked to provide a second set of valid credentials.

Once all opening conditions have been satisfied (Dual User, Time Delay, etc.), the lock motor will activate and lock access will be granted.

3.7.3 Open a Lock – One Time Code at the Keypad

You can open a lock using a One Time Code at the keypad by doing the following:

1. Wake up the CenconX keypad.
   Note: if you use one of the numeric keys to wake up the keypad, this will be read as the first digit of a One Time Code.
2. Use the numeric keys to complete the entry of the One Time Code, then press the <return key> (←).
3. If in Dual User mode, you will be asked to provide a second set of valid credentials.

Once all opening conditions have been satisfied (Dual User, Time Delay, etc.), the lock motor will activate and lock access will be granted.

3.7.4 Open a Lock – One Time Code using Mobile Device

Refer to sections 3.12.4.2 Open a Lock (Single User mode) and 3.12.4.3 Open a Lock (Dual User mode)

3.7.5 Open a Lock – Remote Disable

With the application of the Alarm Box, the opening sequence can be disabled by asserting a signal on the Alarm Box. The signal may come from an external alarming system that could be connected to this lock to prevent it from opening.

Please observe the following while using the Remote Disable:

- The Remote Disable assertion will not block users from accessing the menus on a Display Keypad
- The signal must be asserted prior to the user authentication for it to be recognized by the system
- Duress combinations will still trigger the alarm signal, even if Remote Disable is asserted
- A Keypad with a display will show 'Lock #x NOT open' when the Remove Disable is asserted. The 'x' would be replaced by a lock that is targeted to be opened
- A non-Display Keypad will indicate that the opening of the lock has failed if an opening is attempted with the Remote Disable asserted. The Keypad will produce 3 low beeps accompanied by 3 **RED** LED flashes

3.8 Change Time/Date/DST

Follow these steps to change the Time/Date/DST on a CenconX Keypad:

1. Enter an Authorized User ID and Combination.
2. Navigate through the Main Menu and select "Time/Date".
3. Select one of the follow sub-menu options:
    a. "Time Format" – Choose between 24Hr and 12Hr
    b. "Date Format" – Choose between yy_mm_dd, mm_dd_yy, and dd_mm_yy
    c. "Set Time/Date" – Input the time and date with the number pad
    d. "Observe DST" – Select either Enable or Disable
4. "Success updated" appears onscreen. The Keypad will beep three times and flash a **GREEN** LED once complete.

Note: If the Time/Date is not set after a prolonged power outage, access time lock schedules cannot be enforced and may result in the inability to open the lock until the Time/Date is set.

3.9 Battery Levels

The battery level of the CenconX keypad will be one of the following states (listed from highest to lowest power):

- Good
- Low Battery
- Critical Battery
- Dead Battery

To check the battery level at the CenconX keypad, do the following:

1. Enter an Authorized User ID and Combination.
2. From the Keypad display Main Menu, select "System", then press the <return key> (←).

3. Select "Sys Info", then press the <return key> (←).
4. Select "Keypad", then press the <return key> (←)
5. Select "Batt Level", then press the <return key> (←) to view the battery level.

If using a mobile device, the Battery Level will be retrieved from the lock and sent to the software backend whenever the mobile device is used to operate the lock.

Note: If the Keypad is using an AC Adapter, then the battery level indicator will always be at "Line Powered".

3.9.1 Low Battery Warning

Low Battery Warnings indicate that the batteries need to be replaced immediately to ensure continued and safe operations of the device.

3.9.1.1 Low Battery Warning – Display Keypad

Keypads with a display will provide the following indicators as a Low Battery Warning:

- Upon wake-up, the Keypad will emit 2 high beeps and 2 **GREEN** LED flashes, followed by 2 low beeps and 2 **RED** LED flashes.
- The screen will display "Low Battery" on wake-up and at the end of an open sequence.

3.9.2 Critical Low Battery Warning

Critical Low Battery Warning indicates that the system will not respond to any other commands until the battery is replaced.

The CenconX Keypad will provide the following indicators as a Critical Battery Warning:

- Upon wake-up, the Keypad will emit 3 high beeps and 3 **GREEN** LED flashes, followed by 3 low beeps and 3 **RED** LED flashes.
- The screen will display "Critical Low Battery" on wake-up.

3.9.3 Replacing Batteries in Critical Low Battery State

When in Critical Low battery state, and the batteries are within the secure container, the system must do a restart when a battery (or batteries) is applied to the Keypad. The restart can be forced by pressing the # key when the new battery is applied to the Keypad. The safe should be opened and the inside batteries replaced.

Note: If the Time/Date is not set after a prolonged power outage, access time lock schedules cannot be enforced and may result in the inability to open the lock until the Time/Date is set.

3.10 View Audits

Note: This function is not UL evaluated.

Audits can be viewed directly on the CenconX Keypad display screen. A maximum record of 50 events can be viewed on the Keypad display screen. The Keypad will display:

- The code indicating the Event/Action
- The Date and Time of the Event/Action
- The ID of the User who performed the Action

To view audits from the display, the User must have Audit Privileges enabled. The Admin and Manager User IDs are granted Audit Privileges by default.

Follow these steps to view Audits on screen:

1. Enter an Authorized User ID and Combination.

2. Navigate through the CenconX Menu and select "Audits".
3. Navigate through each Audit transaction with the Arrow buttons on the Keypad.

To view the codes defined for each audit, please refer to Appendix A.

3.11 Locks

Certain functions and commands can be carried out on the Keypad without the use of software.

3.11.1 Physical Installation of a Lock

For information and steps on how to physically install a safe lock to a system, refer to the CenconX Keypad & Lock Installation Guide (Document # CX004.0524).

3.11.2 Reset a Lock

Each CenconX safe lock can be reset to factory defaults. A lock reset can be done one of two ways:

1. Master Reset via the Keypad (both Display and Non-Display versions)
2. Mechanical Reset via the Reset Box (Item/Order # ?????).

When a lock is reset:

- The Master Combination is reverted to the default (1-2-3-4-5-6-7-8).
- All Managers and Standard Users are deleted.
- All System and lock settings will be reset to their default.
- All locks will be uninstalled and unpaired from any Keypad.

Two items will not be deleted:

1. Audits.
2. Open count.

3.11.3.1 Master Reset – CenconX Keypad

Note: A Lock Reset can be performed at the keypad by the Admin user.

Follow these steps to reset a safe lock on a CenconX Keypad:

1. Enter an Authorized User ID and Combination.
2. Navigate through the Main Menu and select "System".
3. Select "Locks" from the sub-menu.
4. Select "Reset".
5. Select "Yes" to confirm.
6. "Confirm Reset" will appear on screen. Select "Yes". "Reset Success" will appear on screen when the lock is reset.

When the Master Reset is successful, the keypad will respond with 3 short beeps and 3 **GREEN** led flashes

3.11.3.3 Mechanical Reset

A mechanical reset can be done utilizing the Reset Box (Item/Order # ?????). Refer to the Reset Box User Guide (Document #~~7039.0521~~) for more information. The Mechanical Reset is not UL evaluated.

It is important after the reset operation, that the Reset Box is disconnected from the operational lock. If the safe door is closed with the reset box attached, the lock will no longer open.

Note: The number of resets that can be performed using the Reset Box is pre-determined

3.11.2 Open a Lock During Time Delay

3.11.2.1 Open a Lock During Time Delay – Display Keypad

Follow these steps to open a safe lock during a Time Delay on a CenconX Keypad:

1. Using the Keypad, input the User ID and Combination.
2. "Lock # Start Delay" will appear on screen and provide timer feedback. The type of feedback depends on the setting for count feedback (the time may count down, up, or only show time remaining). A key must be pressed to check the Time Delay status.
3. Once the Time Delay period expires, "Lock # status Confirm" appears on screen.
4. If a lock is in the confirmation window, it can be opened. Press a key to exit the Time Delay Status.
5. Input the User ID and Combination.
6. From the sub-menu, select "Open Lock".
7. The lock will open, and the screen will display "Lock Open". After a few seconds, the lock will close.

3.11.3 Cancel a Time Delay

If desired, a Time Delay period can be cancelled. Some things to know when cancelling a Time Delay:

- The opening activity is cancelled.
- The Time Delay Period will end, and there will be no Confirmation period.
- The Lock cannot be opened.
- Re-authentication will initiate a new Time Delay period.

3.11.3.1 Cancel a Time Delay – CenconX Keypad

Follow these steps to cancel a Time Delay on a CenconX Keypad:

1. While a safe lock is currently in a Time Delay, press the <return key> (←) on the Keypad.
2. Input a valid User ID and Combination.
3. From the sub-menu, select "Cancel TD".
4. "Lock Dly Cancelled" will appear on screen and the Keypad will beep three times and flash a **GREEN** LED.

3.11.4 Allow Time Delay Override

For a user to execute a Time Delay Override, the lock must be configured to allow Time Delay Override. The Time Delay Period and Confirmation Window period must be set.

To allow the Time Delay Override feature, a Software Admin or Manager User must enable the feature for the specific lock.

3.11.5 Open Lock During Time Delay Using Override with Combo

3.11.5.1 Open Lock During Time Delay Using Override with Combo – CenconX Keypad (???)

Follow these steps to Open a lock during a Time Delay using Override on a CenconX Keypad:

1. Using the Keypad, input the User ID and Combination.
2. "Lock 'N' Start Delay" will appear on screen where 'N' represents the lock number. The screen will then provide timer feedback.
3. There is no continuous feedback. A key must be pressed to check on the Time Delay status. When a key is pressed, the Keypad will display the feedback for the 'most urgent' lock.
4. Press a key to exit the Time Delay Status screen.
5. Input the User ID and Combination.
6. From the Time Delay Menu, select "Open Lock".
    a. For multi-lock systems, select the corresponding lock number on the keypad

b. If the selected lock has Time Delay and Time Delay Override enabled, and the User has Time Delay Override w/ Combo privileges for the lock, then the lock will open

3.12 Mobile App – dormakaba Safe Locks Mobile Application

The following section describes how to set up and use the dormakaba Safe Locks Mobile Application and use a mobile device to interface with the CenconX lock system.

3.12.1 Mobile App – Registration Setup

After downloading and installing the mobile app, you must complete the setup and register your mobile device with the software backend.

Note: To proceed, you will need an ID and temporary PIN. This must be provided by the software administrator prior to completing the mobile registration process.

1. Open the mobile app.
2. On the Registration "Setup" screen, under "Device ID", copy the device ID number and give it you your software administrator. The Software admin will use this information to enroll your mobile device in the software.
3. On the Registration "Setup" screen, enter your network data by choosing from one of the following two methods:
    a. Network setup using QR code:
        i. Click the "scan a QR code" button.
        ii. When prompted, allow the app to access your mobile device's camera.
        iii. Align the target frame with the QR code. After a few seconds, the application will automatically detect and process the QR code.
        Note: this QR code will be provided by your Software Administrator when enrolling your device.
    b. Manual Network Setup:
        i. Click the "enter manually" button.
        ii. On the "Enter manually" screen, enter the URL address, Port Number, and Secret key in the fields provided. (Note: The "https://" characters will be automatically incorporated in the "URL address" field.)
        iii. When all fields are filled in, click the "continue" button.
4. Wait a few seconds for the network data to be processed and authenticated.
5. If you are prompted to, click the "update" button to update the mobile app.
6. You will now be asked to Log in to the app.

3.12.2 Mobile App – Logging In

Note: You must first register your mobile device before attempting to log in. If logging in for the first time, you will need an ID and temporary PIN. This must be provided by the software administrator.

3.12.2.1 First time Logging In

1. Open the mobile app.
2. On the "Login" screen, enter your ID and temporary PIN in the fields provided.
3. Click the "Login" button.
4. Set a new personal PIN by entering a new pin in the "Enter a new PIN" field.
5. Confirm your new PIN by entering it again in the "Confirm PIN" field.
6. Click the "Change PIN" button.
7. On the "Setup" screen, read over the **terms of use** and **privacy policy** by clicking their respective names.
8. Click the check box ☑ to accept the terms of use and privacy policy. **Note:** this is required to continue.
9. Click the "continue" button.

10. If desired, click the check boxes ☑ to consent to using/sharing analytics. **Note:** these are optional, and not required to continue.
11. Click the "continue" button.
12. You will be directed to the "Find lock" screen.

3.12.2.2 Logging In (standard)

1. Open the mobile app.
2. On the "Login" screen, enter your ID and PIN in the fields provided.
3. Click the "Login" button.
4. You will be directed to the "Find lock" screen.

3.12.3 Mobile App – Navigating the mobile app

Located on the bottom of the screen are the following four buttons that, when pressed, will take you to screens containing all of the tools you'll need to operate the lock system using your mobile device.

These screens are described in the following sections.

3.12.4 Mobile App – "Find Lock" Screen

The "Find Lock" Screen allows you to use your mobile device to connect to and open locks via Bluetooth.

Note: Your mobile device's Bluetooth settings must be enabled to find and open locks.

Note: Before attempting to "Find" a lock, ensure the CenconX keypad is awake by pressing one of its buttons.

3.12.4.1 Finding a Lock

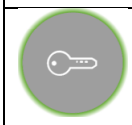
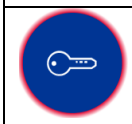
1. Open and log in using the mobile app.
2. Navigate to the "Find Lock" screen by clicking the Find lock icon.
3. When prompted, allow the app to access the device's location.
4. If using an Android phone > When prompted, allow the app to send you notifications.
5. The app will scan for available locks in your area. When the scan is complete, a list of locks will appear on the screen. You can scan for locks again at any time by pressing the "refresh" button.

3.12.4.2 Open a Lock (Single User mode)

You can open one of the locks that appears in the "Find Lock" list by doing the following:

1. Click on one of the locks on the "Find Lock" screen.
2. On the "Lock details" screen, the user can open the door in one of two ways:
    a. Key Button:
        i. Press the Key Button to open the lock via Bluetooth.
    b. Manual (Opening code):
        i. If you do not have a valid opening code, press the "request opening code" button.
        ii. Press the "show opening code" button. The app will display the 9-digit opening code.
        iii. Using the CenconX keypad, enter the 9-digit opening code,
        iv. Press the <return key> (←) on the keypad.

Note: The appearance of the Key Button will change depending on a variety of factors. See chart below for Key Button appearance vafghfgh

	Key Button description
	• Disabled Key Button
	• Disabled Key Button • Green outer ring indicates the lock is open • Green ring remains until the close code is successfully retrieved
	• Enabled Key Button • Red outer ring indicates error opening lock • Red ring will flash 3 times
	• Enabled Key Button

3.12.4.3 Open a Lock (Dual User mode)

You can open one of the locks that appears in the "Find Lock" list by doing the following:

1. Click on one of the locks on the "Find Lock" screen.
2. On the "Lock details" screen, the user can open the lock in one of two ways:
    a. Key Button:
        i. Press the Key Button to open the lock via Bluetooth.
    b. Manual (Opening code):
        i. If you do not have a valid opening code, press the "request opening code" button.
        ii. Press the "show opening code" button. The app will display the 9-digit opening code.
        iii. Using the CenconX keypad, enter the 9-digit opening code,
        iv. Press the <return key> (←) on the keypad.
3. The app will prompt you to enter a second credential. A secondary credential can be presented in one of two ways:
    a. Second mobile device:
        i. A second user can complete the opening sequence by using the Key Button on their own device, or by manually entering an opening code as described previously.
    b. Same mobile device:
        i. Press the "use this phone" button.
        ii. Hand your phone to the second user and have them enter their ID and PIN in the fields on the "Login second user" screen.
        iii. Second user > press "Login" button.

3.12.4.4 Close a Lock

Once a lock has been opened, the user can close the lock by doing the following:

1. On the "Lock details" screen, when the lock is in the open state, press the "enter close code" button.
2. In the close code window, the user can choose to close the lock by one of two ways:
    a. Retrieve close code:
        i. Press the "retrieve" button.
        ii. Press the "ok" button once the application successfully obtains the close code from the lock.
    b. Manual close code entry:

i. Tap the screen on the close code entry field > " _ _ _ _ _ _ "
ii. Observe the close code that is displayed on the CenconX keypad's display screen.
iii. Enter the close code using your mobile device's keypad.
iv. Press the "ok" button.

3. If the system has been configured to require a photo of an additional close seal/lock, do the following:
   a. If prompted, allow the app to access your mobile device's camera.
   b. Point your device's camera at the close seal/lock, then press the button to take a picture. (**Note:** you can use the A button to turn the camera flash to auto, on, or off)
   c. Press the "save photo" button, or press the "retake" button to attempt a better photo, then repeat steps 3a to 3c.
   d. Press the "ok" button to confirm that the photo has been saved.

3.12.5 Mobile App – "Locks" Screen

The "Locks" Screen contains a list of all the locks that the user has permissions to open.

Information on each of the locks in this list can be accessed by simple clicking on the lock name.

Initially, if the user does not have any permission to open any locks, the "Locks" screen will appear empty.

If the user does have permission to open locks, all locks will appear on this page listed in route order from top to bottom.

In some cases, a lock will appear with a pending upload or download icon indicating that there is new information that needs to be sent to or from the lock.

Upon clicking a lock, the user will have access to the following details:

- **Map**
  - Provides a map showing the location of the lock.
  - The location of the lock is indicated by a large, **RED** pin marker.
  - To enlarge the map, click the "Fit to screen" icon.
  - To return to the details screen, simply click the blue arrow in the top-left corner.

- **Lock Name**
  - Provides the name of the lock and the lock number (determined by its order in the route)

- **Address**
  - Provides the address of the lock (street, city, postal code, etc.)

- **Coordinates**
  - latitude and longitude decimal degree coordinates away from your current location (as defined in the software)

- **Distance from your Current Position**
  - Provides a measurement of the physical distance between the user and the lock.

- **Synchronization with the server**
  - Will notify the user of any pending uploads/downloads.

- Anything that needs to be synchronized will appear in **RED**.
  - To update the firmware, click the Sync button at the bottom of the screen to navigate to the "Sync" screen.

- **One Time Code**
  - Presents the One Time Code that can be used open the lock.
  - The One Time Code will appear in one of the following states:
    - **Hidden** (the code will appear as " ****** ")
    - "Expired" (code can no longer be used because of time limit)
    - "Cancelled" (the dispatcher has cancelled the one time code)
    - "Consumed" (when the code has already been used)
    - "Too far away" (when geofencing is enabled for that lock)

- **Firmware**
  - Provides the firmware version of the Lock and Keypad
  - If the firmware version for either the Lock or Keypad is out of date, it will appear in **RED**.
    - To update the firmware, click the Sync button at the bottom of the screen to navigate to the "Sync" screen.

While viewing a particular lock, if you are close to the lock's location, a banner will appear notifying you that the lock is close by. When this banner appears, you can either click "**DISMISS**" to have the banner disappear, or you can click "**OPEN IT**" to navigate to the "Lock Details" screen.

3.12.6 Mobile App – "Sync" Screen

Sync

The "Sync" Screen is used for mobile device synchronization with the server.

It contains a list of all pending downloads and uploads for all data pertaining to the locks associated with the user.

If there isn't any data that needs to be synchronized, the "Sync" screen will be in an empty state.

When the user needs to perform a synchronization of any kind, the app will indicate this with a red dot above the Sync, download, or upload icons.

If there are network issues, click the "**REFRESH**" button to check for pending downloads/uploads.

Once a safe network connection is established, the pending download and upload queues will be processed.

3.12.6.1 Mobile App – Firmware updates

Unlike the other download/upload types, device firmware updates are not automatically processed and must be acknowledged by the user before processing. To update lock and keypad firmware using the mobile app, do the following:

1. Click the Sync button at the bottom of the screen.
2. In the list of pending downloads, click the pending firmware data package.
3. In the "New firmware available" window, click the "**UPDATE**" button.

3.12.7 Mobile App – "Settings" Menu


Settings

The "Settings" menu contains a variety of tools and information to help the user of the mobile application.

Simply click on "Settings" menu icon at the bottom of the screen, and then click on one of the following:

- **Language**
  - The "Language" setting allows users to change the mobile applications presentation language.

  To change the language, click the language of your choice, then click the blue arrow ← in the top-left corner to return to the main "Settings" menu.
- **PIN**
  - The "PIN" setting allows you to change the personal PIN of the user who is currently logged in to the app.
  - To reset your user PIN, do the following:

    1. Enter your PIN in the "Enter PIN" field provided.
    2. Press the "confirm" button.
    3. Enter a new user PIN in the "New PIN" field provided.
    4. Confirm the new user PIN by entering it again in the "Confirm PIN" field provided.
    5. Press the "Change PIN" button.
- **Privacy Policy**
  - Clicking "Privacy Policy" will display the terms of use for the mobile app. Once you're finished reading, click the blue arrow ← in the top-left corner to return to the main "Settings" menu.
- **Consent**
  - The "Consent" settings page allows you to set or adjust your consent to the terms of use, privacy policy, or the collecting of app based analytical data.
  - Click the check box ☑ to consent, or leave blank ☐ to remove consent.

  Note: The user must consent to the terms of use and privacy policy in order to remain logged in and continue to use the app.

  When finished, click the blue arrow ← in the top-left corner to return to the main "Settings" menu.
- **? Help**
  - Contains useful information to assist you in using the CenconX Lock System including links to websites, documentation, and videos.
- **Reset**
  - Clicking "Reset" will allow the user the ability to reset the application by deleting all saved app data. To consent to a complete app Reset, click the check box ☑ to consent, then click the "Reset" button.
- **Log out**
  - Clicking "Log out" will log out the current user and the app will navigate to the "Login" screen.

4 Keypad replacement

A new Keypad can be installed into a system to replace a damaged unit. This operation can be completed by an authorized user. An Audit record will be recorded to the lock to indicate which user installed the new keypad. Once paired, the system returns to regular operation.

A CenconX keypad can be replaced by one of the following users:

- A lock-recognized Static PIN User can enter their ID and PIN to accept the new keypad
- A One Time Code can be dispatched to a user and entered to accept the new keypad

5 Apexx Series Software

Note: The Apexx Series Software is not UL evaluated.

Apexx Series Software is a multi-faceted client that manages Users, Schedules, and Systems to be used in concert with both Apexx and CenconX safe locks systems. This section outlines certain software functions. Review the software online help by pressing F1 within the client for information not outlined here. Also review the Apexx Software Installation Guide (Document #802.0124) for basic installation steps.

The best and most comprehensive guide to using the Apexx Series Software is the built-in help menu that can be accessed by pressing F1 on your keyboard when running the software client. This section is meant to only highlight some of the software tools.

5.1 Firmware Update

When a new firmware version is available, these files will be available to registered Apexx Series Software users.

Using the Apexx Software client, keypad and lock firmware can be updated. There are four firmware files that can be updated:

- Bootloader for the Keypad
- Application for the Keypad
- Bootloader for the Lock
- Application for the Lock

Important: To update the Lock and Keypad Firmware to the newest version, the Manager user will require the following:

- A PC with the Apexx Series Software client installed
- A USB-to-Mini-USB Cable

The version of firmware currently on your device can be viewed in the CenconX Keypad menu, the dormakaba Safe Locks mobile application, or by using a PC with the Apexx Series Software client installed.

- **CenconX Keypad** – to view the lock and keypad firmware levels, navigate through the keypad's menu and select "System", then select "Sys Info" from the sub-menu and select "FW Level".
- **Mobile Application** – the "Locks" screen on the mobile app shows all system details, including the current firmware version of each device. To update your firmware using the mobile app, see section 3.12.6.1 Mobile App – Firmware updates.
- **Apexx Series Software** – you can view the firmware levels of all keypads and locks in your selected region by visiting the "Dashboard".

Follow these steps to update the lock and keypad firmware:

Important: when updating FW on a system mounted to a safe, always ensure the safe door is open prior to the beginning of the FW update process.

1. Connect the Keypad to the PC by doing the following:
    a. Plug the USB-connector end of the cable into the USB Port of the PC
    b. Plug the mini-USB end of the cable into the mini-USB port on the Keypad
2. On the Keypad, enter a valid User ID and the corresponding combination.
3. From the Apexx Series Software Main Menu, select "Locks" > "Loock Systems".
4. On Apexx Software's "Lock System Search" screen, open the CenconX lock system you wish to update.
5. On the lock system details screen, locate and click the "Update Firmware" button.
6. In the "Firmware Update" window, use the drop-down lists to select your connection type (choose "USB"), and your Firmware file. If your firmware file does not appear in the list, navigate to the "Firmware Management" screen to manage your firmware files.
   Note: refer to the Apexx Series Software's help menu under "Firmware Management" for more details on managing firmware for Apexx and CenconX keypads and locks.
7. Click the "Update Firmware" button. The Firmware Update process will begin, and will conclude after several seconds (the time will vary depending on the size of your lock system).

5.2 Audit Reports

Follow these steps to perform an Audit report using the Apexx Series Software client:

1. From the Apexx Series Software Main Menu, select "Reports" > "Audit Report".
2. Set all of your report criteria by doing the following:

Date Range - the Audit Report will include Audit events that fall between the selected "From" and "To" dates.

- Click the "Date Range" check-box
- Use the interactive Calendars to select a "From" and "To" date. Use one of the following methods:
    - Click the Calendar symbol to open the interactive calendar. Use the arrows to navigate to the appropriate month, then click the calendar to select a specific day for both your "From" and "To" dates.
    - Click the "From" text field, then type a start date (format is Month/Day/Year), then click the "To" text field and type an end date.

Event - the Audit Report will include only Audit events of the type selected by the user.

- Click the "Event" check-box
- Use the slider icons to select one or more Events (event type) from the list provided. An event type is selected when the slider is blue and to the right . An event type is unselected when the slider is grey and to the left .

Devices / Lock Systems - the Audit Report will include only Audits from the selected devices

- Click the "Include all devices" check-box, or

- Click the  check-box next to one or more of the listed devices to include them in the report.

3. Once your Audit Report criteria has been set, click the "Run Report" button.

Appendix A: List of Audits

The following is the list of audit definitions and the codes associated with them.

Table 7 - Audits

Audit Code	Audit Definition	Audit Code	Audit Definition	Audit Code	Audit Definition
1	Power up	29	Battery Critical	49	Holiday Changed
2	RTC Time Set	30	User Mode Changed	50	Observe DST Changed
3	Lock Reset w/ Reset Box	32	Credential Mode Changed	51	Lock Commissioned
4	Lock Reset w/ Master combo	33	PC Link Enabled	52	Lock Activated
5	Lock Installed	34	PC Link Disabled	53	Wrong Combination Tried
8	Time Delay Values Changed	35	RTC Time Reset		
9	Audits viewed Via Keypad or Software	36	Battery Good		
10	Lock Opened	37	Lock Firmware Update Started		
11	Lock Uninstalled	38	Keypad Firmware Update Started		
14	User Added, Modified, or Deleted	39	Time Delay Override Enabled		
17	Keypad Reinstalled	40	Time Delay Override Disabled		
18	Bolt Opened	41	Auto Open of Primary Lock		
19	Bolt Closed	42	Configure Auto Open Setting		
20	Battery Low	43	Configure Input Signal Setting		
21	Time Delay Overridden via Combo	44	Remote Time Delay Override		
22	Wrong Try Penalty Started	45	Remote Force Single User Mode		
23	Duress Alarm	46	Require Combo Change		
26	Open attempted, remotely disabled	47	Schedule Changed		
27	DST Table updated	48	Schedule Assignment Changed		

Appendix B: CenconX Series Release Notes

Software		
Version Number	**Release Date**	**Details**
x.x.x.x (Initial Version)		

Keypad Firmware		
Version Number	**Release Date**	**Details**
x.x.x.x (Initial Version)		

Keypad BLE Firmware		
Version Number	**Release Date**	**Details**
x.x.x.x (Initial Version)		

Lock Firmware		
Version Number	**Release Date**	**Details**
x.x.x.x (Initial Version)		

Door
Hardware

Electronic
Access & Data

Mechanical
Key Systems

Lodging
Systems

Entrance
Systems

Interior Glass
Systems

Safe
Locks

Service

dormakaba USA
1525 Bull Lea Rd.
Lexington, KY 40511

T: 1 888 950 4715
www.dormakaba.com

dormakaba.com

CX003.0524 10-24