ALLEGION™

SCHLAGE®

ENGAGE

User's Guide 8.1.0

About this document

➔ **Note:** This User Guide is designed for the Administrators of ENGAGE™ and product training teams. Administrators who intend to use Allegion Physical Access Control Software (PACS) partners to manage their property should consult their sales associate.

Table 1.1 Revision History

Revision	Date	Comments
	June 2026	Added site approval information.
	March 2026	Added Device Group management and sync information.
	20 MAY 2025	Added **Bulk Import Users** feature information.
	26 SEPT 2024	Added starting badge ID feature information
	06 SEPT 2023	Added mobile credential licensing feature information.
	15 MAY 2023	Removed “Introduction to ENGAGE Technology” section Updated mobile OS requirements
	16 FEBRUARY 2023	Added information about notes field for Users. Added PACS section.
	27 JANUARY 2023	Updated no-tour master credential information.
	30 MARCH 2022	Updates to: ENGAGE 8.1.0 for MIFARE DESFire EV3 support and other product updates
SES20171127F	20 APRIL 2021	Updates to: ENGAGE 7.6.0 for Mobile Credential No-Tour functionality and product updates
SES20171127E	31 MAY 2020	Reformatted doc. ENGAGE 7.5 with updates to: Mobile Credentials Security Updates
SES20171127D	07 DEC 2018	Updates to: ENGAGE 6.1.3 MT20W USB Direct Connect
SES20171127C	15 AUG 2018	Updates to: ENGAGE 6.1.1 Device Groups
SES20171127B	01 AUG 2018	Updates to: ENGAGE 6.1
SES20171127A	28 NOV 2017	Initial release: ENGAGE 6.0

Copyright

©2026 Allegion All rights reserved. SCHLAGE is the property of Allegion. All other brand names, product names, or trademarks are the property of their respective owners.

Contents

ii About this document
ii Copyright

5 Introduction
5 Purpose
5 System and Product Revisions
6 Customer Support
6 Terms and Definitions
7 ENGAGE or PACS Managed Properties
7 Lock Function Definitions

8 Overview of ENGAGE Enabled Products
8 LE and LEB Mobile Enabled Wireless Mortise Locks
9 NDE80, NDEB, and NDEB Si
10 Control Mobile Enabled Smart Lock
11 XE360™ Mobile Enabled Wireless Locks
12 CTE Controller with MTB Mobile Enabled Reader
13 MT20 Credential Enrollment Readers
13 MT20W Credential Enrollment Readers

14 Wi-Fi Network Requirements

15 Best Practices and Things to Remember
15 ENGAGE System Set-up
15 ENGAGE Device Set-up
16 Control Mobile Enabled Smart locks
17 Factory Default Reset
17 Moving Devices Between ENGAGE Accounts
17 Dual Technology Credentials
17 Firmware Updates

18 Daily System and Other Operations
18 Assign New Access
18 Assign New Access (No-Tour)
19 Clearing Access Assignments on Existing Credentials
20 Resident Move Out Processes
22 Remove User and Access and Salvage Credential
22 Reusing a Credential
22 Delete User Access Rights
22 Deleting Devices
23 Retrieving Audit Data from Devices
23 Device Wi-Fi Network Setup
23 Synchronization
23 Setting Device Date and Time
24 Control Mobile Enabled Smart Lock Jump Start Process
24 Managing Devices in Existing Device Group and Synchronization (No Tour)
25 Device Group Segmentation and Synchronization (No Tour)

26 Firmware Updates
26 Automatic Updates
27 Manual Firmware Updates at the Door
27 MT20W Firmware Updates via the Desktop App

28 Web Application
28 Introduction
28 Supported Web Browsers
28 Interface Reference
29 Create Account
30 Log In
31 My Profile
31 Create Site
34 Users
49 Devices
60 Device Groups
62 Schedules
66 Holidays
70 Audits
72 My Team
74 Global Settings
75 Credentials
77 Device Defaults
83 Reader Defaults

84 Mobile Application
84 Introduction
84 Supported Devices and Requirements
85 Log In
85 Main Menu
85 Devices
86 Delete Device
87 Wi-fi Settings
92 Users
93 My Team
94 Sites
97 Updating Device Firmware

103 No-Tour Feature
103 Overview
104 Enable No-Tour Feature
105 Update Credential for No-Tour Programming
107 No-Tour Temporary Maintenance Access

109 PACS Managed Properties
109 Introduction
109 Users
113 Credentials

117 Credentials
118 Enroll Smart Credentials in Bulk
119 Enroll a Smart Credential Individually
120 Enrolling a Credential at a Door
124 Physical Credential Reuse: Best Practices
125 Mobile Credentials
129 Schlage Mobile Access Application
131 Replace a Credential
133 Using Master Credentials
138 Credential Functions

139 Control Mobile Enabled Smart Lock Installation and Commissioning
139 Introduction
139 Prepare to Install the Device
140 Install the Device
142 Factory Default Reset (FDR)
143 Construction Mode
144 Commissioning

147 XE360 Devices Installation and Commissioning
147 Introduction
147 Commissioning in the box
147 Prepare for Installation
148 Install the Device
150 Factory Default Reset Overview
151 Lock Modes
152 Commissioning the Device

155 LE and LEB Devices Installation and Commissioning
155 Introduction
156 Prepare for installation
157 Verify Success of Installation
158 Factory Default Reset
158 Construction Access Mode
160 Commissioning

163 NDE80 and NDEB Devices Installation and Commissioning
163 Introduction
163 Prepare to Install the NDE80 or NDEB Wireless Locks
164 Install the Device
166 Factory Default Reset Overview
167 Create a Master Construction Credential
168 Commissioning the Device

171 CTE Controller and MTB Readers Installation and Commissioning
171 Introduction
171 Prepare to Mount the Device
172 Mount/Install the Devices
174 Factory Default Reset (FDR) Overview
175 Construction Mode Overview
177 Commissioning the CTE
182 Configuration Cards

183 MT20W Installation and Commissioning
183 Introduction
183 MT20W initial power up
183 Commissioning the MT20W
186 Installing the ENGAGE PC Desktop Application
187 MT20W Factory Default Reset
187 MT20W Firmware
191 MT20W USB communication mode
193 MT20W Wi-Fi communication mode (Optional)
195 MT20W LED/Beep Indications

196 MT20 Installation and Commissioning
196 Introduction
196 Initial Power Up
196 Enrolling a Credential
197 MT20 Output Formats

198 Troubleshooting

199 Frequently Asked Questions

202 Appendix A: Capabilities by Property Role

203 Appendix B: ENGAGE Training

204 Appendix C: Credential Functions

Introduction

Purpose

This document provides descriptions of the ENGAGE™ Technology and family of ENGAGE supported products used by ENGAGE Managed Properties.

With details on the following:

- How to set up an account using the ENGAGE Technology web application.
- How to set up and commission ENGAGE enabled devices.
- How to create sites, create users, add devices, assign credentials, etc.
- With links to training videos, frequently asked questions, and things to remember.

System and Product Revisions

Table 3.1 ENGAGE Enabled Devices and Revisions		
System	**Revision Level**	
ENGAGE Software	8.1.0	
ENGAGE Mobile Application	**Mobile App**	**Mobile Device OS**
Android	4.7.33	OS 11 (API 30) or newer
iPhone	3.10.0	OS 15 or newer
Locking Devices		
Control Mobile Enabled Smart Locks	04.10.01	
Control	03.11.01	
LE Wireless Mortise Locks	01.11.04	
LEB Wireless Mortise Locks	03.09.09	
NDE80 Wireless Cylindrical Locks	02.16.03	
NDEB Wireless Cylindrical Locks	03.09.09	
CTE Single Door Controllers	01.08.04	
Credential Readers and Controllers		
RMRU	01.03.06	
MT20W	40.05.00	
MT20	39.00.00	

The latest firmware and software versions are available on the ENGAGE Support Resources website. When updates are available, the latest firmware release notes are provided here for additional details.

➔ **Note:** Allegion strives to provide the best products and service for our customers and will update firmware and software periodically. As a result of periodic updates, your system or devices may be at a newer revision level than represented in this document.

✸ **BEST PRACTICE:** Periodically check for new versions of mobile applications and firmware. Mobile applications may not automatically update.

Customer Support

Website	ENGAGE Support Resources
Document Library	ENGAGE Document Library
Email	engage.techprodsupport@allegion.com
Phone	1.877.671.7011 then option 2, option 2 Monday – Friday from 8 am to 8 pm EST, closed holidays

Terms and Definitions

Terms

Bluetooth: An open wireless technology standard for transmitting/exchanging data between fixed and Mobile devices over short distances. Operates in the 2.4Ghz range shared with Wi-Fi.

Credentials: Authorization for access. These can be physical cards and FOBs, or they can be Mobile, or NFC enabled using a Mobile device.

Commissioning: Commissioning a device enrolls the device into ENGAGE, defines the device name, and prepares the device for later setup steps.

Mobile Credential: A credential stored on a Mobile device. Requires the Schlage Mobile Access application and site administration assignments

Mobile Device: The device carried by the user. May be an iPhone or Android or Tablet.

NFC: Near Field Communication

PACS: Physical Access Control Software (PACS) is property management software provided by others.

Site and/or Property: The term 'site' is used interchangeably with 'property' throughout this document, and both the web and Mobile applications.

Sync: Mobile device communication with a device. This updates all settings in the device and uploads the latest audit information into ENGAGE

Wi-Fi: Wireless local area network technology for connecting computers and electronic devices to each other and to the Internet. Wi-Fi is an abbreviation for wireless fidelity.

Connect Data Rate: A typical router setting. IT professionals use this setting to force a minimum data rate for each device to associate with the Wi-Fi access point to not allow slow talkers to join – improves overall Wi-Fi performance.

Notes, Cautions and Warnings

➔ **Note:** A Note is a helpful hint to help to understand how items may be related or used effectively. If a Note is not followed some features may not work as intended.

CAUTION: A Caution is a topic that may or may have unintended consequences. If a Caution is not followed the system or feature may not function properly or as expected.

WARNING: A Warning is a topic that indicates the system won't work as intended. If a Warning is not followed the system or feature will not function properly or as intended.

ENGAGE or PACS Managed Properties

Administrators will need to decide which type of Access Control management system they will be using with the ENGAGE enabled devices.

ENGAGE Managed Properties

The ENGAGE Cloud-based software and mobile applications offered by Allegion provides robust property-wide access control and monitoring.

An ENGAGE Managed Account provides these options:

- A system managed with ENGAGE Web and Mobile applications
- A self-management system operated by the property owner
- Periodic device and system updates (near real-time)
- Ability to manage up to 5000 credential assignments
- Ability to manage up to 500 door openings
    - Up to 500 doors with Schlage Control locks
    - Up to 300 doors with Schlage XE360 locks
    - Up to 100 doors with Schlage NDE/LE locks

PACS Managed Properties

Software managed by Allegion's Physical Access Control Software (PACS) provides additional features and access control and management by others.

See **PACS Managed Properties** for more information.

Lock Function Definitions

Lock Function	Description
Apartment	Door doesn't relock automatically to prevent the user from being locked out of their residence. The interior pushbutton or deadbolt will allow the resident to lock the door from the inside.
Office	Uses the interior pushbutton or deadbolt to allow the user to lock the door from the inside. Can be overridden by a valid credential.
Privacy	Uses the interior pushbuttong or deadbolt to allow the user to lock the door from the inside. While in 'Privacy mode' valid credentials are denied access.
Storeroom	The lock is secure until a valid credential is presented. The inside lever will always unlock the door.

Overview of ENGAGE Enabled Products

The ENGAGE enabled products described in this section are used with the ENGAGE technology cloud-based web and Mobile applications.

LE and LEB Mobile Enabled Wireless Mortise Locks

LE and LEB Wireless Mortise locks simplify installation by combining the lock, credential reader, door position sensor and request-to-exit switch all in one unit.

LE and LEB is ideal for office and suite entries, conference rooms, common area doors, resident units, and sensitive storage areas with a mortise door prep.

Built-in Bluetooth enables LE and LEB wireless locks to connect directly to smart phones and tablets with no need for a proprietary handheld device for set-up and configuration.

LEB versions of the Schlage Wireless mortise lock include the optional convenience of Mobile Credential access. Your Mobile phone can be used as your access credential instead of requiring a physical card or fob credential. Field upgrade kits are available to retrofit an LE to the newer LEB version.

Greenwich Addison

Fig. 4.1: LE and LEB Wireless Mortise Lock

Built-in Wi-Fi allows LE and LEB Wireless Mortise locks to connect directly to an existing Wi-Fi network enabling automated updates to lock configuration and user access to be accomplished overnight.

With the ENGAGE cloud-based web and Mobile applications, it's easy to configure lock settings, add users, and view audits and alerts from virtually anywhere.

Schlage LE wireless mortise lock product family details:

- Mortise lever lock
- Deadbolt (optional)
- Two escutcheon styles (Greenwich – Addison)
- Mechanical key override
- 4 AA Batteries required (Alkaline only)
- Wireless communication: Bluetooth and Wi-Fi connectivity
- Always allows egress
- Storeroom, Apartment, Office, and Privacy functions available
- Construction mode is based on MASTER and USER access construction credential enrollments

NDE80, NDEB, and NDEB Si

Mobile Enabled Wireless Cylindrical Locks

NDE80 and NDEB Wireless Cylindrical Locks simplify installation by combining the lock, credential reader, door position sensor, and request-to-exit switch all in one unit. The NDE product family is ideal for office and suite entries, conference rooms, common area doors, resident units, and sensitive storage areas with a cylindrical door prep.

NDEB versions of the Schlage Wireless cylindrical lock include the optional convenience of Mobile Credential access. Your Mobile phone can be used as your access credential instead of requiring a physical card or fob credential. Field upgrade kits are available to retrofit an NDE80 to the newer NDEB version.

With built-in Wi-Fi, NDE and NDEB Wireless Locks can connect directly to an existing Wi-Fi network enabling automated updates to lock configuration and user access privileges to be accomplished over-night.

With the ENGAGE cloud-based web and Mobile applications, it's easy to configure lock settings, add users, and view audits and alerts from virtually anywhere.

NDEB

NDE

Fig. 4.2: NDE80 and NDEB Wireless Cylindrical Locks

Schlage NDE wireless cylindrical lock product family details:

- Cylindrical lever lock
- Mechanical key override
- 4 AA Batteries required (Alkaline only)
- Wireless communication: Bluetooth and Wi-Fi connectivity
- Mobile Credential access
- Internal Push Button (IPB) can be configured for additional functions
- Always allows egress
- Storeroom function only (NDE80)
- Storeroom, Office, Privacy, and Apartment functions (NDEB)
- Construction mode is based on MASTER and USER access construction credential enrollments

Control Mobile Enabled Smart Lock

The Schlage Control Mobile Enabled Smart locks were designed specifically for multifamily resident doors and support for the advanced No-Tour access programming features.

The Schlage Control Smart Interconnected Lock adds a lever lock, below the deadbolt that will also retract the deadbolt on exit and allows for one-motion egress.

Residents will appreciate the security and convenience of using a Mobile phone and/or physical credentials to open their doors today.

Newer versions of the Schlage Control Smart Locks include the optional convenience of Mobile Credential access. Your Mobile phone can be used as your access credential instead of requiring a physical card or fob Credential.

Schlage Control Mobile Enabled devices began manufacture in July 2019 and the newer product can be identified by a small "White" dot on the face of the deadbolt between its "Jump Start" connections. See **Fig. 4.3: Schlage Control Deadbolt identifying mark**.

Fig. 4.3: Schlage Control Deadbolt identifying mark

BE467

FE410

Fig. 4.4: Control Mobile Enabled Smart Locks

Schlage Control Mobile Enabled Smart locks details:

- BE467 – Deadbolt
- FE410 – Interconnected cylindrical PASSAGE lever lock and Deadbolt providing single motion egress
- No mechanical key
- Battery "Jump" provided from outside (using a +9Vdc battery)
- 4AA Batteries required (Alkaline ONLY)
- Wireless Communication: Bluetooth (ONLY)
- Always allows egress
- Construction Mode is based on credential Facility Code (FC) only

XE360™ Mobile Enabled Wireless Locks

The XE360™ Series is the next generation of wireless electronic lock from Schlage. Its sleek design offers customers a solution that looks as good as it performs – at an affordable price point.

Schlage XE360 works within No-Tour or offline access control systems.

The Schlage XE360 is ready for the future with the innovative FleX Module™ that allows for communication protocol, memory, and encryption upgrades.

Credential support includes smart, Bluetooth and NFC mobile.

The XE360 Series is a complete solution purpose built for Multifamily applications. Available in tubular, mortise, mortise deadbolt and exit trim, it solves for all openings.

The open architecture design of the XE360 allows it to be managed by ENGAGE™ and other Allegion software or be integrated into popular physical access control and Proptech solutions through Allegion's PACS Alliance program. This enables customers to choose what best fits their requirements now and in the future.

Schlage XE360™ wireless lock product family details:

- Available in tubular, mortise (deadbolt optional) and exit trim
- Mechanical key override (standard)
- Up to two years battery life with 4 AA (Alkaline only)
- Wireless communication: Mobile (Bluetooth® at the door) and No-Tour
- Configurable as Storeroom, Apartment, Office, and Privacy
- Credential support includes Schlage MIFARE®, Bluetooth® and NFC mobile
- Works seamlessly with other Schlage wireless locks, including Schlage Control
- Assuming default settings, 40 actuations per day
- Use of mobile credential is dependent on availability of compatible mobile credential
- With MT20W and smart credential or mobile credential (consult your access control software provider for specific support)

Mortise and Tubular, IPB

Mortise Deadbolt

Exit Trim

Fig. 4.5: XE360 Mobile Enabled Wireless Locks

CTE Controller with MTB Mobile Enabled Reader

The CTE is an ENGAGE enabled single opening controller that allows perimeter and common area openings to be managed.

The CTE single door controller is designed for flexibility and is managed with ENGAGE web and Mobile applications.

The CTE is designed to work with Schlage multi-technology wall mounted credential readers and interface with an electrified lock, electromagnetic lock, electric strike, automatic operator, or exit device to control an opening.

When used with the Mobile Credential Enabled wall mounted readers (MTB11/MTB15), the CTE includes the optional convenience of Mobile Credential access. Your mobile phone can be used as your access credential instead of requiring a physical card or fob credential.

Fig. 4.6: CTE Controller and Wall Mounted MTB15 Reader

CTE single door controller with multi-technology reader details:

- Indoor use only (-31F to +151F)
- Externally powered: +12Vdc or +24Vdc @ 500ma
- Power-Over-Ethernet; POE, or POE+
- Wireless communication: Bluetooth and Wi-Fi
- Provides power directly to the Schlage wall mounted readers – if desired
- Powered and relay outputs available for locking devices to include: E-strikes, E-trims, mag locks, Exit Devices, Auto-Operators, etc.
- The CTE works exclusively with the Schlage MTB11 and MTB15 credential readers.
- Construction mode is based on MASTER and USER access construction credential enrollments
- All new CTEs ship with a MTB by default.

Fig. 4.7: Mobile Credential Enabled identifying symbol

Fig. 4.8: MTB11 and MTB15 Readers

Mobile Enabled Multi-Technology Wall Mounted Readers

Multi-technology wall mounted readers are designed to simplify your access control solutions and are designed to work with the Schlage CTE.

Multi-technology readers will allow a transition from existing population proximity credentials to a more secure encrypted Smart card technology without having to change readers as new technologies are available.

Mobile Enabled Multi-Technology Wall Mounted readers are identified by the Bluetooth symbol on the cover. See the symbol below:

Earlier versions of this reader, without this Bluetooth symbol will not support Mobile Credentials. Older MT and SM series readers can be easily replaced with MTB series readers to enable Mobile Credentials.

- MT20 will only read the credential access ID
- The MT20 will not write information to a credential
- The MT20 is not compatible with the No-Tour ENGAGE feature

MT20 Credential Enrollment Readers

The Schlage MT20 Multi-Technology Enrollment Reader simplifies the enrollment of smart and multi-technology credentials.

The MT20 will use the computer USB port for power and communication.

There are no installation or setup processes needed for the MT20.

The MT20 uses a Human Interface Device (HID) Keyboard Interface and requires the user to put the computer cursor in the desired data field to receive the credential data when a credential is presented.

The MT20 is an ISO 14443 and ISO 15963 contactless credential reader, and is compatible with Schlage smart credentials, PIV credentials and most proximity credentials up to 37-bits.

➔ **Note:** See **MT20 Output Formats** on page **197** for more information.

Fig. 4.9: MT20

Fig. 4.10: MT20W

A sticker on the bottom of the reader will identify the device as either MT20 or MT20W.

MT20W Credential Enrollment Readers

The Schlage MT20W multi-technology enrollment reader is designed to simplify the enrollment of multi-technology credentials. The MT20W is used to enroll credentials into ENGAGE and to read and write data to smart card credentials for No-Tour features.

When the MT20W is commissioned into an account the ENGAGE No-Tour feature is automatically enabled.

The MT20W will use the computer USB port for power and may be setup to use a locally available Wi-Fi network for communication to ENGAGE or the MT20W may use the wired USB port for communication with ENGAGE.

Schlage MT20W: Credential enrollment and programmer details:

- Powered by a standard computer USB connection, or USB power block
- Communicates with ENGAGE via local Wi-Fi network or computer USB
- Uses Bluetooth Low Energy (BLE) connection when commissioning
- The MT20W is used to enroll user credentials into the ENGAGE Managed Account and to program smart card credentials for access updates using No-tour

➔ **Note:** MT20W Reader reads Smart Cards only; it does not read prox cards.

Wi-Fi Network Requirements

- Please review the following Wi-Fi Network and supported device requirements with the local IT Administrator.
- Control Mobile Enabled Smart Locks and MTB Mobile Enabled Readers do not support Wi-Fi network connectivity while, NDE, NDEB LE, LEB, and CTE devices may be configured to utilize the local Wi-Fi network for daily updates and automated system maintenance.

Understanding and planning the Wi-Fi environment before starting an account is a good first step. Although, Wi-Fi connectivity is not required for basic ENGAGE operation, using a convenient Wi-Fi communication connection across the property and enabling nightly device updates will greatly automate and simplify daily management operations.

The local IT professional should check the Mandatory Connect Data Rate router setting when ENGAGE devices fail to associate with the local Wi-Fi network.

The **Automatic Mandatory Connect Data Rate** is a typical router setting IT professionals use to force a minimum data rate for each device to associate with the Wi-Fi access point.

The **Connect Data Rate** setting is intended to increase Wi-Fi network performance and not allow weak signal or slow data rate devices to connect.

Table 5.1 Wi-Fi Network Requirements

Required Wireless Frequency	2.4 GHz (802.11 b/g) (XE360, NDE80, MT20W, CTE/MTB reader)			
Alternate Wireless Frequency	2.4 GHz (802.11 b/g/n) (XE360, LE/LEB, NDEB and CTE/MTB reader)			
Mandatory Connect Data Rate	24 Mbps when working with NDE and MT20W XE360, NDEB, LE, LEB, CTE and RU/RM do not have any mandatory data connection data rates concerns. They adhere to the data rates defined by the 802.11 b/g/n specifications.			
Wi-Fi Network Security Types	WPA2 (PEAP)	WPA2	NOT RECOMMENDED	
	Wi-Fi SSID: case sensitive and must be EXACT USERNAME PASSWORD *	Wi-Fi SSID: case sensitive and must be EXACT PASSWORD *	WEP Wi-Fi SSID: case sensitive and must be EXACT PASSWORD *	Open No Wi-Fi security No Password
* Password	Must be 64-character length (max) and English alpha-numeric and special characters allowed – per local IT requirements			

Best Practices and Things to Remember

ENGAGE System Set-up

- Administrators who review and confirm default settings before commissioning the first device, will save time setting up their property and should not require device Sync updates after commissioning.
- Before commissioning any devices, the Administrator should confirm:
  - Will the property use MASTER CREDENTIALS? If so, review **Using Master Credentials** now.
  - Are all **Schedules** defined and properly entered?
  - See **MT20W Installation and Commissioning**, and commission the MT20W as the first commissioned device.
- Determine **Property-Wide Settings** User Expiration date. ENGAGE defaults all User Expiration Dates to five (5) years after enrollment automatically.
- Property device schedules should be defined before any device is commissioned. A schedule made or edited after a device is commissioned, will require Sync device updates before the new or updated schedule is followed.
- Common area access **Device Groups** should be defined before User access assignments are attempted.
- New or modified Device Groups require **Synchronization** of devices, before any group update is valid for that device.
  - Remember, devices must be commissioned before they are available to be selected for a Device Group.
- After assignment of a door into a Device Group, that device will requires Sync before the device knows which group it is assigned.
- Each User/Resident should NOT be assigned more than one credential.

⚠ CAUTION:
Both HIGH and MAX reader sensitivity settings reduce device battery life.

ENGAGE Device Set-up

- Define the **Property-Wide Settings** before commissioning devices.
- For best reader response and improved battery life, it is recommended to disable the Prox or Smart credential technology on multi-technology readers that is not needed or used.
- For locks that are in spotty Wi-Fi network areas, use the Mobile device data connection and turn off the lock Wi-Fi for better Sync performance.
- Normal Reader sensitivity is recommended for most properties.
  - Reader sensitivity may be set to HIGH or MAX and is most useful when small format FOB credentials are in use.

⚠ CAUTION: Control device Audit information is stored in a circular buffer. The oldest audits may be overwritten by the latest Audits when audits are not routinely gathered in a timely manner.

Control Mobile Enabled Smart locks

- Control devices do not support Wi-Fi connectivity.
- Every door access or device setting update MUST use the local **Synchronization** (Door File updates) process and the **Mobile Application**.
  - Control devices require a Sync at the nearby device using the ENGAGE Mobile Application to gather audits.
- Control devices do support User Schedules; however, Control devices do not support Holiday Schedules, or Door Schedules programming because they do not apply to manual deadbolt operation.
- Control construction mode enrolls the Facility Code of the first card presented.
  - Control construction mode will allow ALL OTHER credentials with the SAME Facility Code to have access.

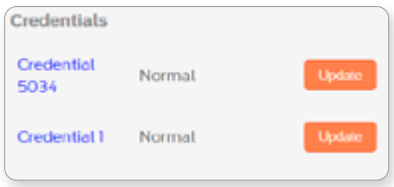
Schedules

- **Schedules** can ONLY be created or modified by the **Web Application**.
- All devices are programmed with the same set of User Schedules defined by ENGAGE at that time.
- Administrators should define ALL schedules needed in the property before commissioning any device. Otherwise every installed and commissioned device may require reprogramming when a new schedule is made or updated.
- A schedule change will require the Administrator to program each door.
  - User Schedule start/stop times and day-of-the-week settings are programmed into each device upon commissioning or with the **Synchronization** process (door file updated).
- Scheduled Temporary Access for maintenance should use User Schedules to set the time-of-day and User Activation/Expiration settings to enable and disable dates.
  - User credentials that are allowed to "Expire" will be available for reuse with all 11 sectors available for reprogramming
- A device Sync (door file update) is needed to communicate new schedule settings to a device.
- No-tour device programming DOES NOT update device schedule.

Master Credentials

- Consult the local authority to ensure that **Using Master Credentials** programming is allowed at the property location.
- When Master Credentials are defined or deleted ALL devices MUST be Sync updated.
- Device Sync (Door File updated) is required to enroll or remove the Master Credential.
- Master Credentials MAY NOT be reused.

Update ICONS



- Device and User Update ICONs ! within the ENGAGE Web and Mobile Applications indicates a device change has been entered into ENGAGE, and the device or the credential requires updating.
- Credential Update ICONs within the ENGAGE Web and Mobile Applications indicates a change has been entered into ENGAGE, and the credential requires updating.
- Credential Update ICONs are provided next to the credential name any time the credential has changes or updates pending and the credential needs to be programmed.

➔ **Note:** The credential update ICON remains until the credential is successfully programmed with the desired changes. Changes are not valid until the credential is presented to affected doors/devices.

- Device Update ICONs ! are provided next to the device name, any time the device has changes or updates pending, and the device needs to be programmed.

➔ **Note:** The device update ICON remains until Audit information is returned to let ENGAGE "KNOW" the update at the door has been accomplished. Once an update is acknowledged in a returned Audit, ENGAGE removes the Update ICONS

Factory Default Reset

- Factory Default Reset (FDR) is used to recover a device that was previously commissioned or in Construction mode.
- FDR does not remove the device from its ENGAGE account when previously commissioned.
- FDR returns the device to its out-of-the-box configuration, with one exception:
  - Administrators may DISABLE Construction Mode after commissioning on NDE, LE and CTE family of products.
  - FDR will not RESET the Block Construction setting when Disabled.

Moving Devices Between ENGAGE Accounts

- To move a device to another, ENGAGE account:
  - Delete the device from the original ENGAGE account to make it available in the new ENGAGE account.
  - Perform a Factory Reset Default (FDR) on the device to return it to the out-of-the-box settings
  - Commission the device into the new ENGAGE account.

Dual Technology Credentials

- "No Tour" capable multi-tech devices can be configured to disable proximity credentials for better performance and battery life.
  - When proximity technology is disabled, the device will no longer "look" for unnecessary credentials and the user experience of presenting credentials to a device for access will provide faster response.
- Use the Property Wide credential settings to disable proximity credentials automatically while commissioning devices
- Wall mounted readers used with Schlage CTE requires a Configuration Card to disable Proximity Credentials.

Firmware Updates

- **Automatic Updates** are the preferred method, when available.
- All devices should be kept up-to-date to ensure the latest security and functionality.

Daily System and Other Operations

This section describes a few of the day-to-day operations that need to be performed by ENGAGE Administrators, Managers, and Operators.

Assign New Access

To allow access to specific areas, the following steps are needed:

1. **Add User**.
2. **Add a Physical Credential to a User** or **Add a Mobile Credential to a User** to be used for access.
3. **Assign Access** privileges to the individual user.
4. The assigned doors will need **Synchronization** before the new user and access assignments will be valid.

Assign New Access (No-Tour)

➔ **Note:** See **No-Tour Feature** on page **103** for more information.

To allow access to specific areas, the following steps are needed:

1. **Add User**.
2. **Assign Access** privileges to the individual user.
3. **Add a Physical Credential to a User** or **Add a Mobile Credential to a User** to be used for access.
4. The assigned doors will need **Synchronization** before the new user and access assignments will be valid.

Clearing Access Assignments on Existing Credentials

Administrators will want to recover, save and reuse credentials whenever possible. It is important to clear all credential assignments from a returned credential so that the credential will have all 11 door assignment available. Credentials with cleared door assignments can be treated as new and reissued to a new user without any restrictions.

Follow these steps to clear all the current door assignments on a physical credential.

1. **Log In** to the web application.
2. From the **Users** tab, select the User associated with the credential you want to clear.
3. Click **Assign Access**.

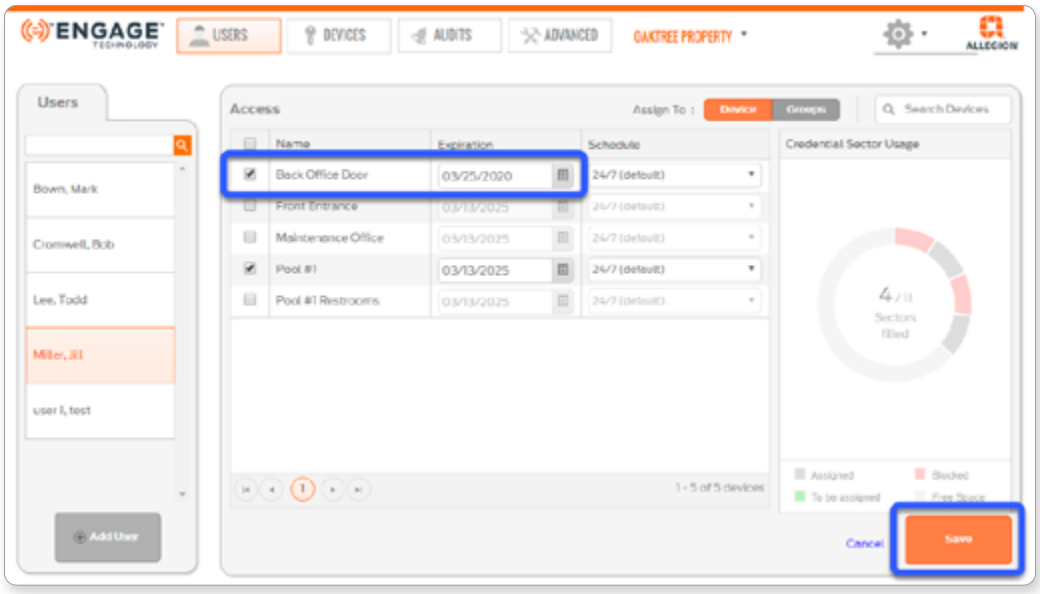


Fig. 7.1: Set Expiration Date to Expire “Today”

4. From the Assign To: button: select Device, set each of the assigned individual lock Expiration to the current date.
5. From the Assign To: button: select Groups, set each of the assigned Door Groups Expiration to the current date.
6. Select Save to update the credential details.
7. To complete this process, the credential must be updated with todays expiration setting and then stored away until tomorrow.
   a. Follow the **Update Credential for No-Tour Programming** process to program the credential with newly defined expiration settings.
   b. Tomorrow (after the credential has “Expired”) all 11 door assignments will again be available for new assignment.

Resident Move Out Processes

When a resident moves out, it is important to recover the credentials and plan for the credentials next use. The Administrator may follow one of these methods for credential reuse.

New User Waiting for Space and Credential Returned

Use this method if a new tenant is moving in at the same time the previous tenant is moving out and access rights are the SAME.

1. **Log In** to the web application.
2. Go the the previous resident's user record.
3. Edit and remove the previous resident's name and enter the name of the new resident.
4. Edit the Email Address, ADA, and the Activation and Expiration dates as needed.
5. Click Save.

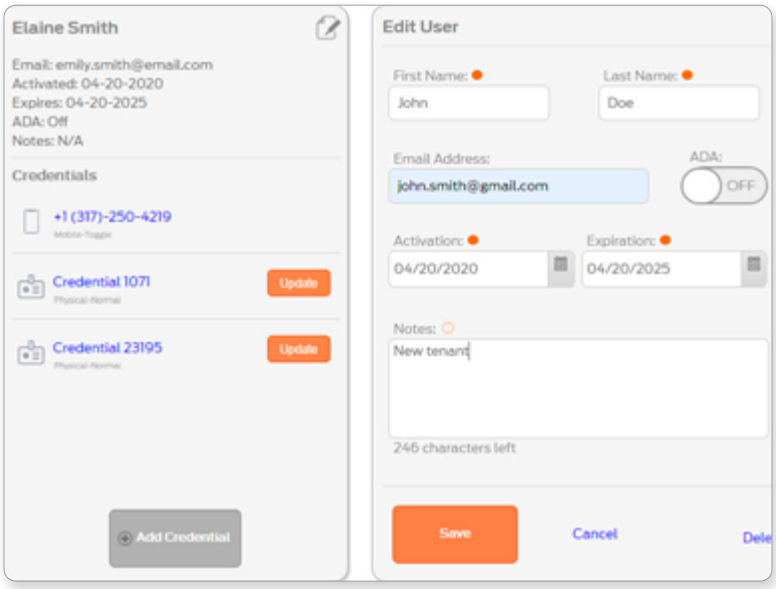
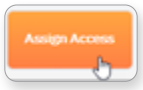
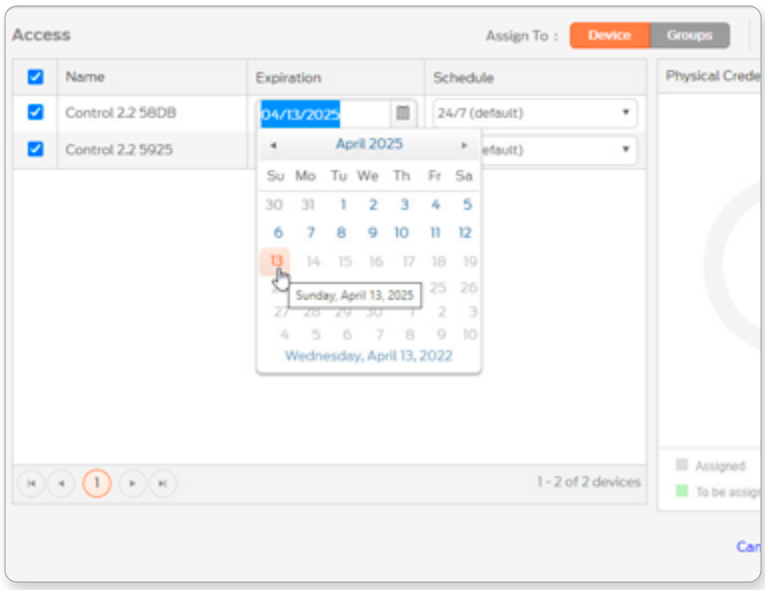


Fig. 7.2: Update Resident Name

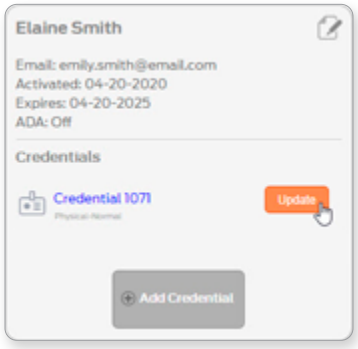
6. Click the Assign Access button.



7. Change the Expiration for each door.
8. Click Save.

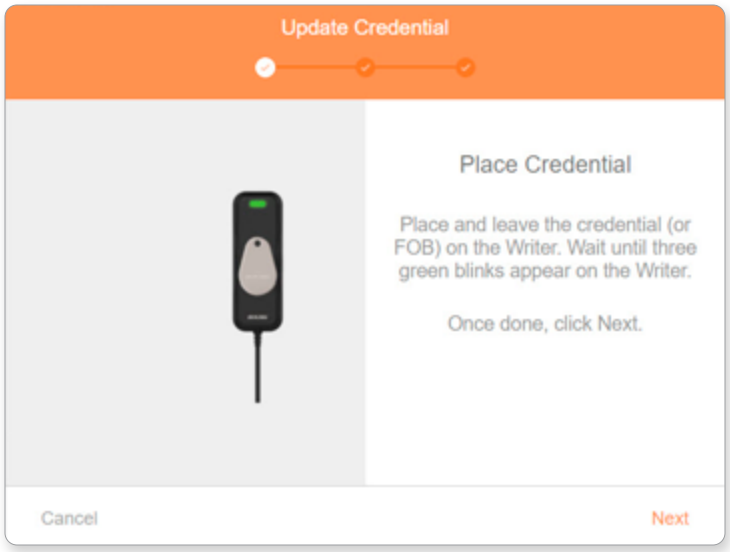


9. Click the Update button.



The previous ENGAGE User Audit information is maintained for history and any new accesses resulting from this credential reuse are reported with the new residents' name.

10. Present the credential to the writer. Follow the on-screen instructions.
11. Click Next.
12. Verify that the update was successful. Click Finish.
13. Hand the updated credential to the new resident.



Resident Moves Out - Credential returned to stock

Use this method when a credential is returned but it is not immediately being reissued to a new user with the same access. Administrators will want to recover, save and reuse credentials whenever possible.

It is important to clear all credential assignments from a returned credential so that the credential will have all 11-door assignment available.

To return a previously programmed credential to stock, follow the **Clearing Access Assignments on Existing Credentials** section.

Credentials with cleared door assignments can be treated as new and reissued to a new user without any restrictions.

Resident Moves Out - Credential Not Returned

Use this method when a resident moves out and their credential is not returned.

When a resident moves out without returning their access credential, the Administrator must delete all access assignments and Sync each door that the missing credential had access.

Updating door access to remove a credential will require one of the normal update options to be performed: Sync, Over-night update or No-Tour.

WARNING: A lost credential or a credential not returned when moving out must have its access removed and be immediately removed (Sync) from all assigned devices to ensure security.

No-Tour Resident Moves Out

When a resident moves out, the Administrator may follow one of these methods for physical credential reuse:

1. If a new resident is moving in at the same time an old resident is moving out, and their access rights are to be the SAME, the Administrator may choose to:
   a. Rename the old resident in ENGAGE with the new resident name.
   b. Hand the returned credential to the new resident.

   ➔ **Note:** The previous ENGAGE User Audit information is maintained for history and any new accesses resulting from this credential reuse, are reported with the new residents' name
2. If a credential is just being returned (not re-issued), follow these steps to take control of the returned credential, properly manage the ENGAGE property database, and to make the credential available for reuse and reprogramming:
   a. Change the name on the credential to "Unassigned" (or other).
   b. Set the User Expiration date to "Today".
   c. Remove (delete) all access assignments currently assigned to the credential.
   d. Successfully program the credential with the Schlage MT20W.

   ➔ **Note:** The returned credential is now unassigned and has no door assignments. Tomorrow, after midnight of the programmed Expiration date, the credential will be available for use and reassignment as a new credential.

Remove User and Access and Salvage Credential

To completely remove a user and their credential access from ENGAGE, the Administrator will need to "Clear access assignments" on the current credential and then delete the user from ENGAGE.

Follow these steps to remove the user and salvage their assigned credential.

1. **Log In** to the web application.
2. Follow the **Clearing Access Assignments on Existing Credentials** section to set the credential to expire "Tomorrow."
3. Wait for the credential to expire.
4. **Delete Credential**.
5. **Delete User**.

WARNING: Deleting a credential requires all devices that had access with that credential undergo Synchronization before the deleted credential is denied access at the door.

Reusing a Credential

See **Physical Credential Reuse: Best Practices** on page **124** for more information.

Delete User Access Rights

1. **Remove Access**.
2. **Delete Credential**.

Deleting Devices

Deleting devices can be accomplished using the ENGAGE Web Application or the ENGAGE Mobile Application. The ENGAGE Web Application is preferred for ease of use and data entry however both methods are described here.

Using the Web Application

1. **Delete Device**.

Using the Mobile Application

1. **Delete Device**.

Schlage Control audits can only be retrieved at the door using the Sync process and the ENGAGE Mobile Application. All other ENGAGE device audits may also be gathered remotely using over-night Wi-Fi network connections

Retrieving Audit Data from Devices

Device Audits are information collected by the devices whenever any action is taken. Actions performed at the door will be recorded and many device statuses are reported through Audit information.

Using Mobile Application

1. **Retrieve Audits**.

Using Web Application

1. **Audits**

Device Wi-Fi Network Setup

Device Wi-Fi connectivity is normally set up during the initial device installation and commissioning process. However, **Wi-fi Settings** can be changed or updated at any time.

To enable nightly Wi-Fi updates, configure any Wi-Fi enabled device to use the Wi-Fi network that is locally available at the device.

Once the Wi-Fi settings are entered, the Administrator will be able to verify the Wi-Fi connection using the **Test Wi-Fi Connection** feature from the **Mobile Application**.

WARNING: The manual Sync process is required for Control Mobile Enabled Smart Locks because they do not support Wi-Fi connectivity and cannot take advantage of the automated ENGAGE Nightly Wi-Fi "Call-In" feature. Frequent Sync processes are required to prevent lost Device and User Audits. Control Locks store only 1000 events. New Audit events will overwrite the oldest events when Sync is not performed in a timely fashion and the Audit memory can overflow.

Synchronization

Synchronization (sync) updates devices using the latest system settings and programmed access rights. Sync also captures and returns the latest Device and User Audits for review by the Administrator.

A device requires synchronization when the exclamation point appears next to the device name while viewing All Devices.

Nightly Wi-Fi Call-in Sync

When Wi-Fi enabled devices are used, the nightly Wi-Fi "Call-In" process (Sync) is automatically enabled. No additional action is required to enable nightly Call-Ins, other than making the proper **Wi-fi Settings** in the device and allowing the device to connect to ENGAGE via the local Wi-Fi network at the door.

➔ **Note:** Take advantage of Wi-Fi enabled devices to keep them up to date and to have the latest Audit information handy. Overnight Firmware Updates can be scheduled as well. For more information, refer to the **Automatic Updates** section.

Mobile Application Sync

- **Manually Sync Device**

Setting Device Date and Time

Device date and time is automatically checked and set each time a mobile device is connected and communicating with an ENGAGE device. Setting the date and time should only be necessary when the device power has been removed for an extended period (Battery replacements, jump start-Control).

1. **Log In** to the mobile application.
2. Select the In Range menu.
3. Select the device that needs its date and time verified/updated.
4. Verify the device was connected to and is communicating with the mobile device.
   - View the LED on the device. It should be flashing RED indicating the device is Connected.
   - View the Mobile device screen and ensure the device is connected
5. Verify the device date and time settings have been set correctly.

Control Mobile Enabled Smart Lock Jump Start Process

Schlage Control devices allow an external +9Vdc battery to be applied for access when the internal AA batteries are depleted. **Jump Start** is the only method for emergency access when the batteries are completely depleted. Control devices with depleted batteries may lose the correct time when "Jump Start" is used or anytime batteries are replaced. Any scheduled access that is not 24/7 may be affected. All that is needed to reset the time is to briefly **CONNECT** with the ENGAGE Mobile Application. Connecting with the Mobile device will set the **Date and Time** on the device to the same time on the Mobile device. If the device time is lost during Jump Start or Battery replacements, all device audits will be recorded with inaccurate times

Perform a Schlage Control Jump Start

1. Touch and HOLD a new alkaline 9-Volt battery to the Control contacts just below the thumb turn.

   ➔ **Note:** Battery connection orientation is not important as the lock accepts either polarity.

2. While holding the 9-volt battery in place, wait a few seconds until the lock completes its power-on reset.
   - The Control device will provide one (1) RED LED flash and then three (3) GREEN LED flashes and three (3) beeps.
3. While still HOLDING the external battery in place, present a valid credential for access.

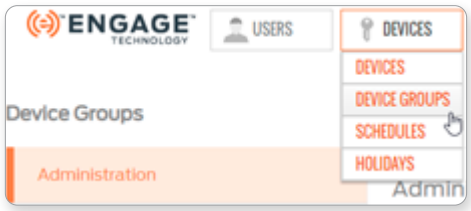
   ➔ **Note:** The "Jump Start" battery is removed after the valid credential presentation, because the thumb turn will physically interfere with the externally applied battery when turned

4. The Control device will engage the deadbolt to allow the user to turn the thumb turn for NORMAL access.

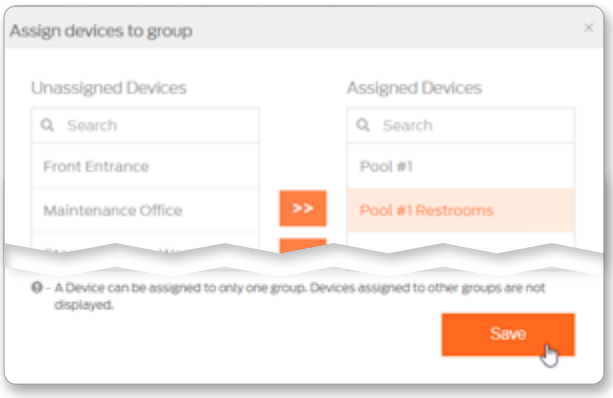
Managing Devices in Existing Device Group and Synchronization (No Tour)

When devices are added or removed from the existing device group and Users are already assigned to this Device group. Only Devices need to be updated or synchronized.

1. **Log In** to the web application.
2. From the Device tab, select Device Groups.



3. Click on the Device Group to add or remove devices in the group. See **Assign Devices to Device Group**.
4. Click Save. A pending Indicator will be displayed on devices that were added or removed.
5. Synchronize the device(s) for the Device group update to be valid. See **Manually Sync Device**.



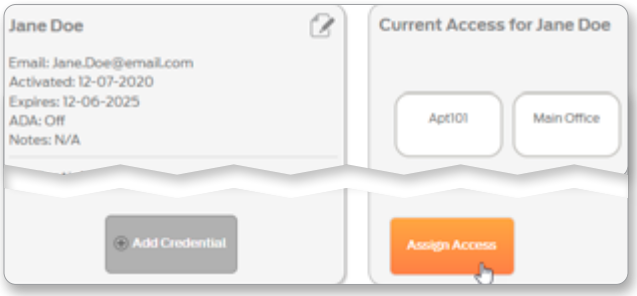
For existing User assignments to the Device group, the Credential does not need to be updated by placing it on MT20W. If a user is being newly added or removed from a device group, then we need to update both the devices and User/ Credentials.

Device Group Segmentation and Synchronization (No Tour)

When some Devices from a device group need to be moved to a new Device group, it is recommended to create two new Device groups, instead of splitting the existing Device group. Both User assignments and Devices must be synchronized after new device groups are created and devices assigned.

1. **Log In** to the web application.
2. Before splitting the existing group and creating two new device groups, make sure to expire the existing User assignment to device group. See **Clearing Access Assignments on Existing Credentials**.

   ➔ **Note:** If the user is unassigned from the device group without expiring the user's assignment, the sector will be blocked for that credential. Once existing Access Assignments are cleared, existing users will no longer have access to devices in the device group.
3. Either remove the devices from this device group or delete the device group before creating new device groups and adding devices to it. See **Assign Devices to Device Group**.
4. Create two new Device Groups. See **Add Device Group**.
5. Assign Valid Devices to the newly created Device groups. See **Assign Devices to Device Group**.
6. Devices need to be Synchronized for the Device group changes to be valid. See **Manually Sync Device**.
7. Assign users to the new Device groups. See **Assign Access**.
8. Users assigned to the Device group need to be Synchronized to update access. See **Update Credential for No-Tour Programming**.



➔ **Note:** Any Create/Update/Delete of Device group – Devices need to be updated/Sync'd, which is done in **step 6**. Any time a Credential is assigned or unassigned to a device group, it needs to be updated via MT20W (No tour).

Firmware Updates

Each device on a property should be kept up to date to ensure device compatibility and operations. Additionally, keeping all firmware at the latest revision will ensure the latest ENGAGE features and product updates are available.

Table 8.1 Firmware update method compatibility

Device	Via BLE	Via Wi-Fi	Via Mobile Wi-Fi	Automatic Updates	Desktop Application
Control	✓	✗	✗		✗
CTE/MTB	✓	✓	✓	✓	✗
LE and LEB	✓	✓	✓	✓	✗
NDE80 and NDEB	✓	✓	✓	✓	✗
XE360	✓	✗	✗	✗	✗
MT20W	✓	✓	✓	✓	✓
MT20	✓	✓	✓	✓	✗

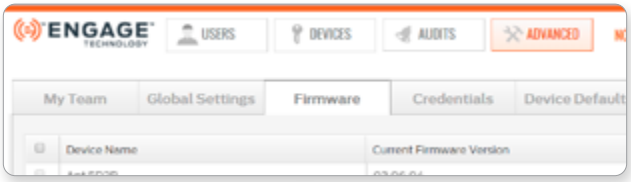
⚠ CAUTION:
The device will not operate as a locking device for the few minutes the device is downloading firmware and will be flashing the RED and GREEN LED during the process.

Automatic Updates

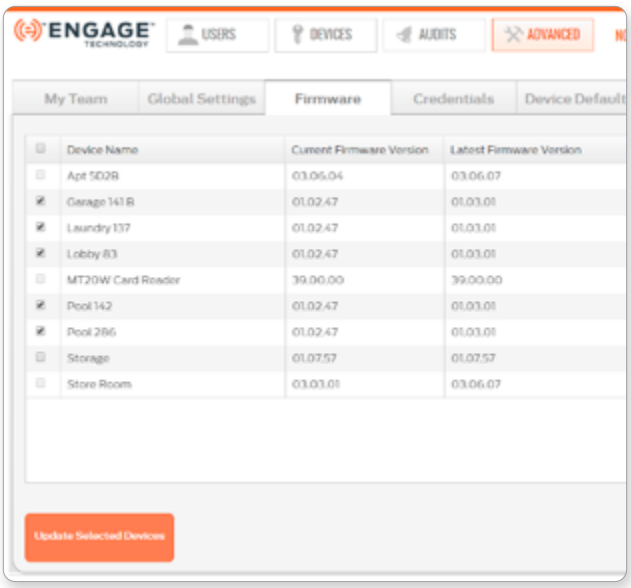
➔ **Note:** Devices must have their Wi-Fi network configured and a local Wi-Fi network available before automatic firmware updates are possible. See **Wi-fi Settings**.

This is the preferred method of firmware updates. It is faster than using the Bluetooth communication option and may be automated and scheduled using the Web Application. Automated Wi-Fi firmware updates are performed in the early morning hours so that user access is less likely to be affected during the update process. Once completed the device will reset and begin operation using the newly download firmware.

1. **Log In** to the web application.
2. Select ADVANCED tab.
3. Select the Firmware tab.



4. Compare the Current Firmware Version on each device to the Latest Firmware Version that is available. If a firmware update is available, check the box next to the Device Name.
5. Select the Update Selected Devices button.



6. See the momentary Firmware updates have been scheduled. Message.

7. Wait until the next day to review the device firmware status.

   ➔ **Note:** If a selected firmware update is not successfully accomplished overnight:

   - Ensure that the device has Wi-Fi connectivity enabled
   - Ensure the local Wi-Fi is operating
   - Ensure local Wi-Fi was available at the door over-night – was there an outage?
   - Verify Wi-Fi network communication and settings in the device are correct.

Manual Firmware Updates at the Door

Manual firmware updates are performed while nearby the device using the **Mobile Application**. Manual firmware updates are available for all ENGAGE enabled devices using Bluetooth communication or a local Wi-Fi connection for faster updates when available.

- **Via BLE**
- **Via Wi-Fi**
- **Via Mobile Wi-Fi**

MT20W Firmware Updates via the Desktop App

➔ **Note:** See **Desktop Application** on page **189** for more information.

Web Application

Introduction

The ENGAGE Web Application is used to set up and manage a property with ENGAGE enabled devices. Administrators will use the ENGAGE Web Application for property management data entry and general maintenance. Management of the property may be accomplished from virtually anywhere using a web browser.

The web application provides the easiest way to enter data and view your property information via a standard keyboard and a larger screen.

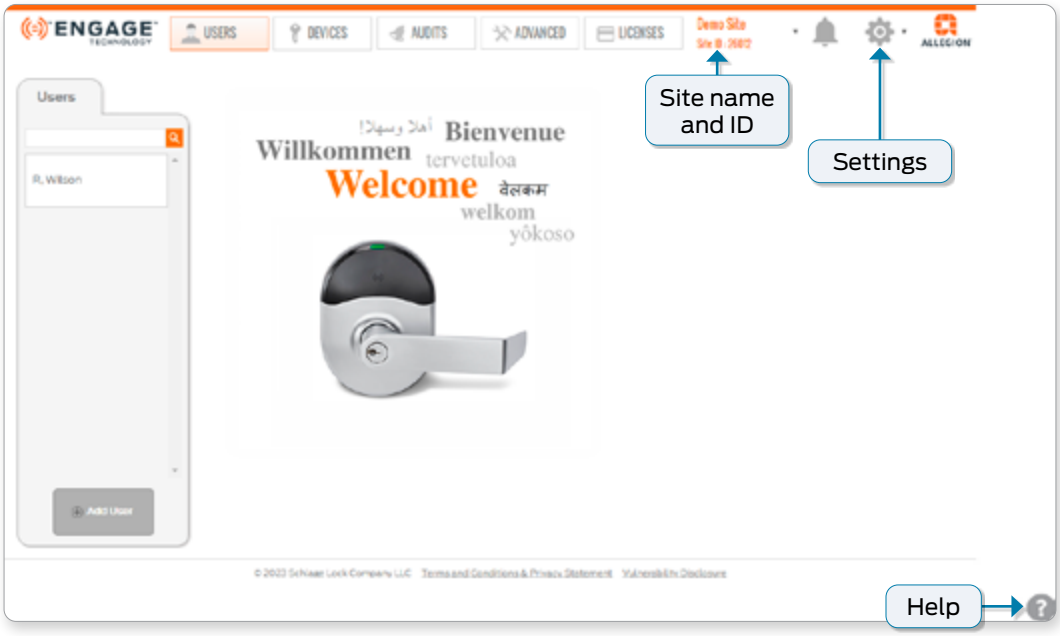
For the latest information, go to https://us.allegion.com/en/home/products/categories/software/ENGAGE-web-mobile-apps.html and click on Mobile & Web Requirements.

Supported Web Browsers

We support and test major revisions for Chrome, Safari, Firefox, and Edge for the last two years such as:

- Chrome 87 or newer
- Safari 14 or newer

Interface Reference



Create Account

Administrators must create an account in ENGAGE to manage team members, users, devices, schedules, global settings, and other functions for their properties.

1. **Log In**.
2. Select Create Account.

Fig. 9.1: ENGAGE Logon Screen

3. From the New Account screen, complete all fields.
   a. Email Address: must be unique and not used for any other ENGAGE Managed Property.
   b. Password: (rules)
      - At least 10 characters
      - One Upper Case
      - One Lower case
      - One Number or symbol
      - No 2 repeating entries
   c. Confirm Password: reenter your password
   d. First Name: enter your first name
   e. Last Name: enter your last name
4. Read the Terms and Conditions and check the box to acknowledge.
5. Select Sign Up.

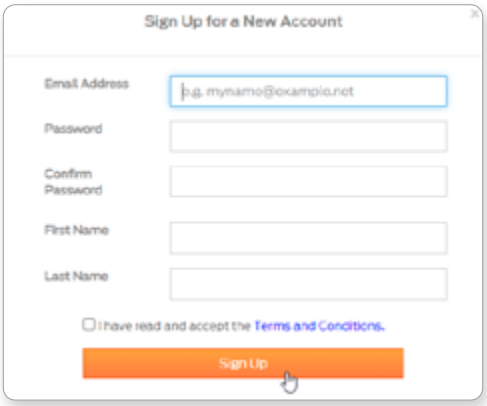


Fig. 9.2: ENGAGE Create Account Screen

6. Select OK when account has been successfully created.

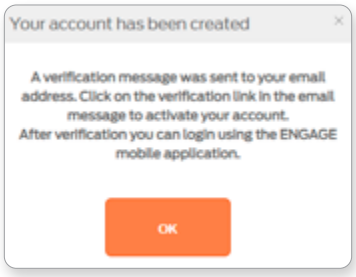


Fig. 9.3: ENGAGE Account Created

If you do not receive the verification email within a few minutes, check your Spam and Trash folders.

Verify the email address entered is correct and/or resend the invitation.

7. Go to the email used to create the account and open the verification. Look for an email from allegion.automated@allegion.com.
8. Select Confirm my account to activate.

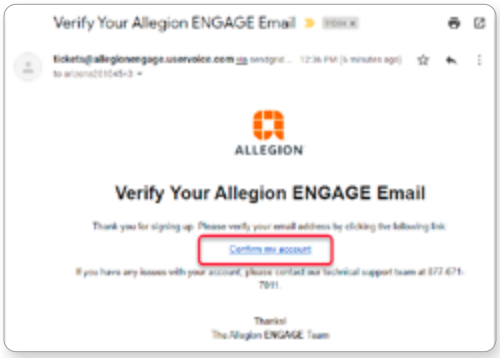


Fig. 9.4: Verification Email

Log In

1. Navigate to https://portal.allegionengage.com/signin.
1. Enter the email address you used to set up your account and your password.
2. Select Sign In.

Fig. 9.5: Login screen

My Profile

Hover over the gear icon to view the MY PROFILE option. Click on it to edit name, change password, or delete account.

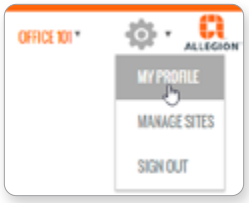


Fig. 9.6: My Profile

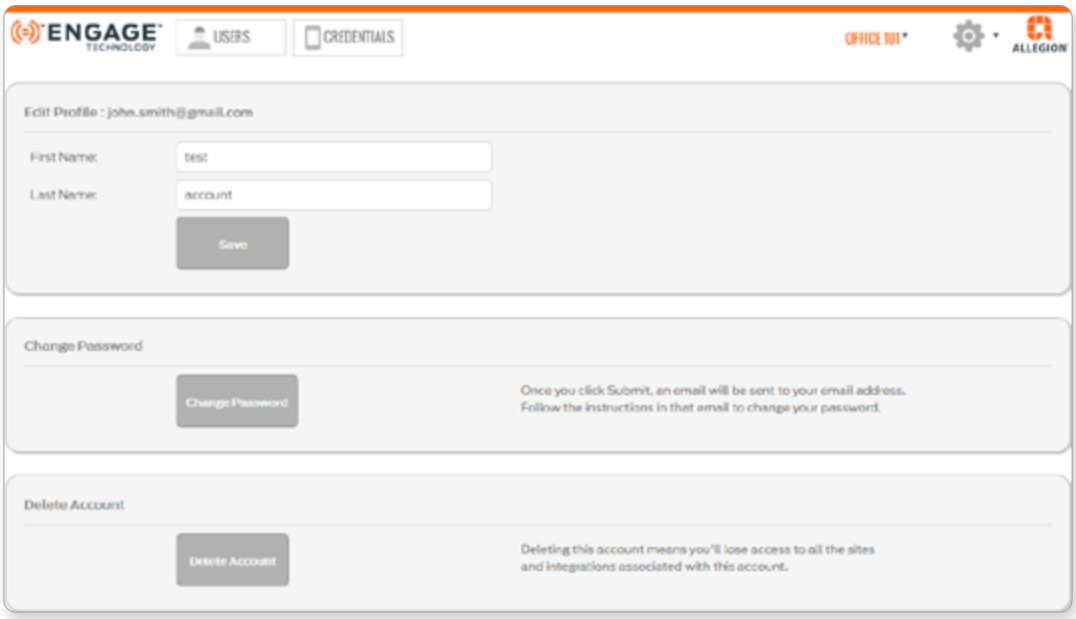


Fig. 9.7: Edit Profile

Administrators should think through their property needs and desired features before beginning in order to save time and streamline the installation process.

Create Site

A Site is a group of users and devices; a property.

1. **Log In.**
2. From the Settings menu, choose MANAGE SITES.

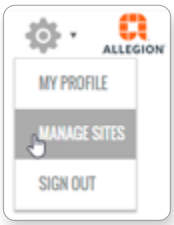


Fig. 9.8: MANAGE SITES

3. Select Create New Site button.

Fig. 9.9: Create New Site Button

3. In the Create New Site screen, select ENGAGE from the Site Software drop-down.
4. Approval is required to create a new ENGAGE site. Click the link.

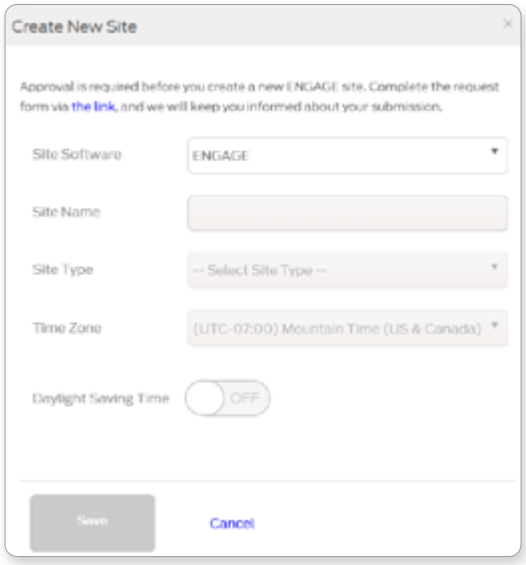


Fig. 9.10: Create New Site Screen

5. Fill in the request form and then click the Submit request button.
6. The Site request will be submitted to the local sales office for approval. Please allows one (1) business day for a response. Watch for an email with further instructions.

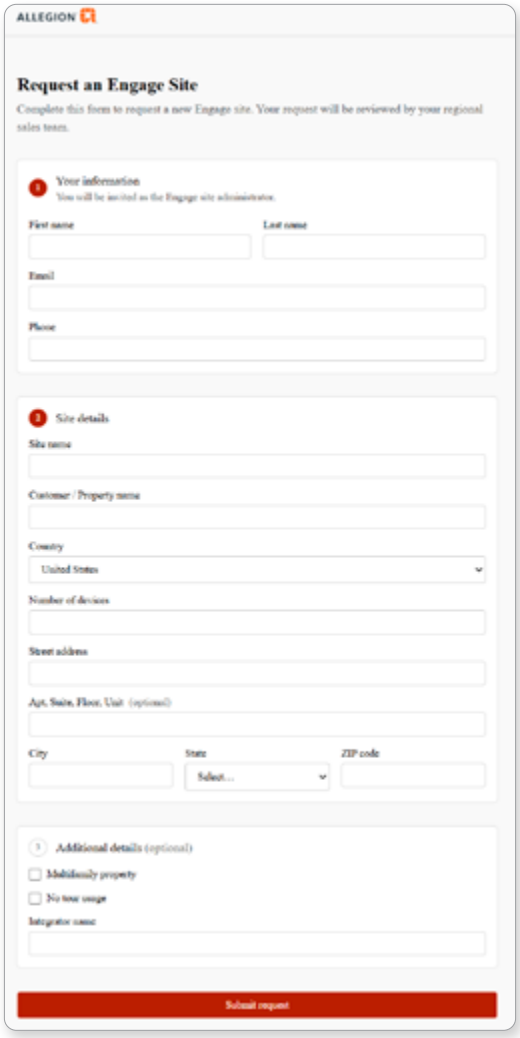


Fig. 9.11: Request an ENGAGE Site

Users

Users are people who need to gain access to an opening in your site. They must also be assigned a Credential before access can be granted.

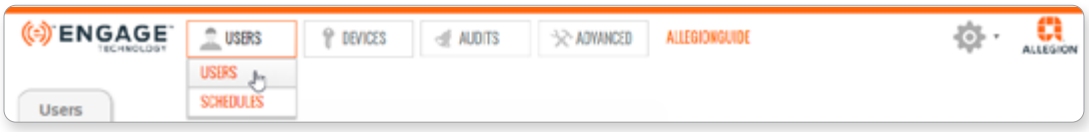


Fig. 9.12: Users Tab

Table 9.1 Users Properties			
Property	**Description**	**Required**	**Default**
First Name	enter the first name of the user	yes	none
Last Name	enter the last name of the user	yes	none
Email	enter user email address	no	none
Activation	Date of activation	yes	current date
Expiration	Date user profile expires	yes	five (5) years from current date
Notes	can be used to capture additional information about the user (e.g. resident ID, employee ID, memo)	no	none
ADA Enabled	When the individual User ADA setting is ON, the user is allowed modified access times. Door Default ADA setting is 30 seconds. This ADA Relock time setting can be changed on a per door basis from 1 to 255 seconds. Sync is required to update new or edited ADA settings. Control Mobile Enabled Smart Locks do not support ADA.	no	off

Add User

1. **Log In** and open the **Users Tab**.
2. Select Add User.

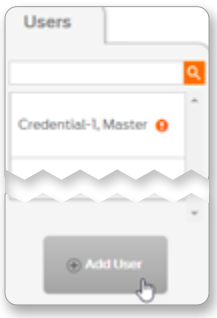


Fig. 9.13: Add User Button

4. From the Add New User screen, complete the fields:

   ➔ **Note:** See **Table 9.1 Users Properties** for details.

5. Select Save.

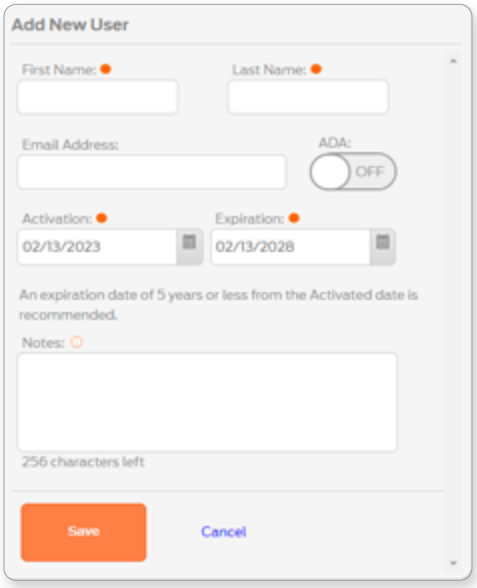


Fig. 9.14: Add New User

6. The User added banner is displayed and the user information screen displays.

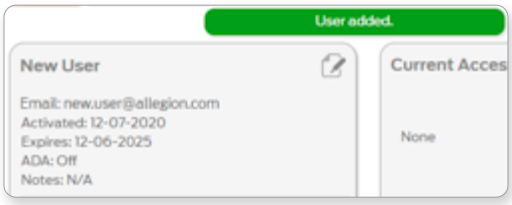


Fig. 9.15: New User Added

Edit User

1. **Log In** and open the **Users Tab**.

2. Select a current user.

Fig. 9.16: Select a User

3. Select the edit user button.

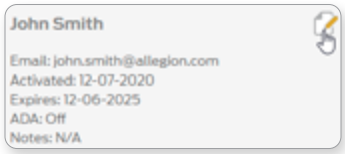


Fig. 9.17: Edit User Button

4. From the Edit User screen, make changes to the fields:

   ➔ **Note:** See **Table 9.1 Users Properties** for details.

5. Select Save.

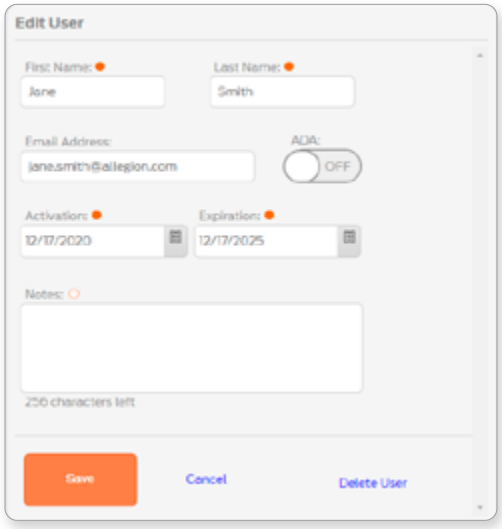


Fig. 9.18: Edit User

6. The User info updated banner is displayed and the user information screen displays.

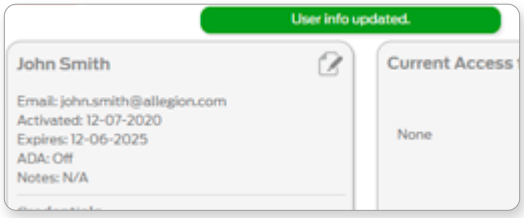


Fig. 9.19: User Info Updated

Delete User

1. **Log In** and open the **Users Tab**.

2. Select a current user.

Fig. 9.20: Select a User

3. Select the edit user button.

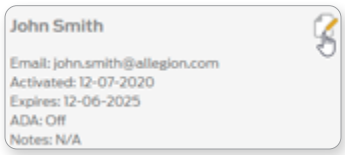


Fig. 9.21: Edit User Button

4. Select Delete User.

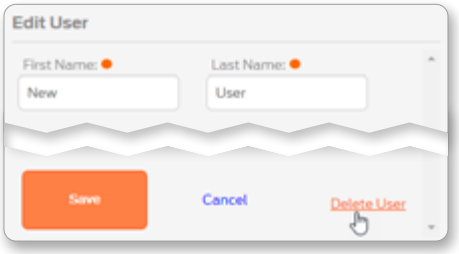


Fig. 9.22: Delete User Button

5. Type DELETE into the Confirm: box. Then select the Delete button.

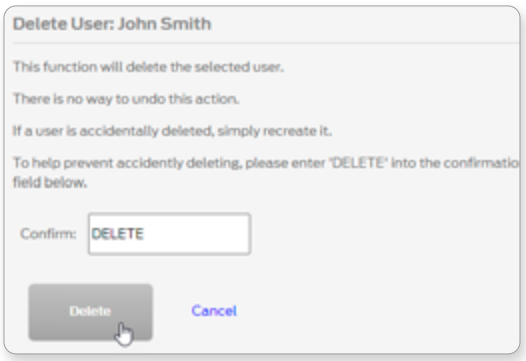


Fig. 9.23: Confirm User Deletion

6. The User deleted banner is displayed.

Fig. 9.24: User deleted

Bulk Import Users

The Bulk Import Users feature in ENGAGE simplifies the process of adding multiple users at once and automates the creation of Schlage Mobile BLE credentials for both ENGAGE and PACS managed sites. This feature is designed for ENGAGE Site Administrators and Managers, enabling them to efficiently create mobile BLE credentials using a CSV file upload process.

IMPORTANT: Please ensure you have enough mobile licenses in the inventory before using this feature. See **View Mobile License Inventory** on page **126** for more information.

BEST PRACTICES:

1. Ensure enough licenses are available in the inventory before bulk importing users.
2. Verify the Bit Format and Starting Badge ID settings in the site, as the Bulk Import Users feature auto-provisions Badge IDs when creating credentials.
3. Always ensure the data in the CSV file is accurate and complete before uploading.
4. Save a copy of the CSV file before uploading to keep a record of the imported users.
5. Regularly check ENGAGE notifications for updates on the import process.
6. Use error reports to quickly resolve issues and re-import corrected data.
7. Ensure that access to doors is assigned to users following the import process, enabling them to use the Schlage Mobile Access App for accessing doors. See **Assign Access** on page **44** for more information.
8. For tour sites, the doors must be synced after access has been assigned to users. See **Manually Sync Device** on page **86** for more information.

1. **Log In**.
2. Hover over Users and select Import Users.

Fig. 9.25: Import Users Menu

3. Click the Download Template button.

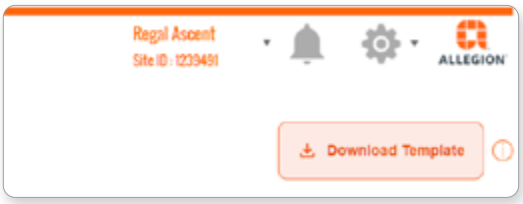


Fig. 9.26: Download Template Button

4. Once the template is downloaded, open it and populate the file.

   ➔ **Note:** You must populate at least five (5) records.

Field Name	Notes
FirstName	User's first name
LastName	User's last name
MobilePhoneNumber	User's ten-digit mobile phone number ➔ **Note:** Only USA mobile phone numbers are supported.
License	Specify the license type. See **License Type** on page **125** for more information.
Notes (optional)	Any additional notes about the user

5. Upload the file to ENGAGE.
   - Drag and drop the .csv file into the box, or use the Upload a file button.

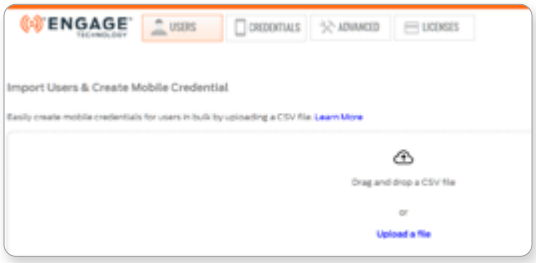


Fig. 9.27: Upload .csv File

6. Click the Proceed button.

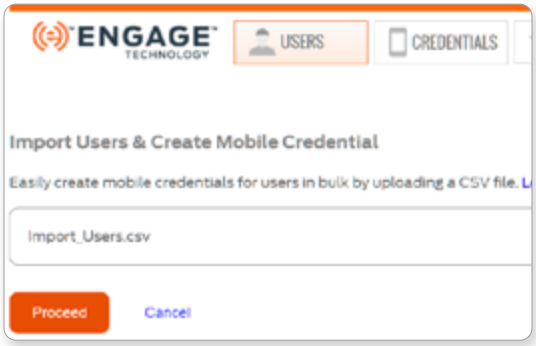


Fig. 9.28: Proceed Button

7. The file will be read and any errors will be displayed. Click Continue to import the credentials.

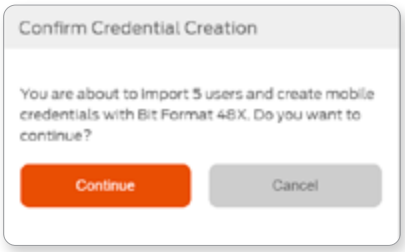


Fig. 9.29: Confirm Credential Creation

8. The credentials will be created.

   ➔ **Note:** Depending on how many files the system is processing, the file may be added to the queue. Site administrators and Managers can continue using the system during this process.

9. Click the Check Status button to view the status.

Fig. 9.30: Confirm Credential Creation

10. The status will be displayed. If an error report was generated, click the Download Error Report button.

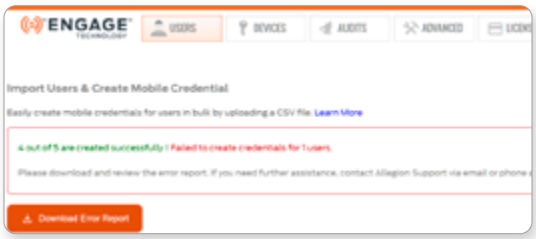


Fig. 9.31: Status Messages

11. Additionally, notifications are displayed in the upper right corner. Click the bell icon to display the messages. Click the message for further details, and to download an error report that was generated.

Fig. 9.32: Error Messages

12. You may see any of the following messages in the notification area.

Message	Description
Bulk Import Completed Successfully	Credentials were created for all users in the CSV file.
Bulk Import Partially Completed with Errors	Credentials were created for some users, but others failed.
Bulk Import Failed	The import failed completely.
System Error During Bulk Import	The system was unable to process the CSV file.

Common Issues

- Ensure the file format is CSV and matches the template structure.
- Ensure the license type is valid and available in the inventory (1, 5, or Reusable) and matches the ENGAGE inventory.
- Ensure all phone numbers are ten digits and not already used for existing credentials.

Add a Physical Credential to a User

Adding a credential to a user connects the credential to the specific user. This process identifies the user in both the ENGAGE Audits and in the ENGAGE Device databases.

1. **Log In** and open the **Users Tab**.

2. Select a current user.

Fig. 9.33: Select a User

3. From the Users card, select Add Credential.

Fig. 9.34: Add Credential Button

4. The Add Credential card will display. The Select Existing Credential tab will display by default. Select an existing credential from the list.

   ➔ **Note:** If there are no existing credentials available, see **Enroll a Smart Credential Individually on page 119.**

5. Select the Credential Function from the drop-down list.

   ➔ **Note:** See **Credential Functions** on page **138** for more information.

As you select each different credential function from the drop-down list, notice that the description above the list changes.

CAUTION: Control Mobile Enabled Smart Locks cannot relock, so a TOGGLE credential will act as a NORMAL credential when presented.

6. Select Save.

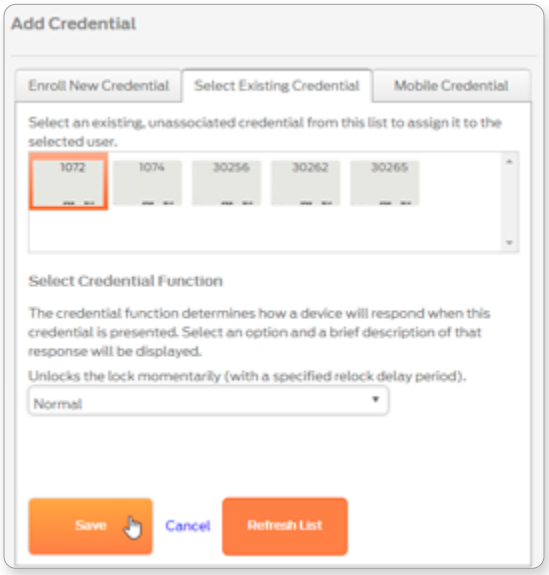


Fig. 9.35: Add Credential

7. The Credential assigned banner is displayed and the credential displays under the user information.

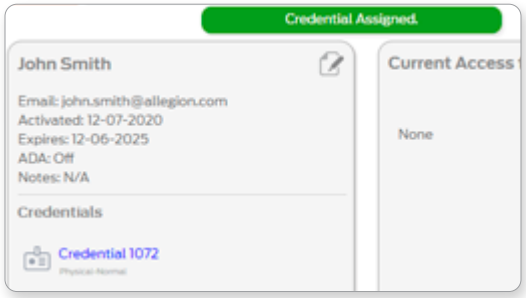


Fig. 9.36: Credential assigned banner

Add a Mobile Credential to a User

Adding a credential to a user connects the credential to the specific user. This process identifies the user in both the ENGAGE Audits and in the ENGAGE Device databases. Before a mobile credential may be assigned, a license must be purchased and loaded into the site. See **Mobile Credentials** on page **125** for more information.

Bluetooth communication is required for Mobile Credential use and must be turned ON when using a Mobile phone. The Schlage Mobile Access application will warn the user anytime Bluetooth is turned OFF. Bluetooth is required for this application. Android devices will require Locations Services to be enabled whenever Bluetooth is turned ON although the Schlage Mobile Access application will never track the user's location.

1. **Log In** and open the **Users Tab**.

2. Select a current user.

Fig. 9.37: Select a User

7. From the Users card, select Add Credential.

Fig. 9.38: Add Credential Button

If your screen displays Your devices do not currently support mobile credentials, then select Learn about the path to upgrade here to learn more.

8. Select the Mobile Credential tab on the Add Credential card.
9. Select the desired **License Type** from the drop down box.
10. Type the mobile phone number into the Mobile Phone Number box.
11. Select Save.

    ➔ **Note:** The user's mobile phone will receive an automated text message with additional instructions.

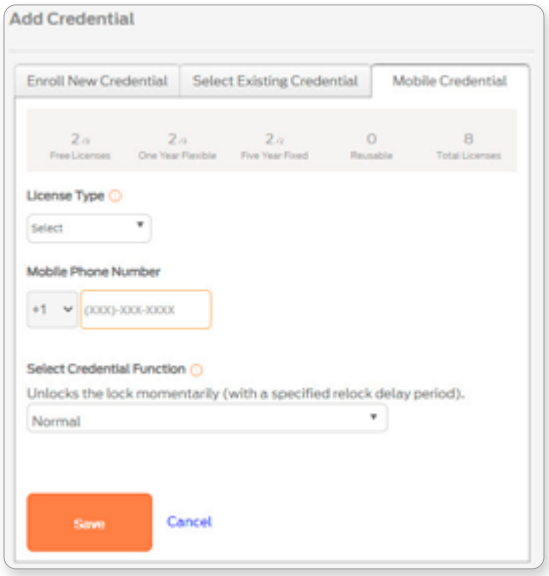


Fig. 9.39: Add Mobile Credential

Edit Credential

1. **Log In** and open the **Users Tab**.
2. Select the user whose credential needs to be edited.

Fig. 9.40: Select a User

3. Select the credential you want to edit

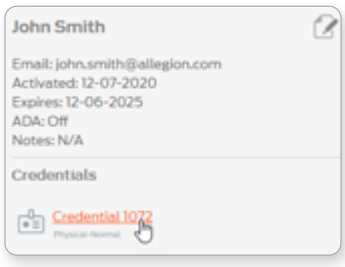


Fig. 9.41: Select Credential

4. Select the desired **Credential Functions** from the drop down list.
5. Select Save.

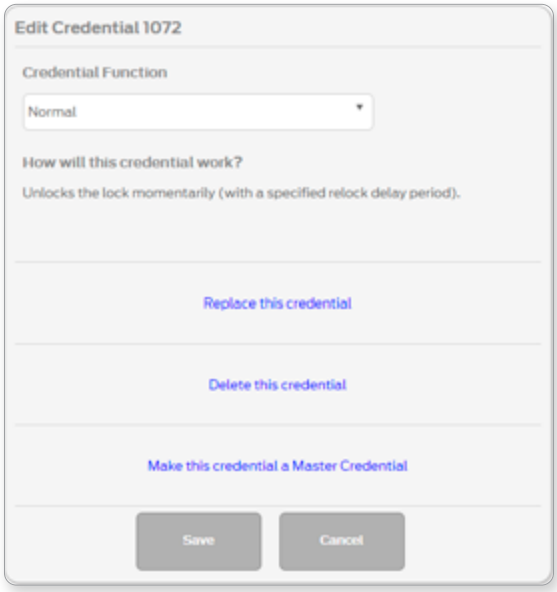


Fig. 9.42: Edit Credential

Delete Credential

1. **Log In** and open the **Users Tab**.
2. Select the user whose credential needs to be edited.

Fig. 9.43: Select a User

3. Select the credential you want to delete.

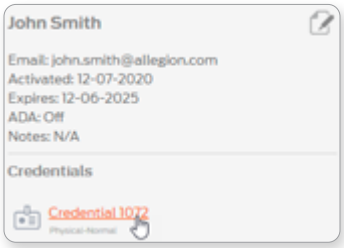


Fig. 9.44: Select Credential

4. Select Delete this credential.

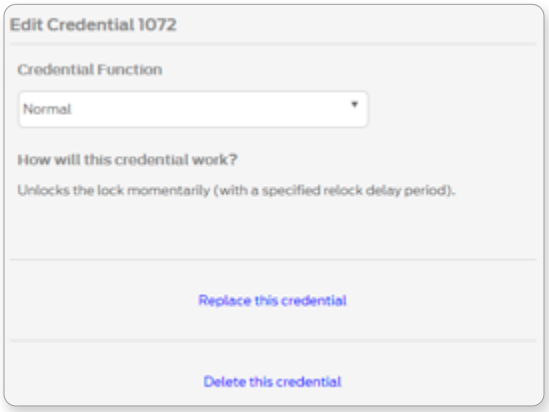


Fig. 9.45: Edit Credential

5. Type DELETE into the Confirm: box.
6. Select Delete.

➔ **Note:** When a **Mobile** credential is deleted, the license will be unassigned, and may be available to be reassigned. See **License Type** on page **125** for more information.

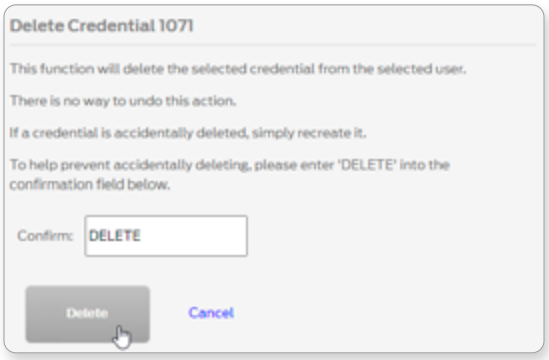


Fig. 9.46: Delete Credential

7. The confirmation message will be displayed.

CAUTION: Devices that had access with the credential must be programmed before the deleted credential will be denied access. ! is shown next to doors that require programming.

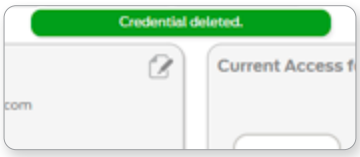


Fig. 9.47: Credential deleted

Assign Access

You can assign access either from the **Users** section or from the **Devices** section.

1. **Log In** and open the **Users Tab**.
2. Select the user whose access needs to be edited.

Fig. 9.48: Select a User

3. Select the Assign Access button.

➔ **Note:** Current access is shown below the Current Access... heading.

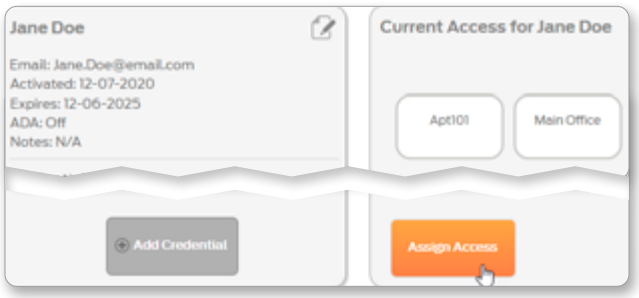


Fig. 9.49: Assign Access button

4. Select check boxes next to each device to assign or remove access. Blue checks indicate that access is assigned.
5. To assign access to a group, first select the Groups button, and then click the check box next to each group to which the user should have access.
6. For each device or group, choose an Expiration and a Schedule from the drop-down lists.
7. Select the Save button.

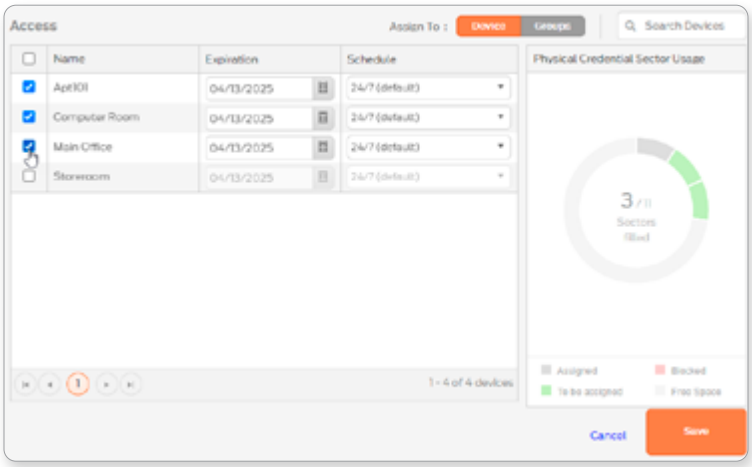


Fig. 9.50: Assign Access

The default expiration date is set to five (5) years from the date the user was first created in the system. The default schedule is 24/7. To add more schedules, see **Add Schedule (Users)**.

8. If the user was assigned a mobile credential for the access you are trying to edit, you may see a message regarding the mobile credential license. You can choose to:
   - Upgrade the license to a free or paid license
   - Make the change and switch to a physical credential
   - Cancel the change.

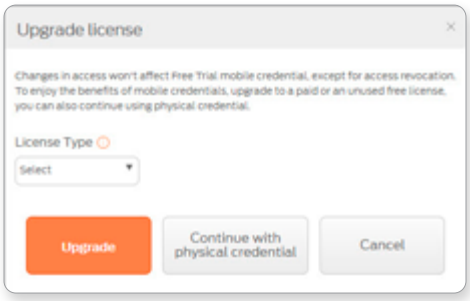


Fig. 9.51: Upgrade license

➔ **Note:** See **Mobile Credentials** on page **125** for more information.

➔ **Note:** The circular graph shows how many sectors are available on a physical credential. Each time you assign a new device to a credential, a sector is used. Mobile credentials do not have this limitation.

⚠ **CAUTION:** Devices must be programmed before the access will be granted. ❗ is shown next to doors that require programming.

Remove Access

Use the steps for **Assign Access**.

A maximum of 16 User Schedules can be defined per property.

Add Schedule (Users)

User schedules are used to restrict access to certain times of the day.

CAUTION: For Control Mobile Enabled Smart Locks: users exiting a room will not be able to use the outside thumbturn to relock the deadbolt after scheduled access time has expired.

1. **Log In** and select Users > Schedules.

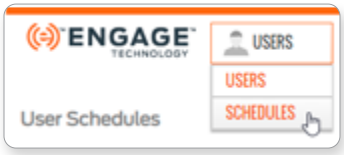


Fig. 9.52: Users > Schedules Button

2. Select the Add New User Schedule button..

Fig. 9.53: Add New User Schedule Button

The default User Schedule is 24/7 for access all the time. All new users are assigned this schedule by default.

The default 24/7 schedule cannot be edited or deleted.

3. Enter the name. Select or enter the start and end times. Select the days during which the schedule should be active.
4. Select the Save button.

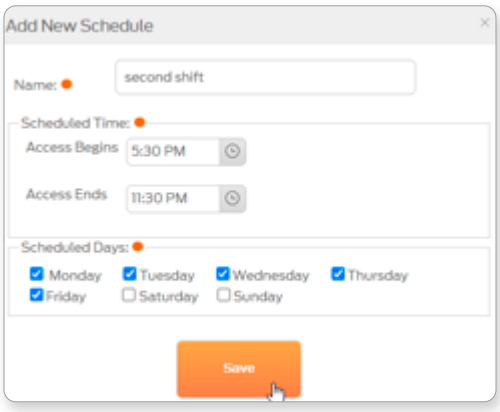


Fig. 9.54: Add New User Schedule

5. The User Schedule added successfully confirmation message will be displayed.

Fig. 9.55: Add New User Schedule Confirmation

CAUTION: Devices that will use the schedule must be programmed before the schedule will be added. ! is shown next to doors that require programming. ANY change made to a schedule for sites using no tour will require ALL credentials to be collected and placed on the MT20W for programming.

CAUTION: For Control Mobile Enabled Smart Locks: users exiting a room will not be able to use the outside thumbturn to relock the deadbolt after scheduled access time has expired.

Edit Schedule

1. **Log In** and select Users > Schedules.
12. Select the schedule you want to edit.

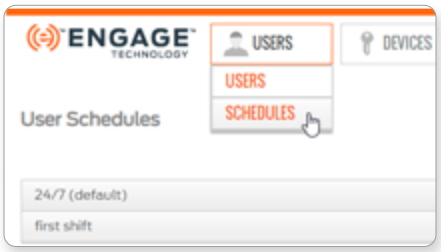


Fig. 9.56: Users > Schedules Button

13. Select the Edit button.

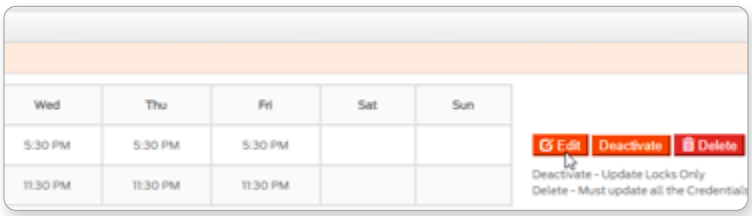


Fig. 9.57: Edit User Schedule Button

The default User Schedule is 24/7 for access all the time. All new users are assigned this schedule by default.

The default 24/7 schedule cannot be edited or deleted.

14. Edit the name. Select or enter the start and end times. Select the days during which the schedule should be active.
15. Select the Save button.

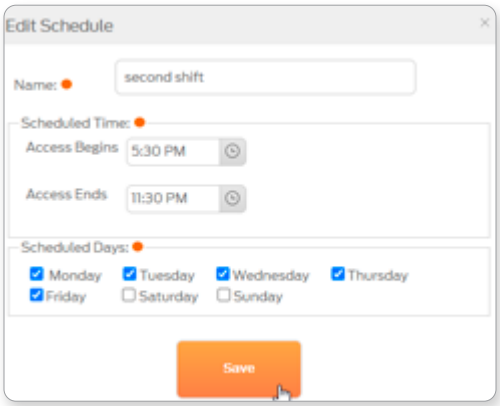


Fig. 9.58: Edit User Schedule

16. The User Schedule updated successfully confirmation message will be displayed.

Fig. 9.59: Edit User Schedule Confirmation

CAUTION: Devices that use the schedule must be programmed before the schedule will be updated. ! is shown next to doors that require programming.

Deactivate or Delete Schedule

Deactivate a schedule if you want to keep the schedule for later use. Delete a schedule if you will not need it again

1. **Log In** and select Users > Schedules.
2. Select the schedule you want to deactivate or delete.

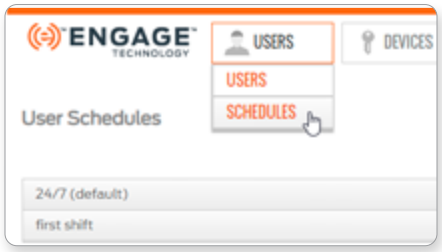


Fig. 9.60: Users > Schedules Button

The default User Schedule is 24/7 for access all the time. All new users are assigned this schedule by default.

The default 24/7 schedule cannot be edited or deleted.

3. Select the Deactivate or Delete button.

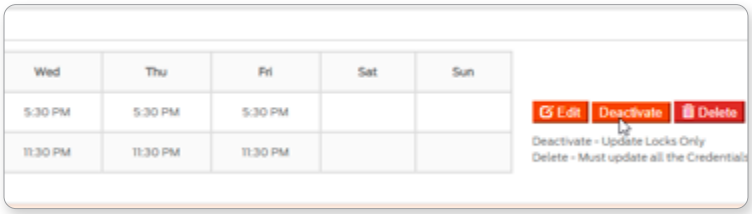


Fig. 9.61: User Schedule Deactivate Button

4. A warning message will be displayed.
5. Select the I Understand button.

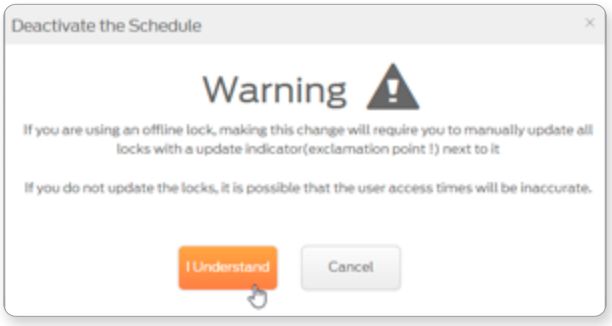


Fig. 9.62: Edit User Schedule

6. The User Schedule deactivated successfully confirmation message will be displayed.

Fig. 9.63: User Schedule Deactivated Confirmation

CAUTION: Devices that use the schedule must be programmed before the schedule will be deactivated. is shown next to doors that require programming.
If you delete a schedule, ALL credentials and locks must be updated.

Devices

Device Settings

When a device is commissioned, the defined Default Device Settings are programmed into the device. Administrators may want to adjust specific device settings to be unique for an opening, situation, or feature. To make individual setting changes, follow these steps for a particular device.

Add Device

Devices are added using the mobile application. See **Add Device**.

Edit Device

1. **Log In**.
2. Select the Devices menu and the Devices pull down.
3. Select a previously commissioned device from the device list.

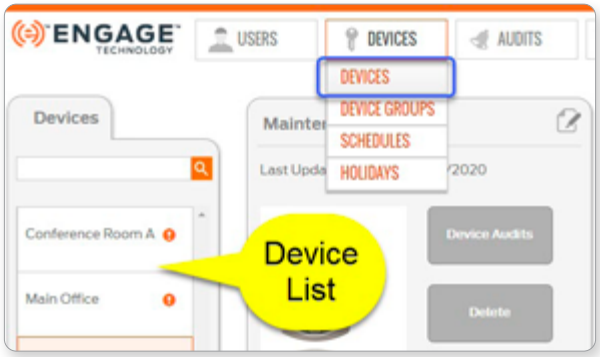


Fig. 9.64: Devices > Devices

4. From the device tab, select the edit icon. The individual device settings screen will display.
5. The following sections describe each of the ENGAGE devices separately.

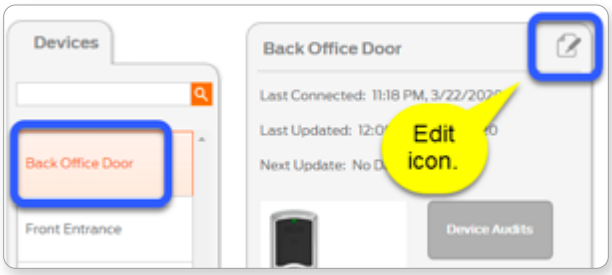


Fig. 9.65: Edit Individual Device

Adjusting the settings here will change the settings for the currently selected device ONLY.

Control Mobile Enabled Smart Lock

Adjust as needed and Save to apply changes.

For Control Mobile Enabled Smart Locks that are commissioned, a Mobile Credential tab will be available.

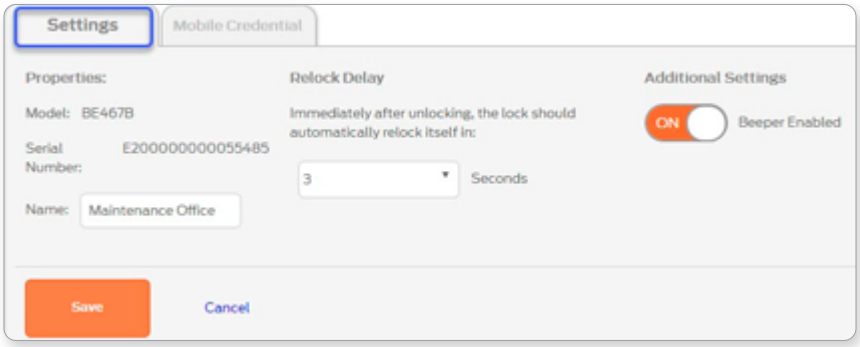


Fig. 9.66: Control Individual Settings

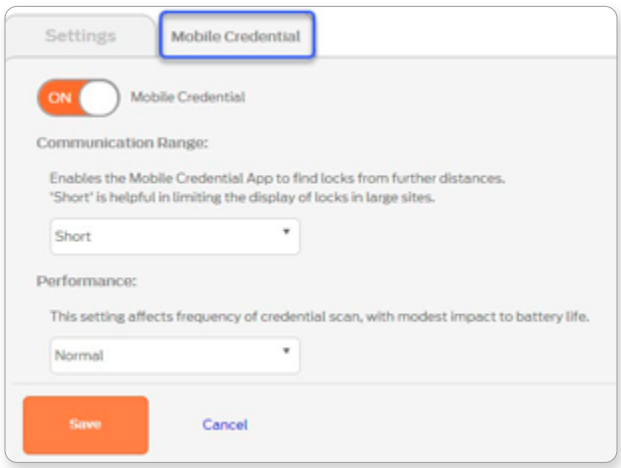


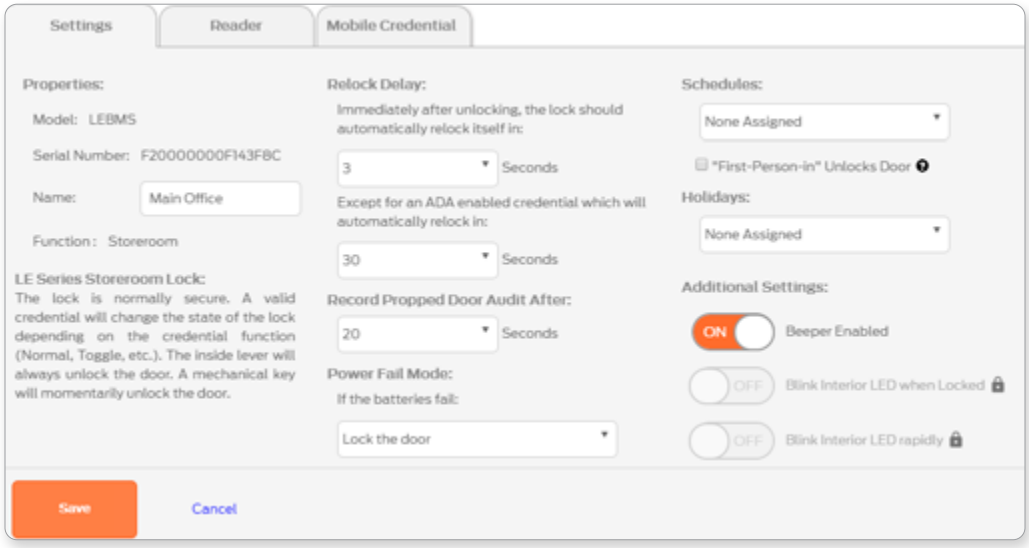
Fig. 9.67: Control Mobile Credential Settings

Table 9.2 Control Mobile Enabled Smart Lock Individual Settings	
Setting	**Description**
Settings Tab	
Name	Device Name
Relock Delay	Immediately after unlocking, set the lock to automatically relock itself between 1 – 30 seconds
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent
Mobile Credential Tab	
Mobile Credential	• OFF: Mobile Credential use is disabled • ON: lock will accept Mobile Credential access
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances ➔ **Note:** This is a PACS only feature. This setting has no functionality or battery life impact when used with ENGAGE.
Performance	Affects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Reduces battery life by a few months as the device scans more frequently.

Adjusting the settings here will change the settings for the currently selected device ONLY.

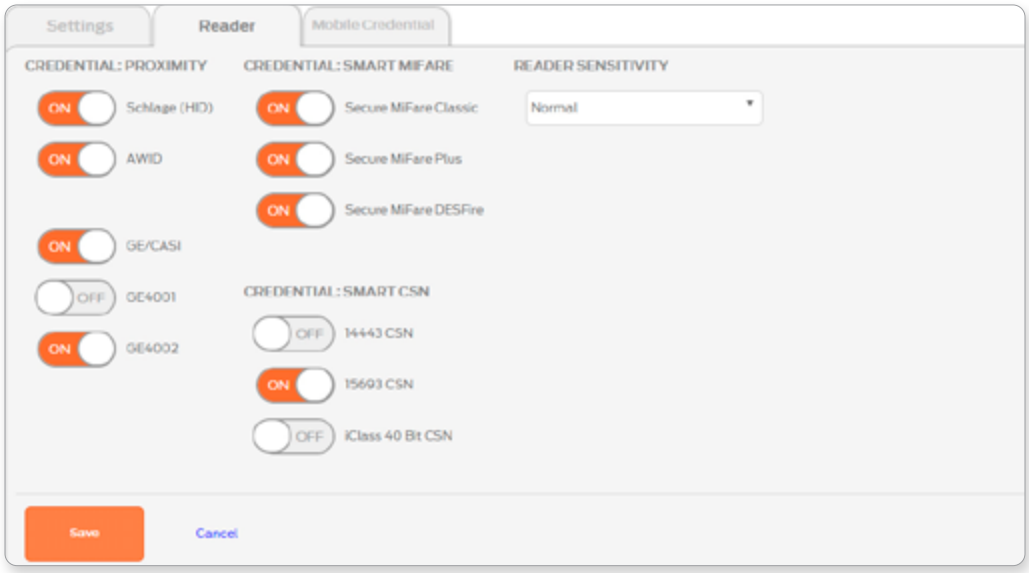
LE and LEB

Adjust as needed and Save to apply changes.



Reader Sensitivity is set to Normal by default and is recommended for most properties. Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.

For best reader response and improved battery life, disable any credential technology that is not needed.



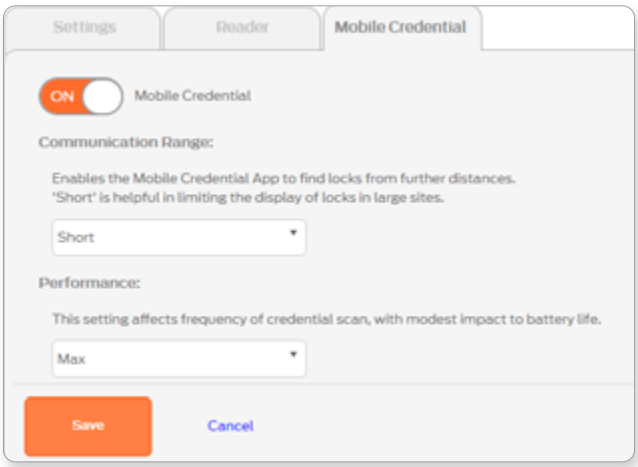


Fig. 9.68: LE Individual Settings

Table 9.3 LE and LEB Device Settings	
Setting	**Description**
Name	The name of the device
Settings Tab	
Relock Delay (seconds)	Immediately after unlocking, set the lock to automatically relock itself between 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 225 seconds.
Record Propped Door Audit After	Reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Power Fail Mode	Defines what the lock should do when entering Critical Battery Mode. • Secure : Locked • Passage: Unlocked • AS IS: no change
Schedules	Assign schedules
"First-Person-In" Unlocks Door	The First Person-in rule keeps a door locked until after a scheduled unlocked AND a valid credential has been presented. The door will then unlock and remain unlocked until the scheduled relock time. This feature prevents access until a valid user is present.
Holidays	Assign Holidays
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent
Blink Interior LED	Requires a DPS sensor and Privacy or Apartment lock functions. • ON: LED on the inside of the device to blink while the door is locked and closed • OFF: default
Blink Interior LED rapidly	Requires a DPS sensor and Privacy or Apartment lock functions • ON: increases how often the Inside LED is flashing for better visibility. • OFF: default
Reader Tab	
Credential Reader: Prox in Use	Choose the technology used by readers in your site: • Schlage (HID) • AWID • GE/CASI • GE4001 • GE4002
Credential Reader: Smart in Use	Choose the technology used by readers in your site: • MIFARE CSN • Secure MIFARE Classic • Secure MIFARE Plus • Secure MIFARE DESFire • 15693 UID (CSN) • iClass 40 Bit UID (CSN)
Reader Sensitivity	• Set to Normal by default and is recommended for most properties. • Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.
Mobile Credential Tab	
Mobile Credential	• OFF: Mobile Credential use is disabled. • ON: lock will accept Mobile Credential access
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.
Performance	Affects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Reduces battery life by a few months as the device scans more frequently.

For best reader response and improved battery life, disable any credential technology that is not needed.

Notice that as you enable certain settings, other settings are disabled. Some settings conflict and therefore cannot be enabled at the same time.

These are the individual default Settings for the selected NDE product family.

Adjusting the settings here will only change the settings for the currently selected device.

NDE80 and NDEB

Adjust as needed and Save to apply changes.

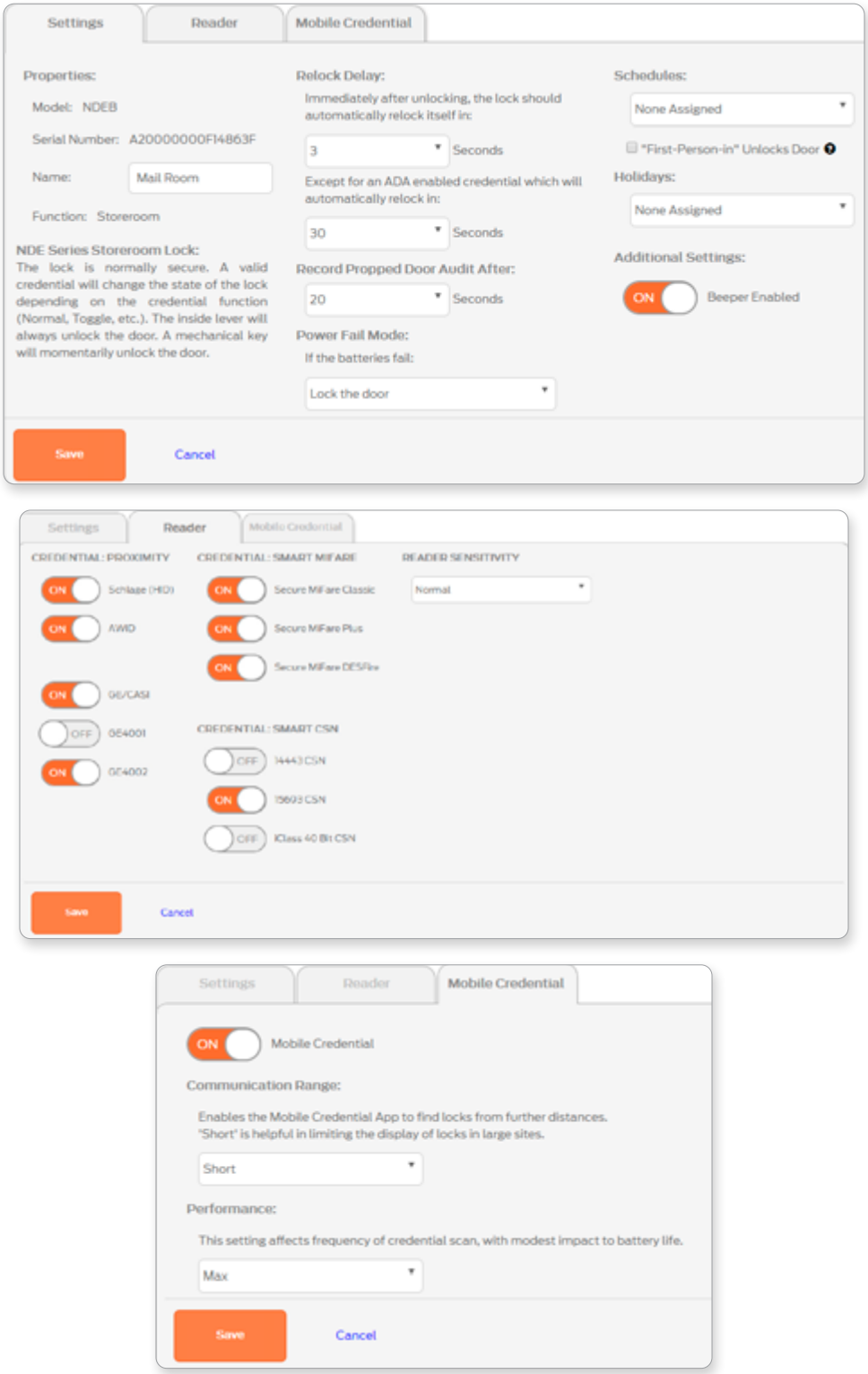


Fig. 9.69: NDEB Individual Settings

Table 9.4 NDE80 and NDEB Device Settings	
Setting	**Description**
Settings Tab	

For best reader response and improved battery life, disable any credential technology that is not needed.

Notice that as you enable certain settings, other settings are disabled. Some settings conflict and therefore cannot be enabled at the same time.

Table 9.4 NDE80 and NDEB Device Settings

Setting	Description
Name	The name of the device
Relock Delay (seconds)	Immediately after unlocking, set the lock to automatically relock itself between 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 225 seconds.
Record Propped Door Audit After	Reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Power Fail Mode	Defines what the lock should do when entering Critical Battery Mode. • Secure : Locked • Passage: Unlocked • AS IS: no change
Schedules	Assign schedules
“First-Person-In” Unlocks Door	The First Person-in rule keeps a door locked until after a scheduled unlocked AND a valid credential has been presented. The door will then unlock and remain unlocked until the scheduled relock time. This feature prevents access until a valid user is present.
Holidays	Assign Holidays
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent
Reader Tab	
CREDENTIAL: PROXIMITY	Choose the technology used by readers in your site: • Schlage (HID) • AWID • GE/CASI • GE4001 • GE4002
CREDENTIAL: SMART MIFARE	Choose the technology used by readers in your site: • Secure MIFARE Classic • Secure MIFARE Plus • Secure MIFARE DESFire
CREDENTIAL: SMART CSN	• MIFARE CSN • 15693 CSN • iClass 40 Bit CSN
CREDENTIAL: SMART HID ICLASS	• Secure HID iClass, SE, SEOS
Reader Sensitivity	• Set to **Normal** by default and is recommended for most properties. • Use a Reader Sensitivity of **High** or **Max** to enable a more reliable reading of physically smaller key fobs due to smaller antenna.
Mobile Credential Tab	
Mobile Credential	• OFF: Mobile Credential use is disabled. • ON: lock will accept Mobile Credential access
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.
Performance	Affects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Reduces battery life by a few months as the device scans more frequently.

These are the individual default Settings for the selected XE360 product family.

Adjusting the settings here will only change the settings for the currently selected device.

XE360

Adjust as needed and Save to apply changes.

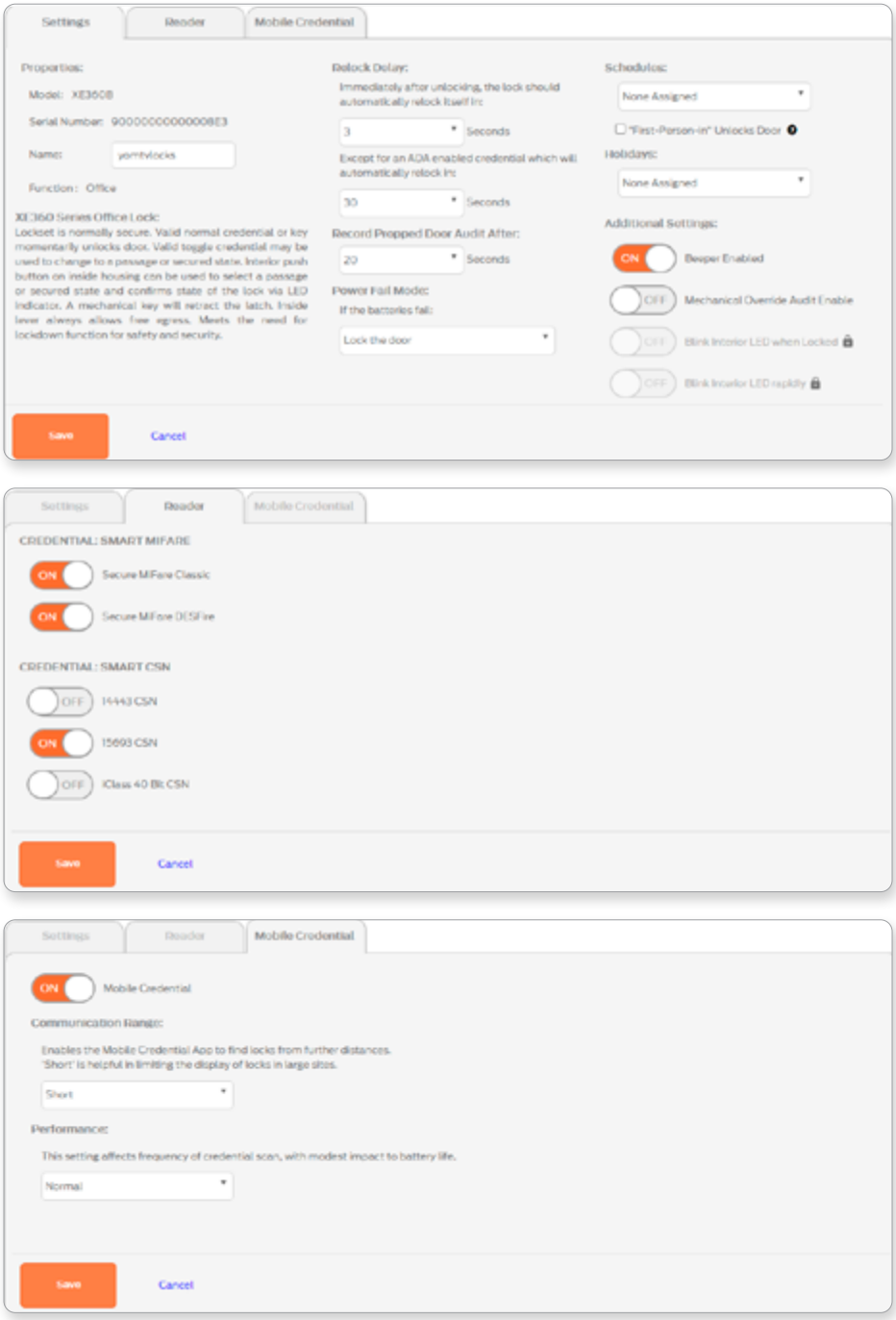


Fig. 9.70: XE360 Individual Settings

Table 9.5 XE360 Device Settings	
Setting	**Description**
Settings Tab	
Name	The name of the device
Relock Delay (seconds)	Immediately after unlocking, set the lock to automatically relock itself between 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 225 seconds.
Record Propped Door Audit After	Reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Power Fail Mode	Defines what the lock should do when entering Critical Battery Mode. • Lock the door • Unlock the door • Leave door in existing state (as-is)
Schedules	Assign schedules
"First-Person-In" Unlocks Door	The First Person-in rule keeps a door locked until after a scheduled unlocked AND a valid credential has been presented. The door will then unlock and remain unlocked until the scheduled relock time. This feature prevents access until a valid user is present.
Holidays	Assign Holidays
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent
Mechanical Override Audit Enbled	• ON: mechanical override audits will be available • OFF: mechanical override audits will not be available
Blink Interior LED when Locked	• Display only, not editable
Blink Interior LED rapidly	• Display only, not editable
Reader Tab	
CREDENTIAL: SMART MIFARE	Choose the technology used by readers in your site: • Secure MIFARE Classic • Secure MIFARE DESFire
CREDENTIAL: SMART CSN	• 1443 CSN • 15693 CSN • iClass 40 Bit CSN
Mobile Credential Tab	
Mobile Credential	• OFF: Mobile Credential use is disabled. • ON: lock will accept Mobile Credential access
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.
Performance	Affects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Reduces battery life by a few months as the device scans more frequently.

For best reader response and improved battery life, disable any credential technology that is not needed.

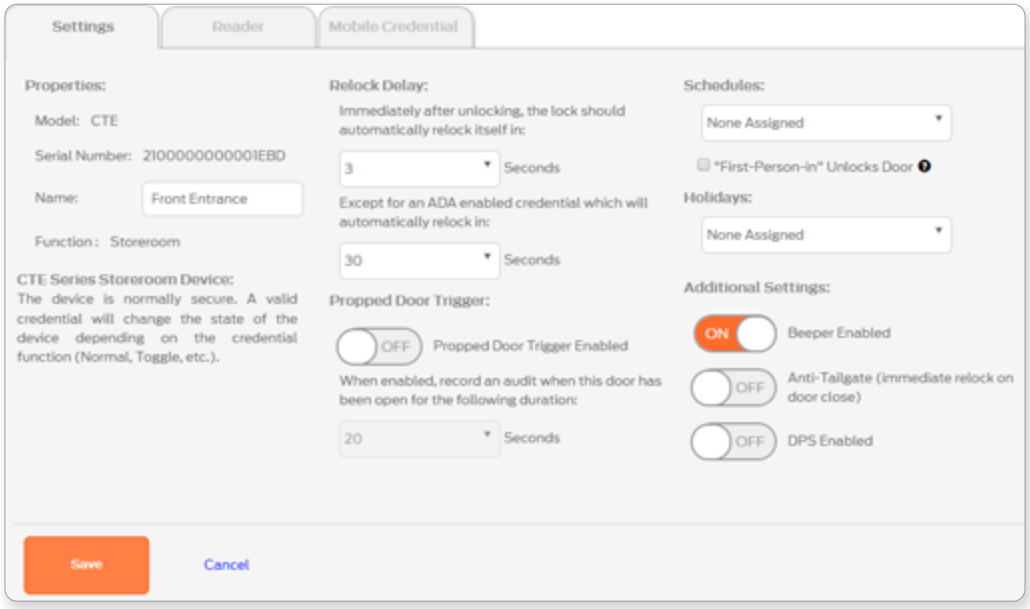
Notice that as you enable certain settings, other settings are disabled. Some settings conflict and therefore cannot be enabled at the same time.

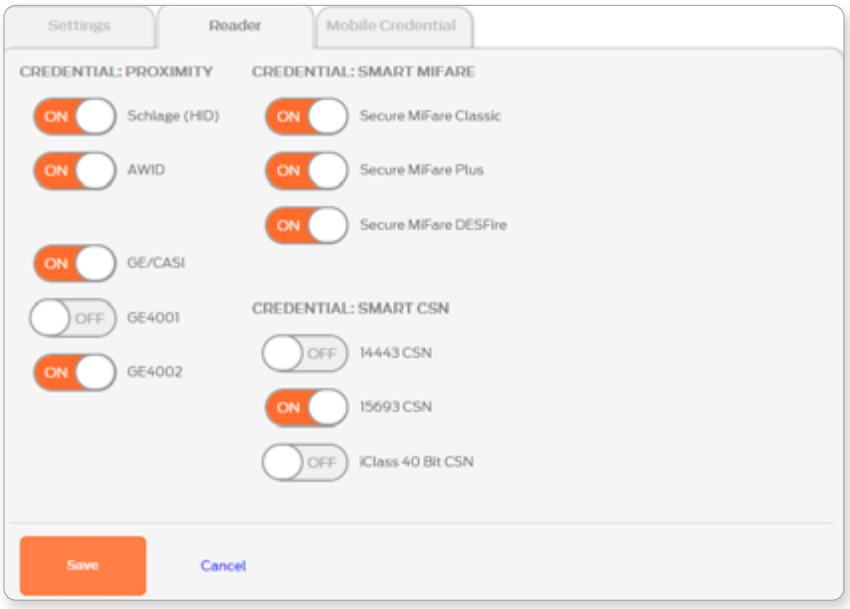
These are the individual default Settings for the selected CTE/MTB product family.

Adjusting the settings here will only change the settings for the currently selected device.

CTE/MTB

Adjust as needed and Save to apply changes.





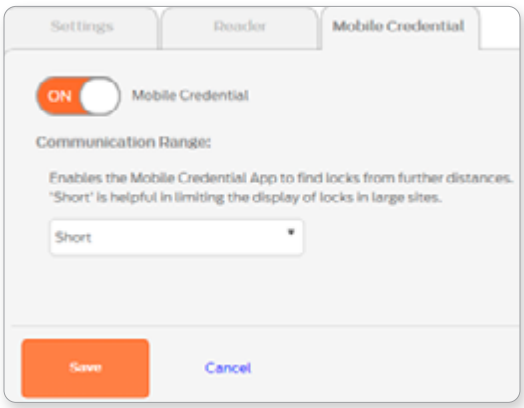


Fig. 9.71: CTE/MTB Individual Settings

For best reader response and improved battery life, disable any credential technology that is not needed.

Notice that as you enable certain settings, other settings are disabled. Some settings conflict and therefore cannot be enabled at the same time.

Table 9.6 CTE/MTB Device Settings

Setting	Description
Settings Tab	
Name	Name of the device
Relock Delay (seconds)	When a valid credential is presented, the locking device unlocks and then relocks. Delayed relocks are from 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 30 seconds.
Propped Door Delay Enabled	• ON (enabled): the Propped Door Delay selection is required. • OFF: the following option is not available ➔ **Note:** The setting applies ONLY to devices that support Door Position Sensor (DPS) for Propped Door Audits.
Propped Door Delay (seconds)	ON: reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Schedules	Assign schedules
"First-Person-In" Unlocks Door	The First Person-in rule keeps a door locked until after a scheduled unlocked AND a valid credential has been presented. The door will then unlock and remain unlocked until the scheduled relock time. This feature prevents access until a valid user is present.
Holidays	Assign Holidays
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent
Anti-Tailgate	• OFF: no special action is taken, the device relocks on the normal relock schedule. • ON: the CTE will use the DPS sensor to immediately relock when the door closes and terminate the relocking period upon closure.
DPS Enabled	• OFF: use when no DPS is installed. • ON: the CTE will know that a DPS is installed and can enable the Door Propped and Anti-tailgate features.
Reader Tab	
Credential Reader: Prox in Use	Choose the technology used by readers in your site: • Schlage (HID) • AWID • GE/CASI • GE4001 • GE4002
Credential Reader: Smart in Use	Choose the technology used by readers in your site: • MIFARE CSN • MIFARE Classic • Secure MIFARE Plus • Secure MIFARE DESFire • 15693 UID (CSN) • iClass 40 Bit UID (CSN)
Reader Sensitivity	• Set to Normal by default and is recommended for most properties. • Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.
Mobile Credential Tab	
Mobile Credential	• OFF: Mobile Credential use is disabled. • ON: lock will accept Mobile Credential access
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.

Delete Device

1. **Log In**.
2. Select the Devices menu and the Devices pull down.
3. Select device from the device list.

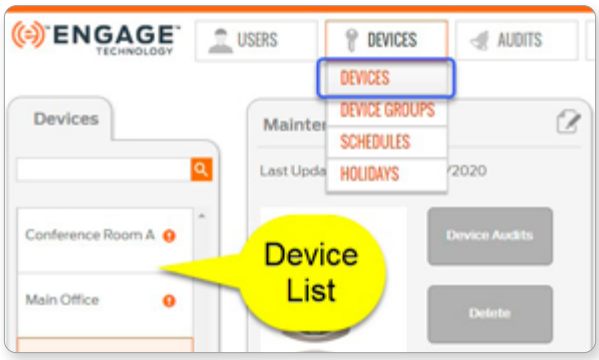
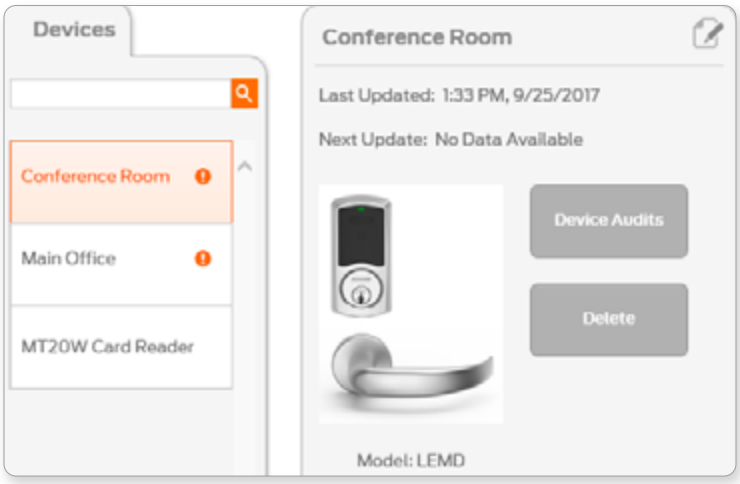


Fig. 9.72: Devices > Devices

4. Select the Delete button.



5. Type delete into the Confirm: box. Select the Delete button to continue.

6. The Device deleted confirmation message will be displayed.

➔ **Note:** FDR (factory default reset) should be performed on the device if it will be used again. See the device documentation for more information.

⚠ CAUTION: ANY change made to a user schedule for sites using No Tour Device Groups will require ALL credentials to be collected and placed on the MT20W for programming.

Device Groups

Device Groups are created to manage any number of doors which have common user access such as a lobby, garage or a pool area.

Device Groups reduce the number of sector (or folder) assignments on a user's physical credential. Individual openings assigned into a Device Group are treated as a single assignment when programming the user credential and requires only one credential sector for access to all doors in the group. Mobile credentials do not have this credential sector limitation.

For a more efficient ENGAGE property setup process, Administrators should define any Device Groups as a "Best Practice" prior to making any individual user access assignments.

➔ **Note:** Devices must be commissioned before they are available for inclusion into a Device Group.

Add Device Group

1. **Log In**.
2. Select the Devices menu and the Device Groups pull down.

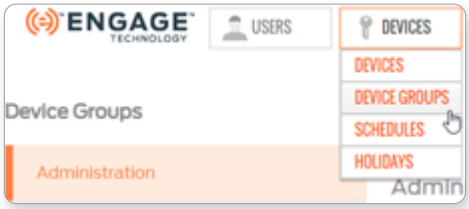


Fig. 9.73: Devices > Device Groups

3. Select Add New Group.

Fig. 9.74: Add New Device Group

4. From the Add New Device Group screen, complete required fields:
   a. Name: enter a descriptive Device Group name.
   a. Description: enter the description so others can easily recognize the purpose of the group.
   b. When finished, Select Save.

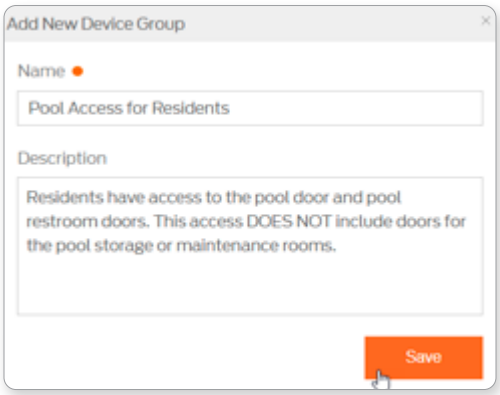


Fig. 9.75: Descriptive Device Group

5. The Device group added successfully confirmation message will be displayed.

➔ **Note:** You should now add devices to the device group. See **Assign Devices to Device Group**.

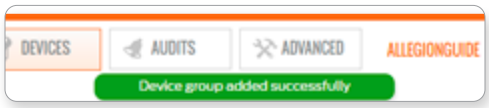


Fig. 9.76: Device Group Added Confirmation

Assign Devices to Device Group

WARNING: A device can be included in ONLY one Device Group. Device Groups should be very static and not require frequent updates. Any updates to a Device Group require a sync of each affected device in the group before the group update is valid.

1. **Log In**.
2. Select the Devices menu and the Device Groups pull down.

Fig. 9.77: Devices > Device Groups

3. Select the device group to which you want to assign/remove devices.

➔ **Note:** If you have not yet created a device group, you will need to do that first. See **Add Device Group**.

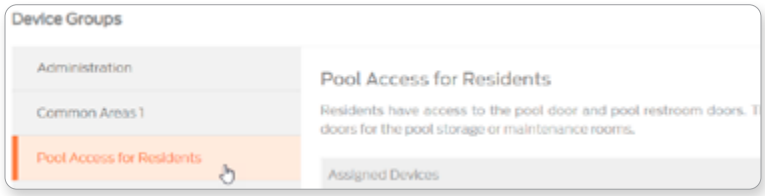


Fig. 9.78: Select Device Group

4. Select the plus sign (+).

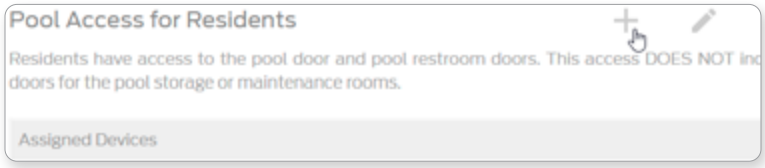


Fig. 9.79: Assign/Remove Devices Button

To select more than one device at a time, hold Ctrl and then select each device.

5. From the Assign devices screen, select the appropriate door(s) to be assigned to the group.
   - Select a device from the Unassigned Devices list.
   - Select > to move device into the Assigned Devices column.
   - Select < to move a device into the Unassigned Devices column.
   - Select >> or << to assign or unassign all devices.
6. When finished, select Save.

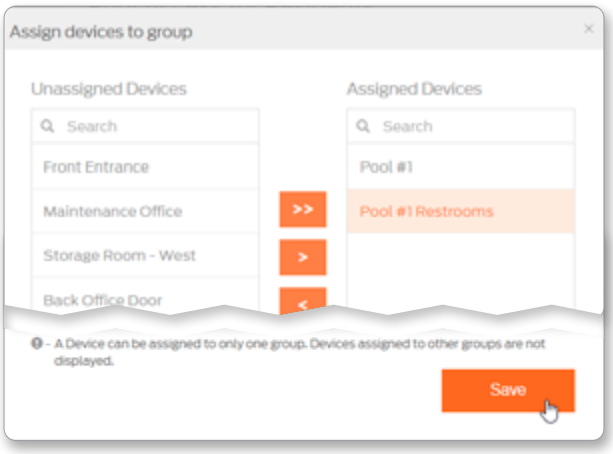


Fig. 9.80: Assign Devices Screen

7. The Devices for group updated successfully message appears.
   - The Device Group also now displays the Assigned Devices.

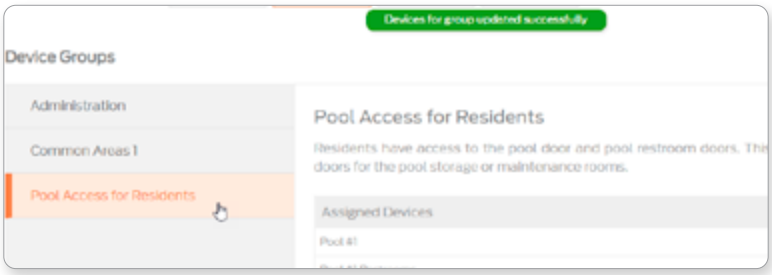


Fig. 9.81: Assigned Devices in Device Group

Only the Administrator can create, edit, and assign Access and Device schedules.

User Schedules may be created before any actual users are entered.

A device unlocking schedule and a device locking schedule will require two device schedule assignments to be defined

CAUTION: ANY change made to a user schedule for sites using No Tour Device Groups will require ALL credentials to be collected and placed on the MT20W for programming.

Schedules

There are two types of Schedules:

- Add Schedule (Users): pg 46
- Add Device Schedule: pg 62

BEST PRACTICE: All schedules should be defined before any devices are commissioned. Devices must be updated before new schedules will be implemented.

Add Device Schedule

Device Schedules are defined to schedule automatic lock/unlock operations at a door. A maximum of eight (8) Device Schedules can be defined per property.

➔ **Note:** Think of Device Schedules as Open Hours, Lock up Time, etc.

CAUTION: Control Mobile Enabled Smart Locks DO NOT support Device Schedules.

1. **Log In.**
2. Select Devices > Schedules.

Fig. 9.82: Devices > Schedules

3. Select Add New Event Schedule.

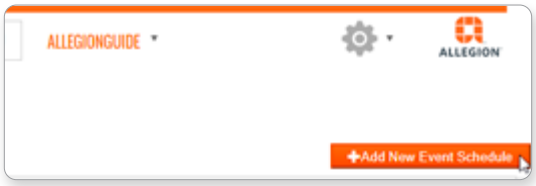


Fig. 9.83: Add New Schedule Button

4. From the Add New Schedule screen, complete required fields.

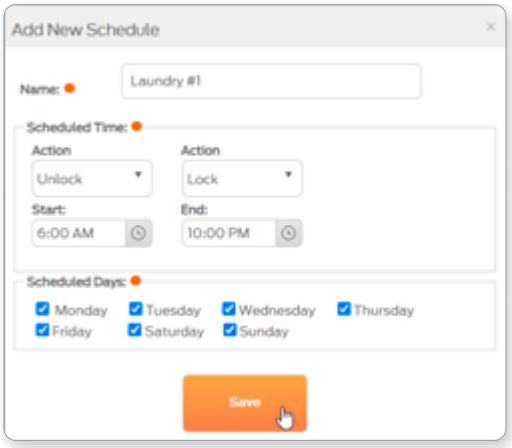


Fig. 9.84: Add New Schedule

5. Select the Save button.
6. You will now need to assign devices to the schedule.

Table 9.7 Device Schedule Action Definitions	
Unlock	Anyone can pass through door without a credential
Lock	Credential required to access door
Do Nothing	Lock state does not change

Undog	Applicable only for RM/RU Devices
Dog on Next Exit	

A device unlocking schedule and a device locking schedule will require two device schedule assignments to be defined

Assign Devices to a Schedule

CAUTION: Control Mobile Enabled Smart Locks DO NOT support Device Schedules.

1. **Log In.**
2. Select Devices > Schedules.

Fig. 9.85: Devices > Schedules

3. Select the schedule to which you want to assign devices. The schedule will be displayed.
4. Select Assign Devices.

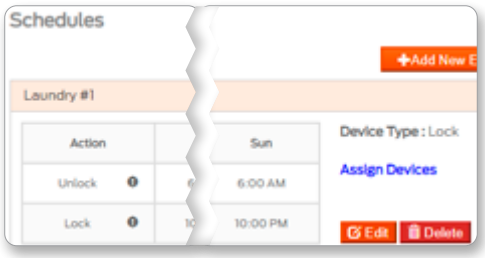


Fig. 9.86: Schedules

To select more than one device at a time, hold Ctrl and then select each device.

5. From the Assign Devices screen:
   - Select a device from the Unassigned Devices list.
   - Select < to move device into the Assigned Devices column.
   - Select > to move a device into the Unassigned Devices column.
   - Select >> or << to assign or un-assign all devices.
6. When finished, select Save.

Fig. 9.87: Assign devices

CAUTION: Devices that use the schedule must be programmed before the schedule will be updated. ! is shown next to doors that require programming.

Remove Devices from a Schedule

Use the same process as **Assign Devices to a Schedule**.

Edit Device Schedule

1. **Log In.**
2. Select Devices > Schedules.

Fig. 9.88: Devices > Schedules

3. Select the schedule you want to edit. The schedule will be displayed.
4. Select the Edit button.

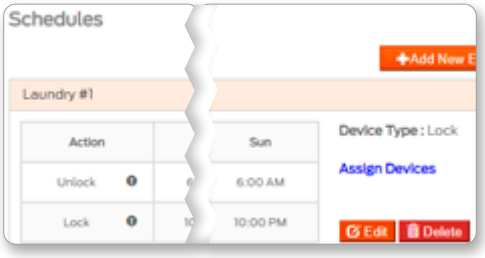


Fig. 9.89: Schedules

5. From the Edit Schedule screen, complete required fields.
6. Select the Save button.

➔ **Note:** Editing the schedule does not change which devices are assigned. See **Assign Devices to a Schedule** on page **63** for more information.

CAUTION: Devices that use the schedule must be programmed before the schedule will be updated. ! is shown next to doors that require programming.

➔ **Note:** If using no-tour, credentials will need to be collected and placed on an MT20W.

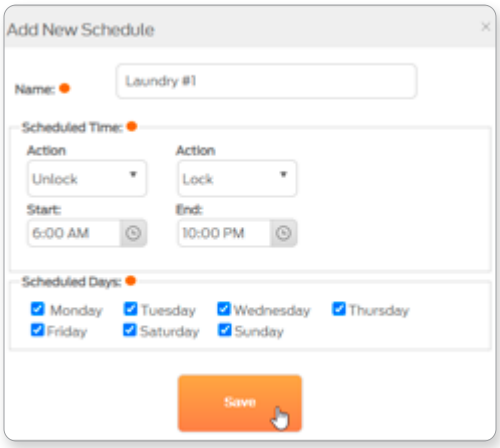


Fig. 9.90: Edit Schedule

Delete Device Schedule

1. **Log In.**
2. Select Devices > Schedules.

Fig. 9.91: Devices > Schedules

3. Select the schedule you want to delete. The schedule will be displayed.
4. Select the Delete button.

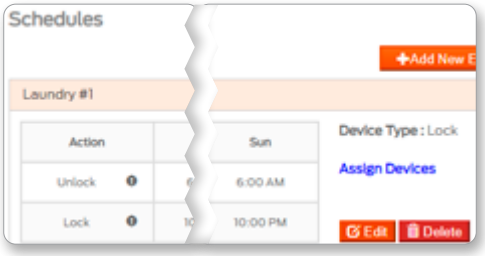


Fig. 9.92: Schedules

5. Select the OK button.

> **CAUTION:** Devices that use the schedule must be programmed before the schedule will be updated. ! is shown next to doors that require programming.

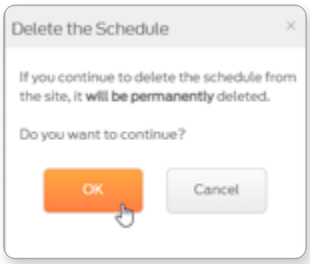


Fig. 9.93: Edit Schedule

Holidays

Holidays are defined by the Administrator to manage doors during holidays or scheduled special events. A maximum of 32 Holiday can be defined per property. Holidays can be defined to span multiple days when necessary, with specific start and stop times. Locks can be set to locked or unlocked. User access during Holidays can be also specified.

CAUTION: Control Mobile Enabled Smart Locks DO NOT support Holiday Schedules.

User access levels

Restricted Access: Pass-Through credential function access ONLY

Locked: Valid credential presentation is required for access

Unlocked: No credential required; passage access is provided

Add Holiday Schedule

Holidays are defined by the Administrator to manage doors during holidays or scheduled special events. A maximum of 32 Holiday can be defined per property. Holidays can be defined to span multiple days when necessary, with specific start and stop times. Locks can be set to locked or unlocked. User access during Holidays can be also specified.

CAUTION: Control Mobile Enabled Smart Locks DO NOT support Holiday Schedules.

1. **Log In.**
2. Select Devices > Holidays.

Fig. 9.94: Devices > Holidays

3. Select Add New Holiday.

Fig. 9.95: Add New Holiday Button

4. From the Add New Holiday screen, complete the required fields:

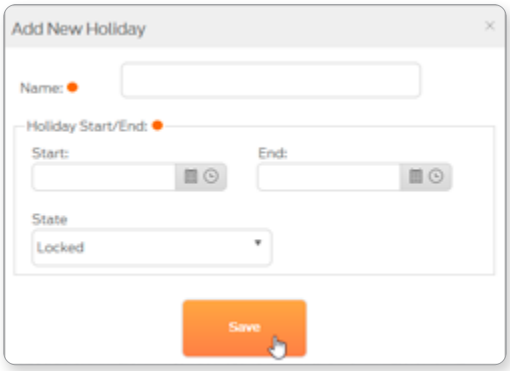


Fig. 9.96: Add New Holiday

5. Select the Save button.

Table 9.8 Holiday Schedule States	
Locked	Credential required to access door
Unlocked	Anyone can pass through door without a credential
Restricted Access	Passthrough credential required to access door
Undog	Applicable only for RM/RU Devices
Dog on Next Exit	

Assign Devices to a Holiday Schedule

CAUTION: Control Mobile Enabled Smart Locks DO NOT support Holiday Schedules.

1. **Log In.**
2. Select Devices > Holidays.

Fig. 9.97: Devices > Holidays

3. Select the holiday to which you want to assign devices. The holiday will be displayed.
4. Select Assign Devices.

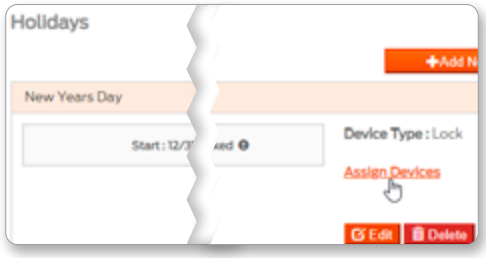


Fig. 9.98: Holidays

To select more than one device at a time, hold Ctrl and then select each device.

5. From the Assign Devices screen:
   - Select a device from the Unassigned Devices list.
   - Select < to move device into the Assigned Devices column.
   - Select > to move a device into the Unassigned Devices column.
   - Select >> or << to assign or un-assign all devices.
6. When finished, select Save.

Fig. 9.99: Assign devices

CAUTION: Devices that use the holiday must be programmed before the holiday will be updated. ! is shown next to doors that require programming.

Remove Devices from a Holiday Schedule

Use the same process as **Assign Devices to a Holiday Schedule**.

Edit Holiday Schedule

1. **Log In.**
2. Select Devices > Holidays.

Fig. 9.100: Devices > Holidays

3. Select the holiday you want to edit.
4. Select the Edit button.

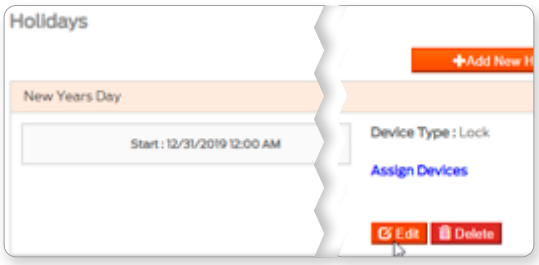


Fig. 9.101: Edit Holiday Button

5. From the Edit Holiday screen, complete the required fields:

Name	Enter a descriptive name for the holiday.
Holiday Start	Select the desired start date and time.
Holiday End	Select the desired end date and time.
State	Select the desired state of the door during this holiday. See **Holiday Schedule States on page 66**.

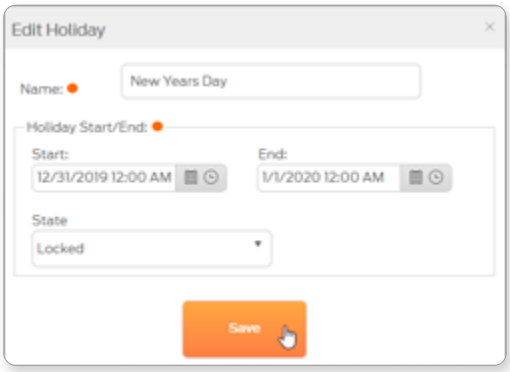


Fig. 9.102: Edit Holiday

6. Select the Save button.

Delete Holiday Schedule

1. **Log In.**
2. Select Devices > Holidays.

Fig. 9.103: Devices > Holidays

3. Select the holiday you want to edit.
4. Select the Delete button.

Fig. 9.104: Delete Holiday Button

5. Select the OK button.

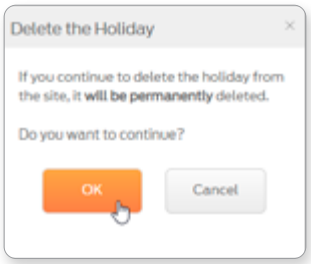


Fig. 9.105: Delete Holiday

Audits

Schlage NDE80, NDEB, LE, LEB, and CTE devices will "Call in" to ENGAGE every night when the Wi-Fi network communication settings are enabled and properly set up. New or updated access rights, schedule additions or changes, device settings updates, and all recent Device and User audits are gathered during nightly Wi-Fi network "Call in."

➔ **Note:** Use the ENGAGE Mobile Application **Test Wi-Fi Connection** feature to verify network settings and proper communication.

⚠ CAUTION: Control Mobile Enabled Smart Locks do not support Wi-Fi connectivity and the nightly "Call in" feature is not available with Control Mobile Enabled Smart Locks. All Control Mobile Enabled Smart Lock updates and Audit gathering must be accomplished at the door using the ENGAGE Mobile Application Sync process.

View Audits for Individual Device

1. **Log In.**
2. Select Devices > Devices.

Fig. 9.106: Devices > Devices

3. Select the desired device from the list.

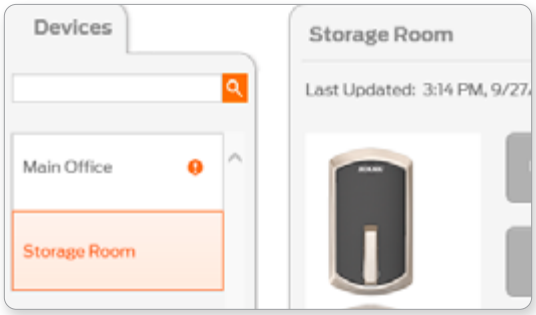


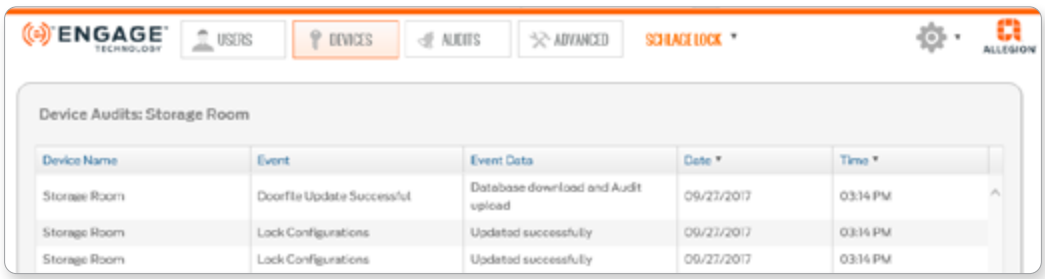
Fig. 9.107: Select Device

4. Select Device Audits button.

Fig. 9.108: Select Device Audits

5. View the available device Audits

➔ **Note:** Use the column headers to quickly sort and find the displayed Audit data.



View Audits for Entire Property

1. **Log In.**
2. Select Audits.

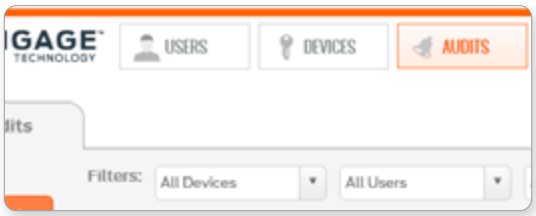
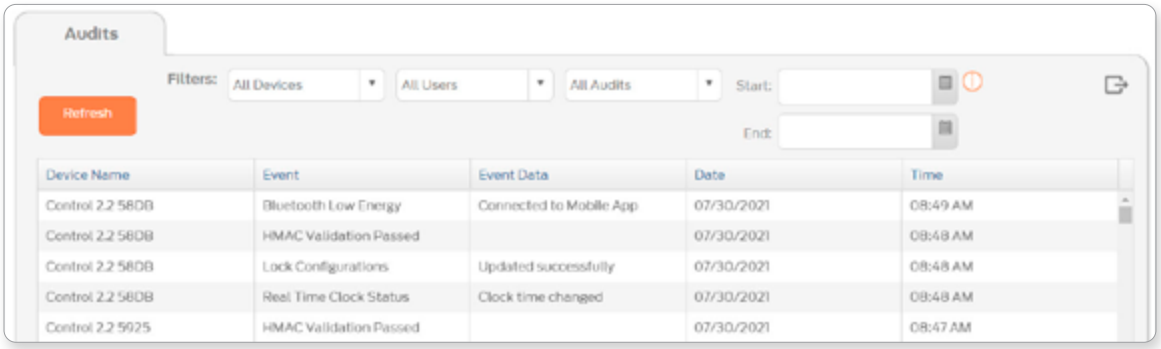


Fig. 9.109: Audits

3. View the available Audits

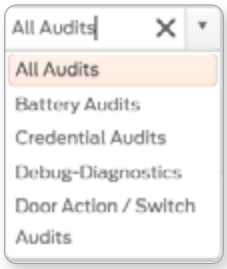
➔ **Note:** Use the column headers to quickly sort and find the displayed Audit data.



4. Use the available Sort and Filter options, as desired.

   ➔ **Note:** Use the Sort and filter options and column headers to quickly sort the displayed Audit data.

   - Sort by all Devices or a specific device
   - Sort by all Users or a specific User
   - Sort by Audit Types (see below)
   - Sort by Start and Stop timeframes



5. Export Audits using the square EXPORT button (Top-Right corner of screen).

   - Data is saved into a .csv file for easy spreadsheet analysis.
   - Save your audit file to disk for archive and analysis.

➔ **Note:** Select the Refresh button to display the latest information.

Team Member assignments and updates can be managed in the ENGAGE web and Mobile applications.

The **ENGAGE web application is preferred** due to ease of entry.

My Team

Adding Team Members allows other individuals to help the Administrator manage the property. Team members can be assigned roles to allow or limit specific capabilities.

➔ **Note:** For specific capabilities of each role, see **Appendix A: Capabilities by Property Role** on page **202**.

Table 9.9 Team member roles

Type	Add Admins	Add Managers	Add Operators	Add/edit users and devices	General maintenance
Administrators	✓	✓	✓	✓	✓
Managers			✓	✓	✓
Operators					✓

Notice one Administrator has already been added. When the ENGAGE account is created, the first user is assigned as the Administrator.

Add Team Member

1. **Log In.**
2. Select the Advanced menu.
3. Select the Add Team Member button on the My Team tab.

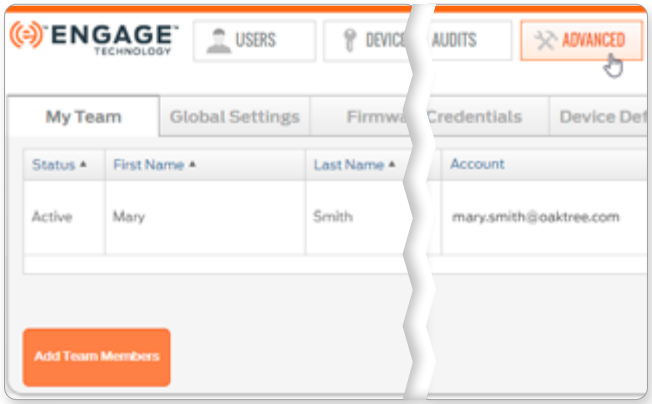


Fig. 9.110: Advanced > My Team

Hover over the question mark for role definitions.

4. In the Invite New Team Members screen, complete all fields:

First Name	enter the first name
Last Name	enter the last name
Email Address	enter the team member's email address
Role	select appropriate role. See **Table 9.9 Team member roles**.

5. Select the Send Invitation button.

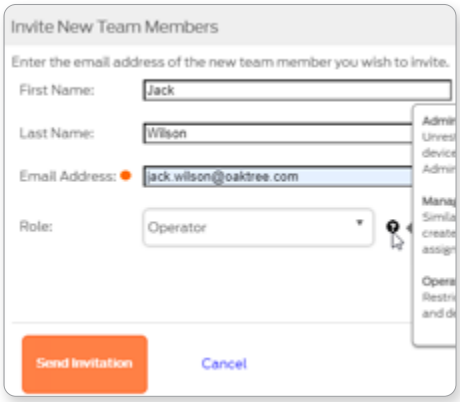


Fig. 9.111: Invite New Team Members

6. View the new team member details listed in the My Team tab. The status will be Invited. The invitation will expire six (6) days after it was sent.

   ➔ **Note:** If the invitation expires, see **Resend Mobile Credential Invitation**.

If the email is not received within a few minutes, have the user check their spam and trash folders.

Invitation expires six (6) days after date sent

If email is **never received**, see **Resend or Delete Invitation** on page **74**.

Create New Account

After the Administrator sends the invitation, the new team member will receive an email that contains a link to accept the invitation.

1. The newly invited team member should go to their email account and open the Allegion ENGAGE Invitation verification email. Select the Accept This Invite link.

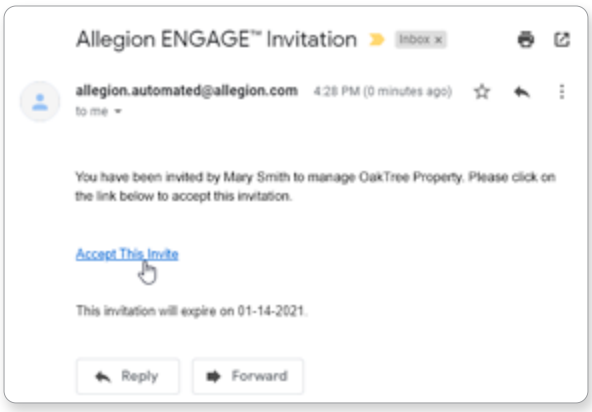


Fig. 9.112: Allegion ENGAGE Invitation Email

2. Read the Terms & Conditions and select the I Accept button to acknowledge and accept the terms and conditions.

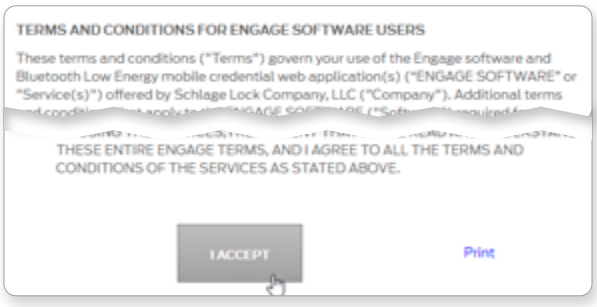


Fig. 9.113: Accept Terms & Conditions

Password Rules:

- At least 10 characters
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 number or symbol
- Not more than 2 identical characters in a row

3. Enter the Account details. Click to check the box to accept the terms and conditions.
4. Select the Submit button.
5. The new team member will receive an email verification message that must be accepted before they can assist with property management.

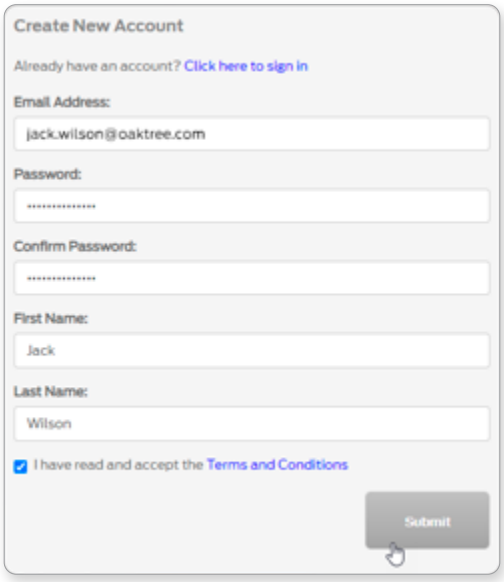


Fig. 9.114: Create new account

Resend or Delete Invitation

Notice the status of each team member. A member who has been invited but has not yet set up and verified their account will show Invited.

It may be necessary to resend or delete an invitation.

1. **Log In.**
2. Select the Advanced menu.
3. From the My Team tab, select Manage for the appropriate member.

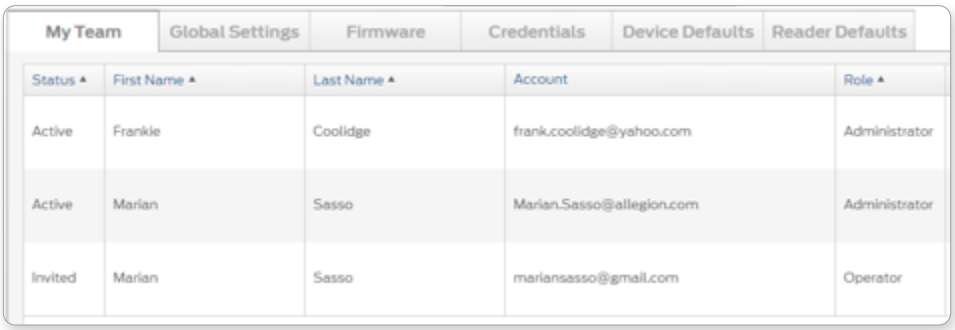


Fig. 9.115: Manage Team Member

4. From the Manage Invitees screen, verify the email address.
   a. If the email address is correct, select Re-Send Invitation.
   b. If the email address is incorrect, select Delete Invitation, and then begin the process again.

Global Settings

These settings affect the entire site.

Table 9.10 Global Settings

Setting	Description	
Time Zone	Time Zone of the site	
Market Segment	Type of site	
Daylight Savings Time	On or Off depending on the location of site	
Wi-Fi Alerts	Enable devices to send Wi-Fi alerts. This feature only affects NDE, LE, and CTE devices and can be disabled to extend battery life.	
Master Credentials	Enable creating master credentials to access all locks on the site. See **Using Master Credentials** for more information.	
No-Tour	Allow cards to carry access updates to Lock. (Must have MT20W to write to smart cards). See **No-Tour Feature** for more information.	
Mobile Credential Settings		
Bit Format	26A	Unrestricted: Mobile Credential Settings may be edited
	34S	
	35X	
	37H	
	37X	
	48X	Restricted: Mobile Credential Settings CANNOT be edited
Facility Code	Enter an appropriate code. Each Facility Code has it's own Starting Badge ID.	
Starting Badge ID	See **Set or Modify the Starting Badge ID** on page **75** for more information.	

Set or Modify the Starting Badge ID

The Starting Badge ID feature in ENGAGE allows site admins to set the starting badge ID for Schlage mobile Bluetooth credentials. Previously, the starting badge ID was automatically set to zero. Now, admins can set and modify the starting badge ID, providing greater flexibility and control. This feature is available for both ENGAGE and PACS-managed sites and applies to open bit formats only.

➔ **Note:** Only ENGAGE Site Admins have the permissions to use this feature, and it is not available for restricted bit formats.

1. **Log In.**
2. Select the Advanced menu.
3. Select the Global Settings tab.
   ➔ **Note:** For PACS managed sites, select the Settings tab.
4. Under Mobile Credential Settings, choose the desired Bit Format.
5. Input the appropriate Facility Code.
6. Click the magnifying glass icon. The current starting badge ID will appear in the Starting Badge ID field, and Next Available [#] will appear below the field.
7. Input the desired starting badge ID in the Starting Badge ID field.
8. Click the Save button. You will see a success message: Starting Badge ID updated successfully.

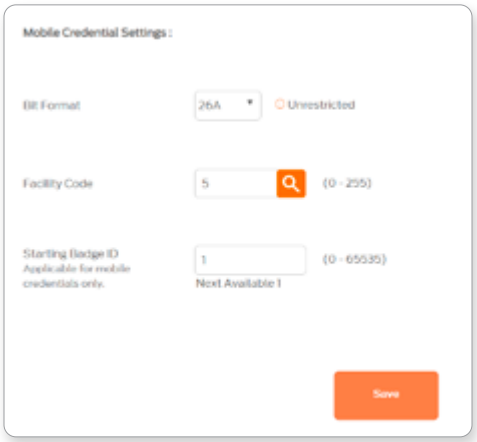


Fig. 9.116: Advanced > Global Settings > Mobile Credential Settings

After completing these steps, any new credential will have the badge ID starting from the set value.

➔ **Note:** While setting the starting badge ID, the text Next Available below the Starting Badge ID field indicates the next available ID that can be used. This helps in understanding the existing starting badge ID for a specific Bit Format and Facility Code combination.

Credentials

1. **Log In.**
2. Select the Advanced menu.
3. Select the Credentials tab.
4. From here, you can choose from the buttons on the left:
   - **Badge ID Search**
   - **View Mobile Credentials**
   - **View All Master Credentials**
   - **Delete Master Credentials**

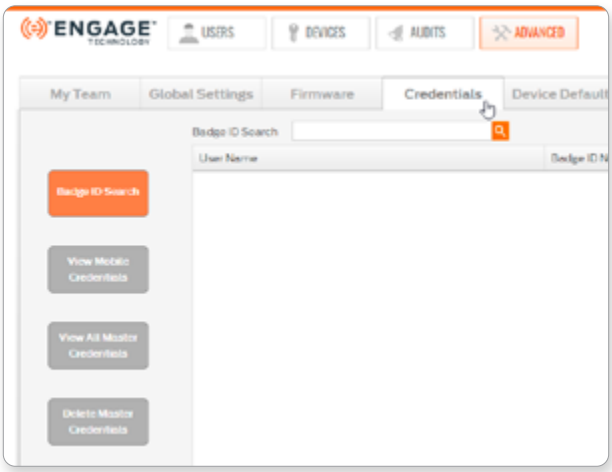


Fig. 9.117: Advanced > Credentials

The badge id search only applies to smart cards scanned on the MT20W device.

Badge ID Search

The Badge ID Search can be used to search for a badge ID so the User can be identified. The 'badge id' can be found on the credential. Enter the exact badge id numbers after the dash as in the example: S26A74678-1138. The badge id search only applies to smart cards scanned on the MT20W device.

View Mobile Credentials

Click the View Mobile Credential button to view all enrolled mobile credentials. You can also export mobile credentials to be used in other systems, such as PACS or PropTech access control systems. See **Exporting Mobile Credentials** for more information.

View All Master Credentials

Click the View All Master Credentials button to view the list of all the users with a master credential assigned by an Administrator. See **Using Master Credentials** for more information.

Delete Master Credentials

See **View and Delete Master Credential** for more information.

Administrators who review each device type and confirm the associated default settings **before commissioning** will save time setting up their property.

Each device is programmed with the Property Wide device default settings defined in the ENGAGE Web application upon commissioning.

Individual device settings may be adjusted after commissioning when desired.Select each device to view and update the desired device defaults.

Device Defaults

When a device is commissioned into ENGAGE, the currently defined Device Default settings in the ENGAGE Web application are loaded into that device. Administrators should think through their property needs and requirements before commissioning any devices to ensure the default settings in ENGAGE are properly set before commissioning any devices. Device settings may be edited and updated at any time however, setting up the device defaults before commissioning any devices provides for a consistent and less error prone installation and setup. Individual devices that need settings other than the property wide defaults may be individually adjusted when commissioning that device or at any time later.

WARNING: Any setting changes or updates made to an installed and previously commissioned device will require Sync or Over-night call-in updates.

Property-Wide Settings

1. **Log In.**
2. Select the Advanced menu then Device Defaults pull down.
3. The following sections are the property-wide default settings for locking devices. Review each setting to ensure the setting meets the property default settings requirements. Adjust as needed and Save to apply changes.
   - **Control Mobile Enabled Smart Lock** on page **78**
   - **CTE** on page **79**
   - **LE and LEB** on page **80**
   - **NDE80 and NDEB** on page **81**
   - **RU/RM** on page **82**

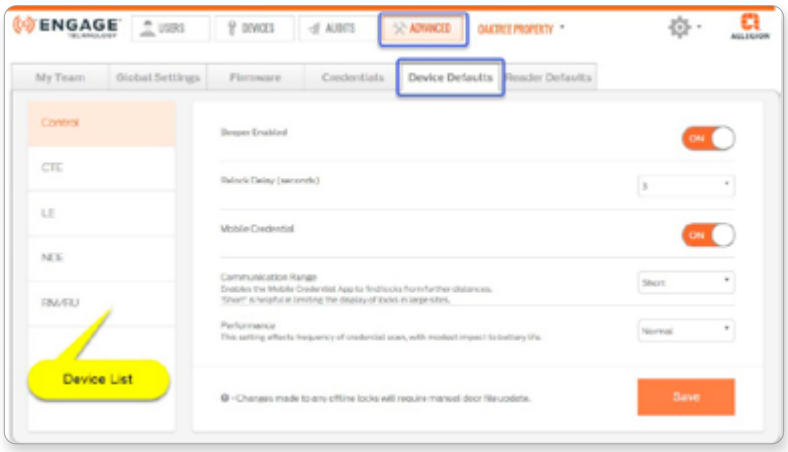


Fig. 9.118: Advanced > Device Defaults

Control Mobile Enabled Smart Lock

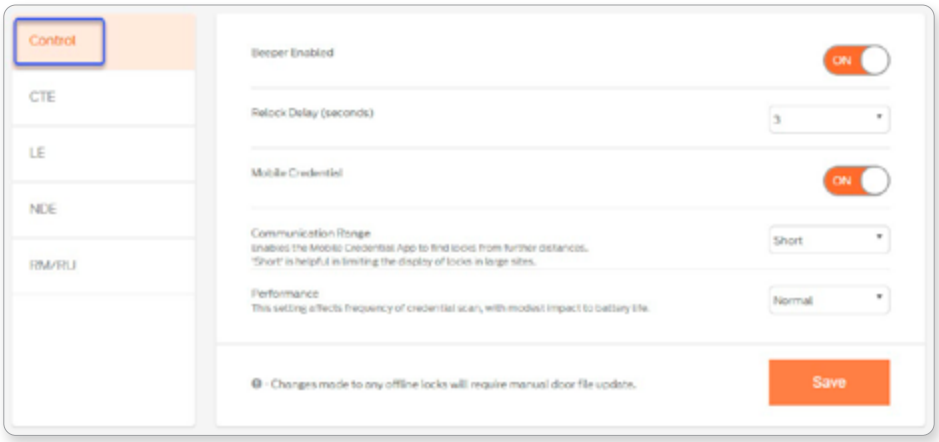


Fig. 9.119: Control Default Settings

Table 9.11 Control Mobile Enabled Smart Lock Property Wide Settings	
Setting	**Description**
Beeper Enabled	When set to ON the lock beeper will sound to provide device status. When set to OFF the lock beeper will remain silent.
Relock Delay	When a valid credential is presented, this is the time the deadbolt thumb turn is engaged for locking and unlocking. Delayed relocks are from 1 – 30 seconds.
Mobile Credential	• ON: Lock will accept Mobile Credential access and the following options are available. • OFF: Mobile Credential use is disabled
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.
Performance	This setting effects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Max setting will reduce battery life by a few months as the device scans more frequently.

CTE

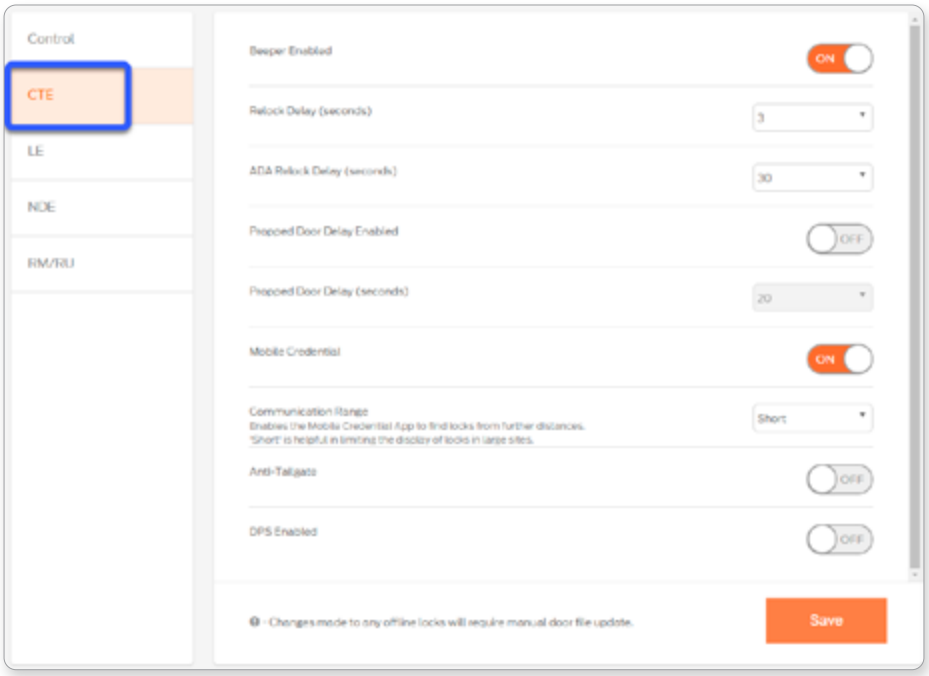


Fig. 9.120: CTE Default Settings

Table 9.12 CTE Device Property Wide Settings	
Setting	**Description**
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent.
Relock Delay (seconds)	When a valid credential is presented, the locking device unlocks and then relocks. Delayed relocks are from 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 30 seconds.
Propped Door Delay Enabled	• ON (enabled): the Propped Door Delay selection is required. • OFF: the following option is not available ➔ **Note:** The setting applies ONLY to devices that support Door Position Sensor (DPS) for Propped Door Audits.
Propped Door Delay (seconds)	ON: reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Mobile Credential	• ON: lock will accept Mobile Credential access and the following options are available. • OFF: Mobile Credential use is disabled
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts
Anti-Tailgate	• OFF: no special action is taken, the device relocks on the normal relock schedule. • ON: the CTE will use the DPS sensor to immediately relock when the door closes and terminate the relocking period upon closure.
DPS Enabled	• OFF: use when no DPS is installed. • ON: the CTE will know that a DPS is installed and can enable the Door Propped and Anti-tailgate features.

LE and LEB

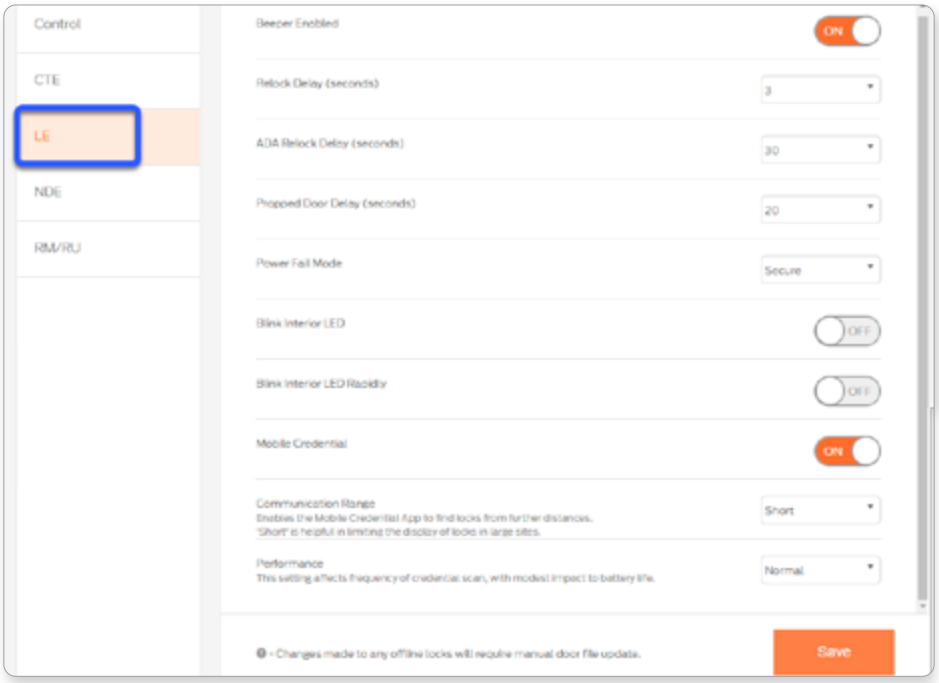


Fig. 9.121: LE Default Settings

Table 9.13 LE and LEB Device Property Wide Settings	
Setting	**Description**
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent.
Relock Delay (seconds)	When a valid credential is presented, the locking device unlocks and then relocks. Delayed relocks are from 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 30 seconds.
Propped Door Delay (seconds)	Reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Power Fail Mode	Defines what the lock should do when entering Critical Battery Mode. • Secure : Locked • Passage: Unlocked • AS IS: no change
Blink Interior LED	• ON: the Interior LED will blink while in Privacy Mode to inform the occupant of the secured status. • OFF: default
Blink Interior LED rapidly	• ON: increases how often the Inside LED is flashing for better visibility. • OFF: default
Mobile Credential	• OFF: Mobile Credential use is disabled. • ON: lock will accept Mobile Credential access and the following options are available.
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.
Performance	Affects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Reduces battery life by a few months as the device scans more frequently.

NDE80 and NDEB

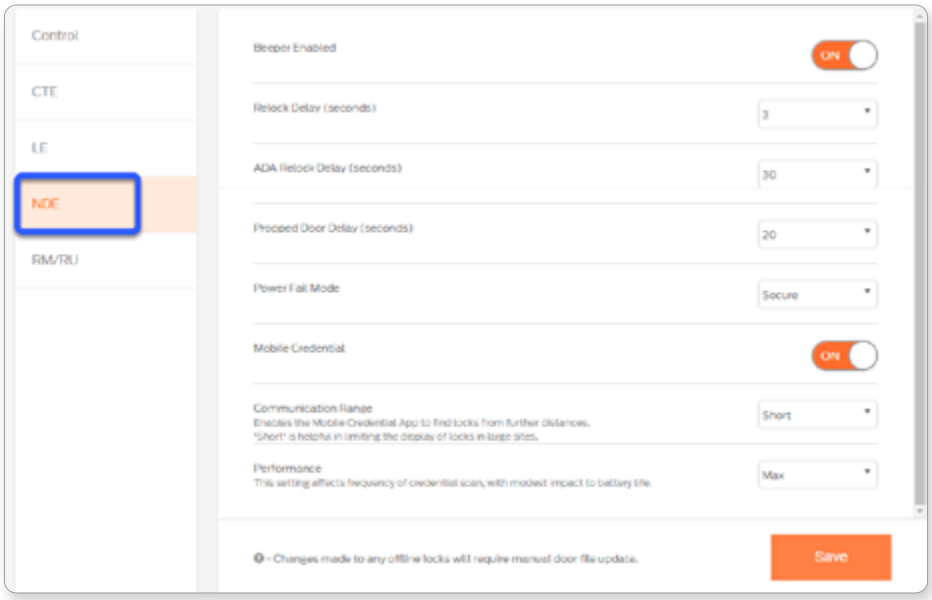


Fig. 9.122: NDE Default Settings

Table 9.14 NDE80 and NEDB Device Property Default Settings	
Setting	**Description**
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent.
Relock Delay (seconds)	When a valid credential is presented, the locking device unlocks and then relocks. Delayed relocks are from 1 – 30 seconds.
ADA Relock Delay (seconds)	Enables ADA operation to allow additional time to access doors. Delayed relocks are from 1 – 30 seconds.
Propped Door Delay (seconds)	Reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.
Power Fail Mode	Defines what the lock should do when entering Critical Battery Mode. • Secure : Locked • Passage: Unlocked • AS IS: no change
Mobile Credential	• OFF: Mobile Credential use is disabled. • ON: lock will accept Mobile Credential access and the following options are available.
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. ➔ **Note:** This is a PACS only feature. This setting has no effect on ENGAGE accounts.
Performance	Affects how often the device scans for a Mobile Credential. • Normal: Default • Max: Highly recommended for best user experience and quicker device unlocking when using Mobile Credentials. Reduces battery life by a few months as the device scans more frequently.

RU/RM

➔ **Note:** The Remote Monitor and Remote Undog (RU/RM) product is included here only to enable Allegion sales teams a means to demonstrate the RU/RM exit device product line to prospective PACS customers. Customers using our PACS providers for their property management will be able to manage RU/RM products, however the Allegion ENGAGE system does not support the RU/RM product

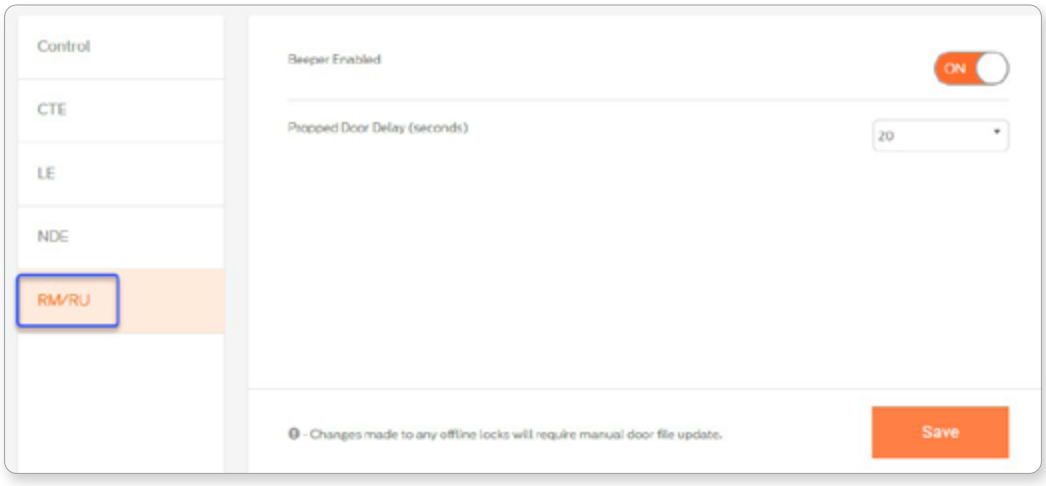


Fig. 9.123: RU/RM Default Settings

Table 9.15 RU/RM Device Property Default Settings	
Setting	**Description**
Beeper Enabled	• ON: the lock beeper will sound to provide device status. • OFF: the lock beeper will remain silent.
Propped Door Delay (seconds)	Reports and records a Propped Door Audit after a specified time. Delayed relocks are from 1 – 255 seconds.

Notice that as you enable certain settings, other settings are disabled. Some settings conflict and therefore cannot be enabled at the same time.

Reader Defaults

Reader Default settings allow for the most common credentials to be available when a device is new out of the box or recently had a factory default reset performed. It is most important for devices to be operational for the broadest Construction Mode credential acceptance ability before commissioning. Each commissioned device will be programmed with the defined reader default settings.

WARNING: Any setting changes or updates made to an installed and previously commissioned device will require Synchronization.

➔ **Note:** Reader Default settings apply to XE360, LE, LEB, NDE80, NDEB, and MTB Reader product families. The MT20 and MT20W credential enrollment readers will read any compatible credential and therefore, do not have Reader Default settings.

Reader Sensitivity is set to Normal by default and is recommended for most properties. Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.

For best reader response and improved battery life, disable any credential technology that is not needed.

1. **Log In.**
2. Select Advanced menu then Reader Defaults tab.
3. Adjust as needed and click Save.

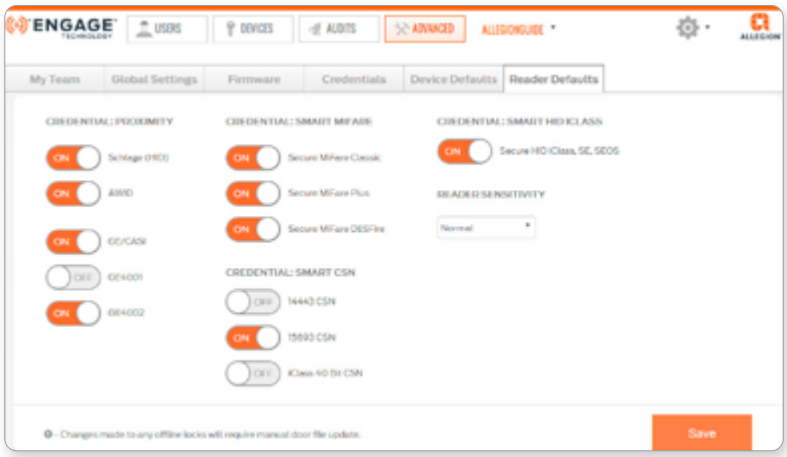


Fig. 9.124: Advanced > Reader Defaults

Mobile Application

Introduction

The ENGAGE Mobile Application is used to commission, program and update a property with ENGAGE enabled devices. Use the mobile application for property management data entry, commissioning devices, and general maintenance.

The ENGAGE Mobile application is used for operations to be accomplished while at the door, or nearby a device using Bluetooth (BLE) communication.

CAUTION: Mobile devices will need Wi-Fi, Bluetooth, and or Cell data for full compatibility. Bluetooth communication is limited in range and the user should be as close as possible to the device for robust Bluetooth communications. (< 10 ft)

Operations normally performed nearby a door include device commissioning, device setup and Sync (door file updates/audit history), performing diagnostics, and may also include firmware updates.

Table 10.1 describes how the functions within the ENGAGE web and ENGAGE Mobile applications can be shared.

Table 10.1 Web and Mobile Application Functions

Function	ENGAGE Web	ENGAGE Mobile
Add/Delete Users	Yes	Yes, easier with Web
Assign Credentials	Yes	Possible, at door enrollments - not recommended
Audits	View Only	Retrieve and View
Commission Locks & Devices	No	Yes
Global Settings	Set and Edit	Not available
Grant User Access	Yes	Yes
Invite Team Members to Manage Property	Yes	Yes
Schedules	Create, Edit, and Assign Schedules	Assign Schedules

CAUTION: Screen shots in this section may vary by device.

For the latest information, go to https://us.allegion.com/en/home/products/categories/software/ENGAGE-web-mobile-apps.html and click on Mobile & Web Requirements.

Supported Devices and Requirements

Mobile Application Phone Support

We support and test the flagship phone models from Apple, Samsung, LG, Motorola, and Google for the last two years, such as:

- iPhone 11 Pro or newer
- Samsung S20 or newer

Mobile Application Operating System Support

We support and test major revisions for Android and iOS for the last two years such as:

- iOS 14 or newer
- Android 10.0 (API 29) or newer

Mobile Application Downloads

- iOS devices: ENGAGE Mobile app - iTunes App Store
- Android devices: ENGAGE Mobile app - Google Play Store

Log In

When the ENGAGE application is first opened on your mobile device, the Log In screen will be displayed. Enter the email address and password that is associated with your account, then tap the Log In button.

If you cannot remember your password, tap Forgot Password? and follow the on-screen instructions.

Main Menu

iOS devices will display a menu along the bottom of the screen. Tap any icon to display that screen.

Android devices have a menu icon in the top left corner.

- **Users**
- **My Team**
- **Sites**
- **Account**
- **Help**

Devices

Table 10.2 Devices Screen

Option	Description
All Devices	All devices in the site are listed.
In Range	Only devices that are within range are listed.
Updates	Only devices that need to be updated are listed.

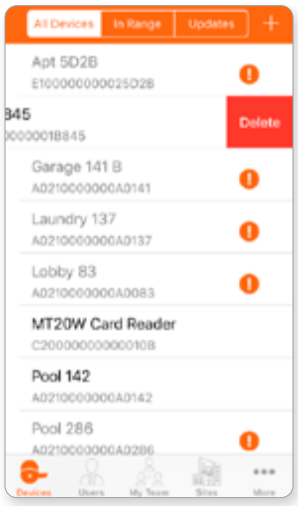
Add Device

1. While near the device you want to add, open the Devices screen.
2. Tap the plus button.
3. Choose the type of device you want to add, and follow the on-screen instructions.

Delete Device

1. Open the Devices screen.
2. Find the device you want to delete in the list.
3. **iOS:** Swipe left on the device name to show the Delete button. Then tap the Delete button.

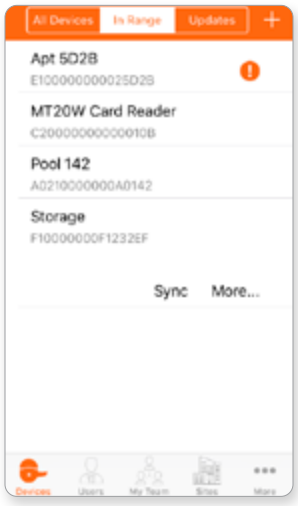
   Android: tap and hold on the name of the device you want to delete. Then tap the trash icon in the upper right corner.
4. The device will no longer be listed in the Devices screen.



Retrieve Audits

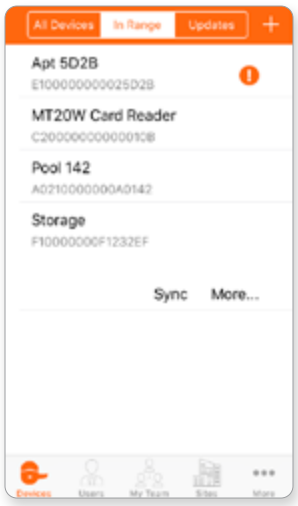
1. While near the device you want to update, open the Devices screen. Then select the IN RANGE tab.
2. Select the device from which you want to gather audits, and then click More.
3. Click the Audits button, and follow the on-screen instructions.

➔ **Note:** Device **Activity** is the default Audit Screen. Select the **Diagnostics** tab for System Audits. Retrieved Audits are always available via the ENGAGE Web Application.



Manually Sync Device

1. While near the device you want to sync, open the Devices screen. Then select the IN RANGE tab.
2. Select the device you want to sync.
3. Click Sync.



Wi-fi Settings

Enable Wi-fi

The ALL DEVICES tab shows all devices commissioned in ENGAGE. Devices in bold are in Bluetooth communication range. The IN RANGE tab shows only those devices that are in Bluetooth communication range.

1. **Log In** to the mobile application.
2. From the Device menu, Select a nearby device.
3. Select More to connect with the device.

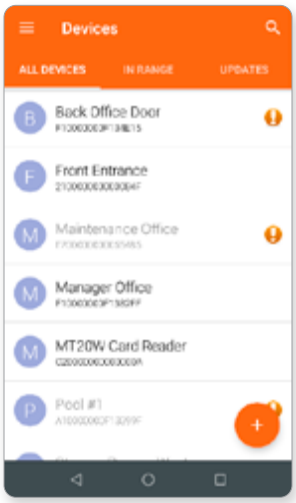


Fig. 10.1: Device

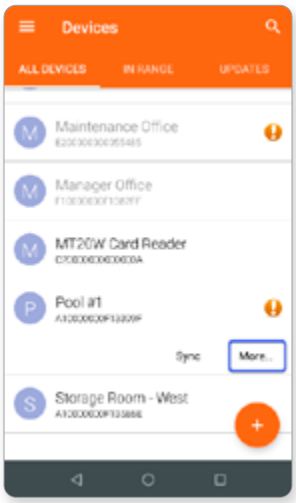


Fig. 10.2: More

4. Once connected, scroll down and select Settings.

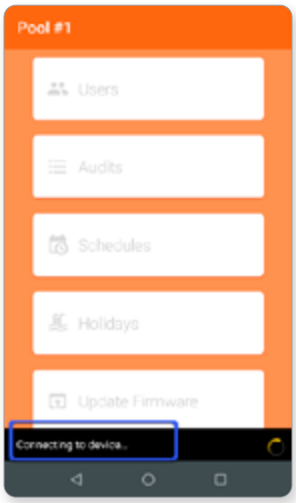


Fig. 10.3: Connecting

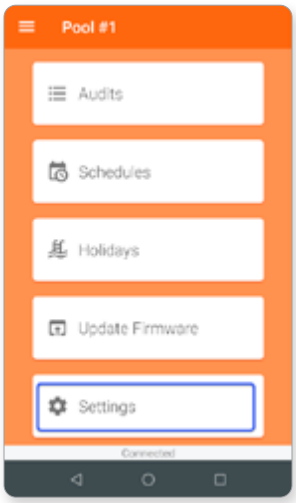
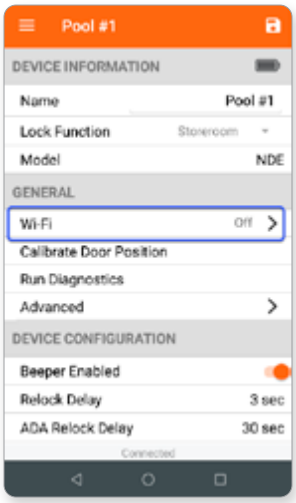


Fig. 10.4: Connected

5. Select Wi-Fi menu under GENERAL.



When enabled, the Wi-Fi network details you save will be automatically stored by the mobile device and displayed in the list. Using saved networks makes it easier to accurately enter Wi-Fi network details when setting up new Wi-Fi enabled devices

6. Move the Wi-Fi slider to the right to enable Wi-Fi connectivity
7. View the full Wi-Fi Configuration menu. By default, the Display/Save Network List is enabled.
8. Select Add Network.

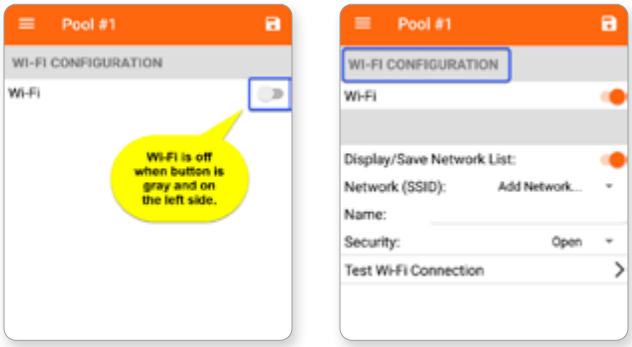


Fig. 10.5: Wi-Fi

9. Enter the Wi-Fi network details:
10. Select Save, or the disc icon.
11. **Test Wi-Fi Connection**.

Fig. 10.6: Wi-Fi

Select a Previously Saved Network

Each time a unique Wi-Fi network is entered and saved, the network details are automatically saved by the mobile device.

CAUTION: A saved network may not be locally available at the physical location of your installed device. When using a saved network, ensure you select the Wi-Fi network that is local to the device being set up and in Wi-Fi range for good communication. If you are unsure, use the "Test Wi-Fi Connection" menu or consult your local IT Administrator. Network settings can be saved from different Wi-Fi access point locations across your property. Network names (SSID) may vary within the same building. Choose the saved network for the device being set up. Remember select the saved network that is local and available at the device being set up.

1. Ensure you have already performed **Enable Wi-fi**.
2. Select the desired device and from the Wi-Fi Configuration screen,
   a. iOS: select Show Saved Network.
   b. Android: select Add Network.

Fig. 10.7: iOS

Fig. 10.8: Android

3. After selecting the network, Select Save
   - The network is selected, the Wi-Fi SSID is displayed on the devices' Wi-Fi configuration screen.
4. Select **Test Wi-Fi Connection**

Fig. 10.9: iOS Saved

Fig. 10.10: Android Saved

Save an Available Network

Saving an available network for a device allows for easier setup when enabling nightly Wi-Fi and firmware updates on other Wi-Fi enabled devices.

1. **Log In** to the mobile application.
2. From the Device menu, Select a nearby device.
3. Select More to connect with the device.

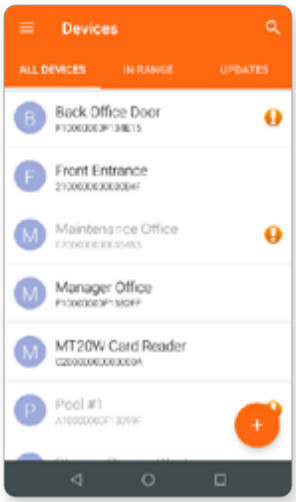


Fig. 10.11: Device

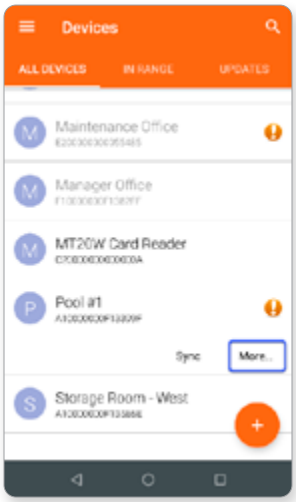


Fig. 10.12: More

4. Once connected, scroll down and select Settings.
5. Select Wi-Fi option.

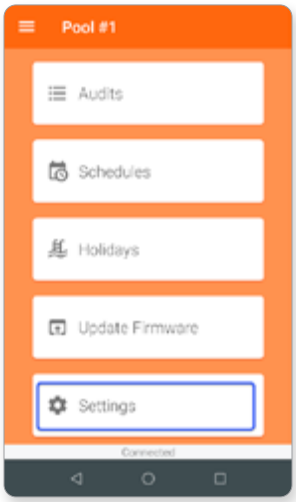


Fig. 10.13: Settings

Fig. 10.14: Wi-Fi Option

WARNING:
Wi-Fi networks that appear in the available network list may not be accessible at your current location.

6. Slide on Wi-Fi to display the Wi-Fi Configuration.

Fig. 10.15: Wi-Fi

Fig. 10.16: Wi-Fi Configuration

Test Wi-Fi Connection

1. While near the device you want to test, open the Devices screen.
2. Tap the device you want to test.
3. Tap Test Wi-Fi Connection.

➔ **Note:** The device LED flashes **AMBER** while Wi-Fi Connection testing is in process. This Wi-Fi Connection test will take a several minutes.

Fig. 10.17: Test Wi-Fi Connection

4. View the device has successfully connected to the host.

➔ **Note:** If the Wi-Fi test fails to connect successfully:

- Ensure your Wi-Fi network **SSID** and **Security** settings are entered correct and try again
- Confirm the local Wi-Fi network settings and that the network is currently available (now) by using your Mobile device to enter the same network settings, connect, and verify the local Wi-Fi network is working
- Note the error message and contact **Customer Support**.

Fig. 10.18: Wi-Fi Test Success

Users

Add User

1. Open the Users tab.
2. Tap the plus button.
3. Fill in the First Name and the Last Name.
4. Click the save button (iOS) or icon (Android).
5. You can now add **Credentials** and **Assign Access** for the new user.

Delete User

1. Open the Users tab.
2. Find the User you want to delete.
3. **iOS:** Swipe left on the user name to show the Delete button. Then tap the Delete button.

   Android: Tap and hold on the name of the user you want to delete. Then tap the trash icon in the upper right corner.
4. The user will no longer be listed in the Users screen.

Edit User

1. Open the Users tab.
2. Tap the User you want to edit.
3. Make the necessary edits.
4. Click the save button (iOS) or icon (Android).

My Team

The My Team tab shows site administrators. See **Team member roles** for more information.

Add Team Member

1. Open the My Team tab.
2. Tap the plus button.
3. Fill in the First Name, Last Name and the Email Address.
4. Choose the Site.
5. Choose from the **Team member roles**.
6. Click the save button (iOS) or icon (Android).

Edit Team Member

1. Open the My Team tab.
2. Click the name of the team member you want to edit.
3. Choose from the **Team member roles** for the team member.

   ➔ **Note:** You can only edit the role in the mobile app. For other edits, see **My Team**.
4. Click the save button (iOS) or icon (Android).

Delete Team Member

1. Open the My Team tab.
2. Find the team member you want to delete.
3. **iOS:** Swipe left on the user name to show the Delete button. Then tap the Delete button.

   Android: Tap and hold on the name of the user you want to delete. Then tap the trash icon in the upper right corner.
4. The team member will no longer be listed.

Sites

All sites are displayed.

Tap Select to see all the devices in the site.

Tap More to see the Site Settings.

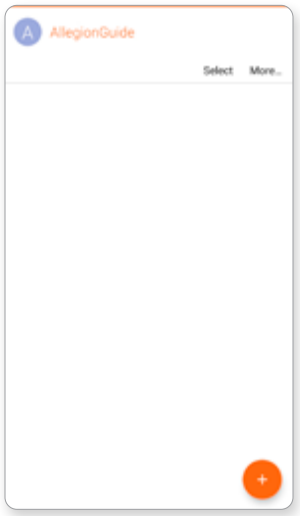
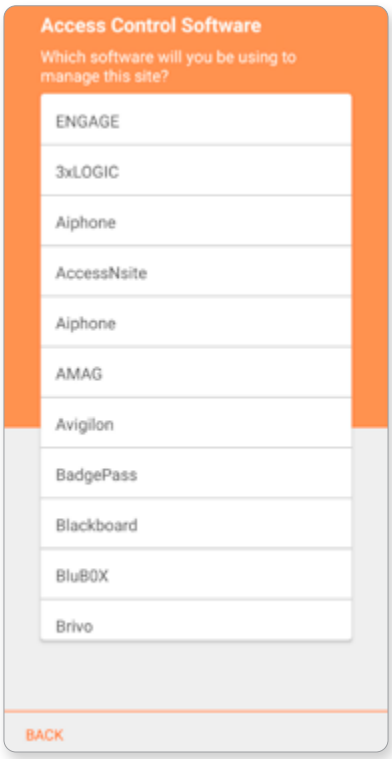


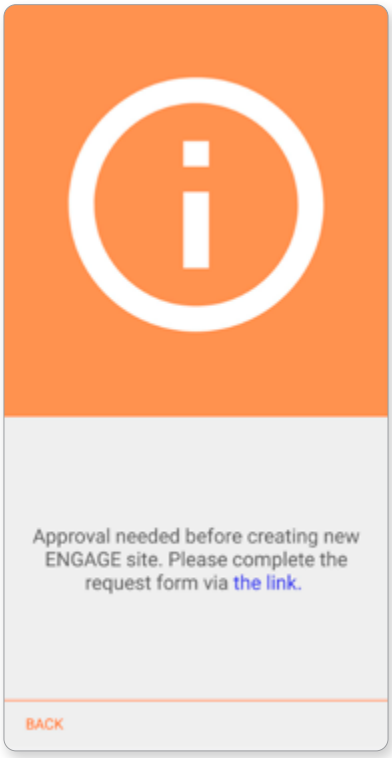
Fig. 10.19: Sites

Add a Site

1. Click the + icon.
2. In the Access Control Software screen, select ENGAGE.



3. Approval is required to create a new ENGAGE site. Click the link.



4. Fill in the request form and then click the Submit request button.
5. The Site request will be submitted to the local sales office for approval. Please allows one (1) business day for a response. Watch for an email with further instructions.

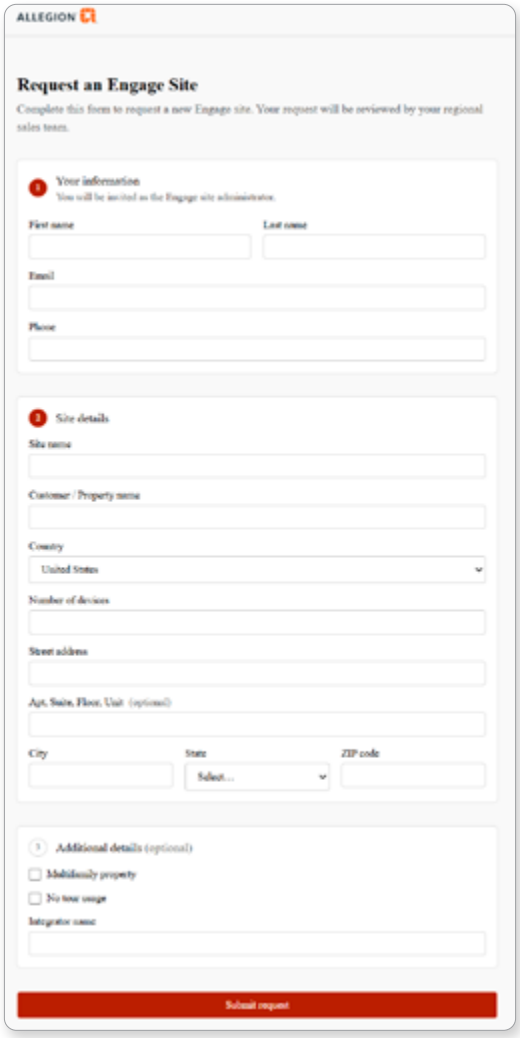


Fig. 10.20: Request an ENGAGE Site

Site Settings

Table 10.3 Site Settings

Name	Options	Description	Edit in Mobile?
Role	Manager, Operator, Administrator	Role of the Team Member who is currently logged in.	No
Site Name		Name of the site	Yes
Site Type		Market segment of the site	Yes
Timezone	All timezones	Timezone of the site	Yes
Daylight Saving Time	on, off	Turn Daylight Saving Time on or off	Yes

Updating Device Firmware

Device firmware should be kept up to date to ensure property-wide device compatibility and operations, and to ensure the latest features and security updates are provided at the door.

All Schlage ENGAGE enabled products will occasionally have firmware updates for new features and continued robust performance.

Firmware updating can be accomplished at the door using the ENGAGE Mobile Application or by scheduling "Overnight" Wi-Fi updates for Wi-Fi compatible and enabled devices using the ENGAGE Web Application.

WARNING: If you are using a Physical Access Control Software (PACS) account, be sure to consult your SAM before updating firmware on any of your devices. Ensure your SAM software version is compatible with the latest ENGAGE device firmware.

IMPORTANT NOTES:

1. Schlage Control Mobile Enabled Smart Lock and standalone MTB Mobile Enabled Reader firmware must always be updated at the door using the ENGAGE Mobile Application.
   - Schlage Control and standalone MTB does not support Wi-Fi connectivity.
2. For Schlage XE360, NDE80, NDEB, LE, LEB and CTE devices, overnight Wi-Fi network firmware updates can be scheduled by the ENGAGE Web Application when a Wi-Fi network connection is available and properly enabled at the door.
   - Nightly Wi-Fi updates require local Wi-Fi network availability overnight for the scheduled firmware updates to be successful.
3. Nightly Wi-Fi updates are scheduled by ENGAGE at random times in the early morning hours.
   - Early morning hours are used to reduce user issue opportunities while the device is inoperative for the few minutes it takes to be updated.
4. Firmware updates take some time to complete.
   - The devices flash the "Amber" LED while the firmware file is being sent to the device.
   - The device parses the file into its memory while flashing the LED RED and GREEN.
   - This process will take several minutes to complete – be patient.

Via BLE

Firmware updates are available for all devices using the ENGAGE Mobile Application. Schlage Control Mobile Enabled Smart Locks and standalone MTB Mobile Enabled Readers require nearby Bluetooth (BLE) communication with the Mobile device for firmware updates, while all other ENGAGE devices may use a local Wi-Fi network connection for faster firmware updates and scheduled overnight firmware updates.

If the device you need is not presented, ensure the device is already commissioned and that you are within Bluetooth (BLE) range.

1. **Log In** the mobile application
2. View the devices In Range.
3. Select the local device to be updated with the latest firmware.
4. Select More.

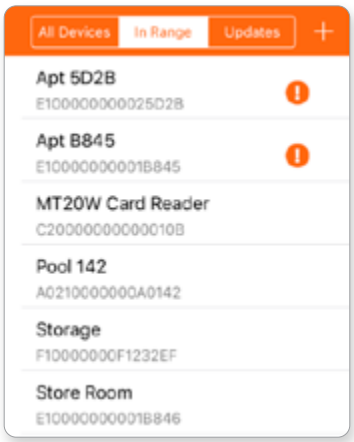


Fig. 10.21: Devices in range

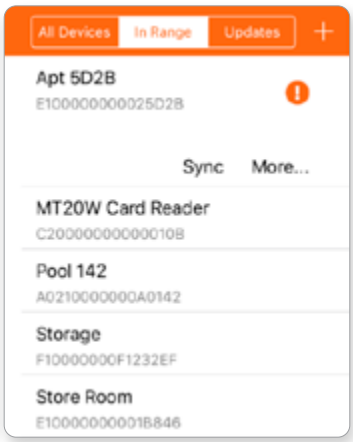


Fig. 10.22: Select More

The device starts flashing the RED LED when connected and communicating.

5. Wait for the device to connect.
6. Select Update Firmware.

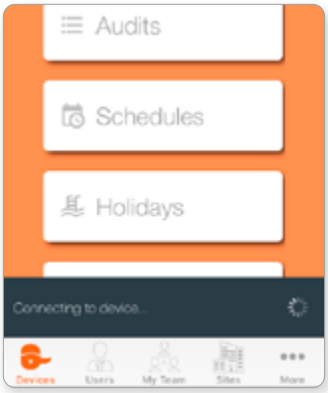


Fig. 10.23: Connecting to device

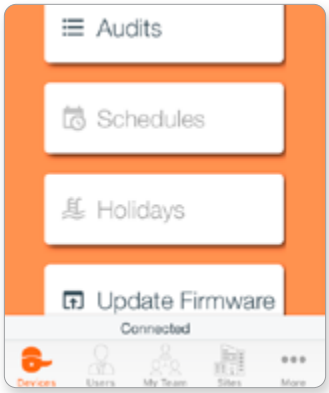


Fig. 10.24: Connected to device

WARNING:
The mobile device MUST stay within BLE communication range while downloading firmware.

7. Select Update.
8. Wait for the update to complete.

Fig. 10.25: Select Update

Fig. 10.26: Wait for the update to complete

9. The following screen displays when the firmware update is successful. Select Finish.
10. The recently updated device loads the new firmware into its memory and REBOOTS itself. The firmware update and reboot process will take a few minutes – be patient.

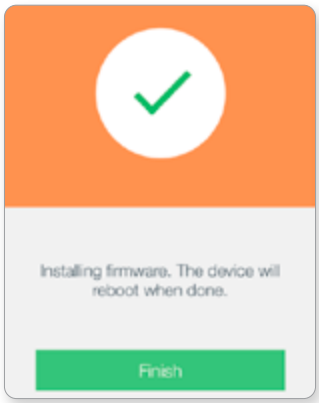


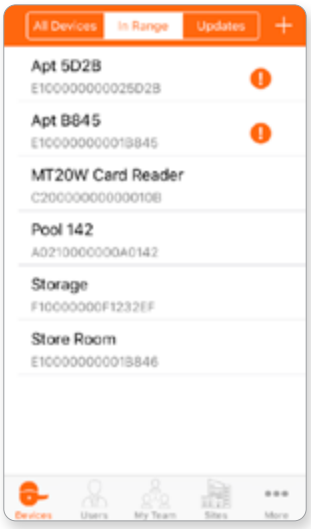
Fig. 10.27: Select finish

Via Wi-Fi

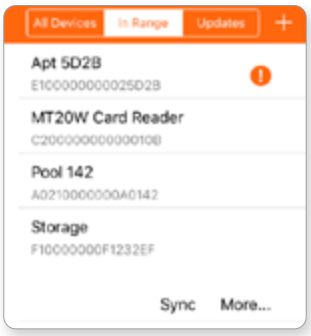
ENGAGE devices with local Wi-Fi connectivity may have firmware updates performed at the door. This method is preferred over the previously described Bluetooth (BLE) method because it uses the local Wi-Fi network for much faster communication and does not require the Administrator and the Mobile device to remain near the door during the firmware update process.

For this example, to update a Schlage LE device using a local Wi-Fi network connection follow these steps.

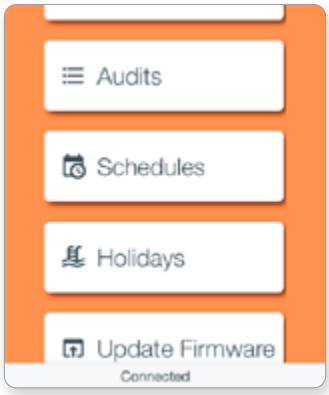
1. **Log In** to the mobile application.
2. View the devices In Range screen.
3. Select the local device to be updated with the latest firmware.



4. Select More.

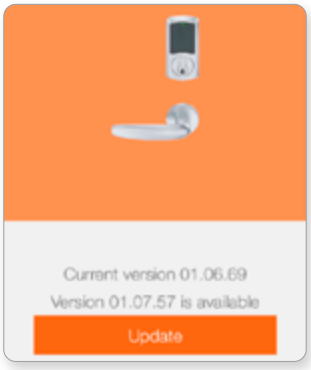


5. Once the device is connected, select Update Firmware in the connected device menu.



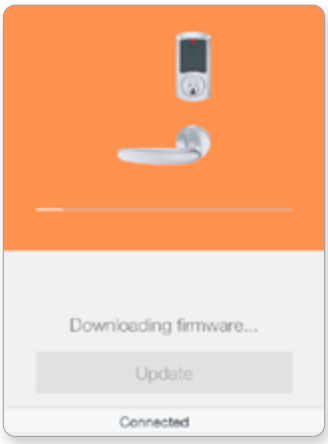
When the firmware version on the device is current a “Firmware is up to date” message is provided. Installing the firmware will take a few minutes, be patient

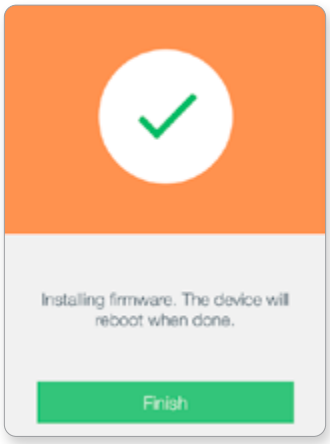
6. Confirm the requested firmware update.
7. Select Update.



WARNING:
During the firmware update and while the LED are blinking, the device will be off-line and will not provide access.

8. Select Finish. After the firmware is downloaded, it will be installed into the device automatically. The device will blink the LED RED and GREEN while installing the new firmware update. This process will take a few minutes, be patient. Once the firmware installation is completed, the device reboots and begins normal operation.

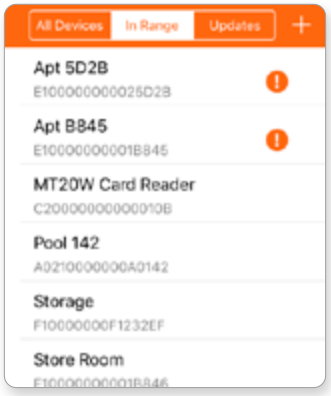




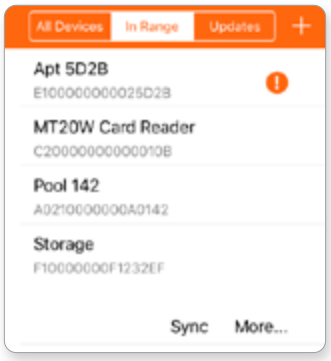
Via Mobile Wi-Fi

When the device does not have a Wi-Fi network connection available or the local Wi-Fi network is not enabled, the firmware download can be performed by temporarily enabling a Wi-Fi connection through the Administrator's Mobile device.

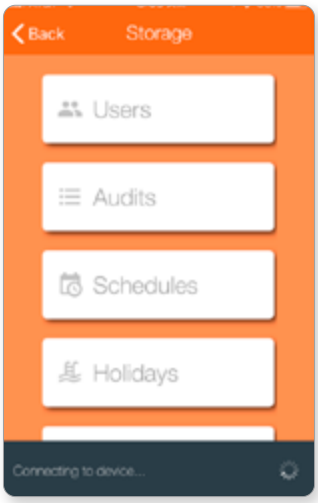
1. **Log In** to the mobile application.
2. View the In Range screen.
3. Select the local device to be updated.

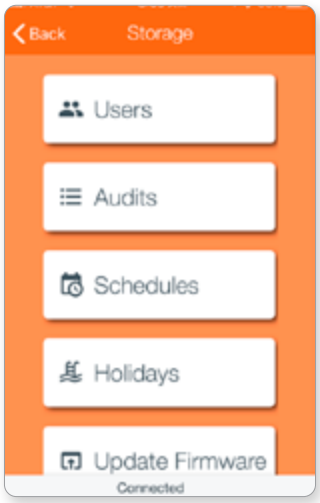


4. Select the device to be updated.
5. Select More ....

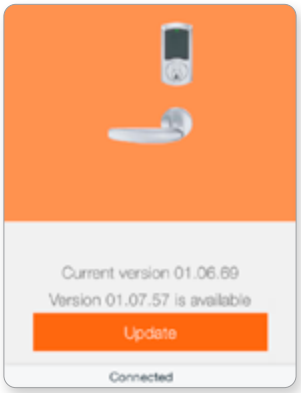


6. Select Update Firmware.

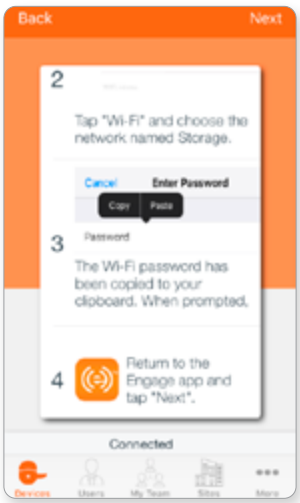




7. Select Update.

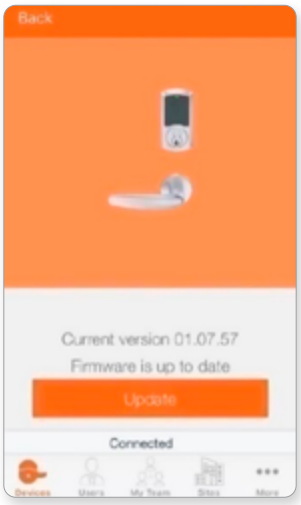


8. The Wi-Fi PASSWORD will be copied into the mobile device's clipboard.
9. Open the Settings menu on your mobile device.
10. Select the Wi-Fi network settings menu.
11. Connect to the Wi-Fi network with the same name as the device you are connected to.
12. Paste the saved password into the Wi-Fi settings field.
13. Join the network.
14. Verify the mobile device connects with the selected device by viewing its Wi-Fi connection information.
15. Return to the previous ENGAGE mobile application screen.
16. Select Next.



ENGAGE will use the selected device to create a local Wi-Fi network between the Mobile device and the lock. The local Wi-Fi network name will be the selected device name. ENGAGE will save the Wi-Fi PASSWORD into the Mobile devices' "Clipboard". Using the Mobile device "Cut and Paste" feature, the Wi-Fi password is then pasted into the Wi-Fi settings password field.

17. The device will blink the LED RED and GREEN for a few minutes. After the RED and GREEN flashing stops, the firmware update is complete. The device will automatically reset and will begin normal operation using the new firmware.
18. To confirm the firmware update:
    a. Connect to the device that was updated.
    b. Select the device, then More …
    c. Select the Update Firmware menu.
    d. View the Firmware is up to date message.



WARNING: ENGAGE will not know that the firmware update process has been accomplished until the next Sync reports the new firmware update.

No-Tour Feature

Overview

The No-Tour feature allows Administrators to assign and change access rights without having to physically visit the lock to make access programming updates.

➔ **Note:** When No-Tour is enabled, access right updates can still always be accomplished through the normal Sync process or when device configuration is also being adjusted.

BEST PRACTICE:
Administrators should Sync all devices when removing or deleting user access to ensure all doors the user had access to are updated.
It is not recommended for a site to be converted from tour to no-tour once credentials have already been added, or to use both tour and no-tour credentials in the same site. See **See Credential Reader Connection to CTE on page for more information.** on page 198 for more information.

Requirements

- A commissioned MT20W Reader or Control Mobile Enabled Smart Lock must be included in the site.
- Physical Smart Credentials or Mobile Credentials
- Once a No-Tour credential is programmed, the User MUST visit the door and present the credential before the access rights will be updated.

CAUTION:
ANY change made to a user schedule for sites using No Tour Device Groups will require ALL credentials to be collected and placed on the MT20W for programming.

Limitations

- The No-Tour feature cannot be used to update device settings.
- Prox Credentials may not be used as No-Tour Credentials

Table 11.1 No-Tour Feature Capabilities and Limitations

Credential Type	Max Doors or Door Groups	Updates to Access Rights	Updates to Device Settings
Physical	11	Yes	No
Mobile	Unlimited	Yes	No
Prox	n/a	n/a	n/a

WARNING: A No-Tour Credential MUST be presented to each updated No-Tour door for access rights to be updated. If a User fails to visit each door using No-Tour programming after a credential replacement or an access deletion, the old or lost credential access will still be enabled because the new lock access programming has not yet been performed. Administrators should Sync all devices when removing or deleting user access, to ensure all doors the user had access to are updated.

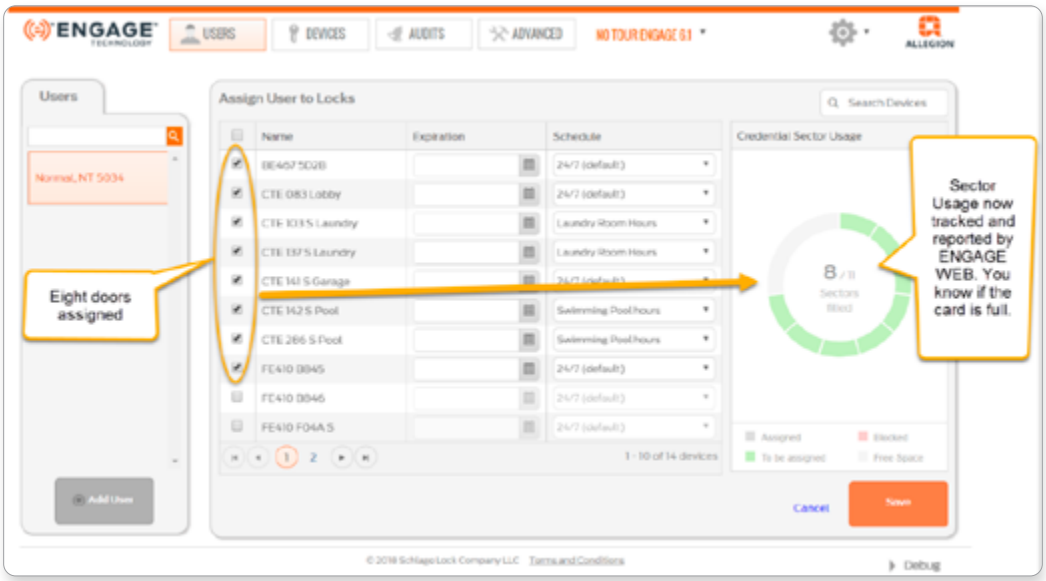
No-Tour Physical Credentials

➔ **Note:** These limitations do not apply to No-Tour Mobile Credentials.

A door assignment counter is displayed when assigning access using a physical credential. There are eleven (11) total available sectors. Each Door or Door Group takes up one sector.

While programming access, the status of each credential sector is displayed as:

- **Assigned** - Used, already assigned and the credential has been programmed
- **Blocked** - Used, already assigned however access to this door is "DELETED"
- **To be assigned** - Planned access assigned, however the credential is not yet programmed
- **Free Space** - Unused, available for new access assignment



➔ **Note:** Physical Credentials that have assigned door access deleted, remain as "Blocked" assignments in the credential sector and will consume one (1) sector or folder in the credential memory.

➔ **Note:** A blocked door is counted in the maximum door programming limit of 11 doors per credential. When the User credential access expires per a defined User Expiration date, the 11 credential sectors are freed-up and new access assignments can be programmed with a new expiration date.

Enable No-Tour Feature

The No-Tour feature is automatically enabled when a Schlage MT20W Credential Enrollment reader or Schlage Control Mobile Enabled Smart Lock is commissioned into the site.

➔ **Note:** When using Mobile Credentials for No-Tour, it may be necessary to enable the No-Tour feature under the **Global Settings** tab.

Update Credential for No-Tour Programming

Physical Credentials

1. Update the user's access rights. See **Assign Access** and **Remove Access**.
2. Obtain the user's No-Tour credential to be programmed with changes.
3. Ensure the MT20W credential reader is powered up ready for use with the "Blue" LED illuminated on solid.
4. From the appropriate user's account, click the Update button.

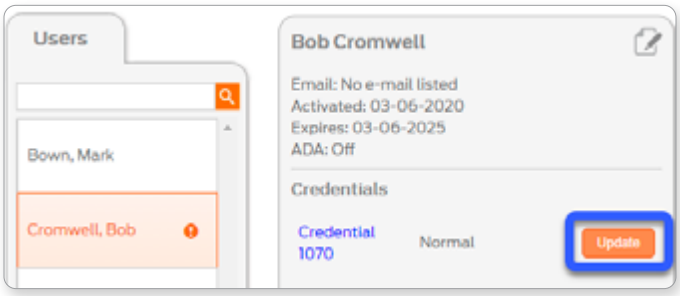


Fig. 11.1: Update Button

5. Place the user's credential on the reader.
6. Wait until the MT20W beeps and blinks **GREEN** 3 times. Then click Next.

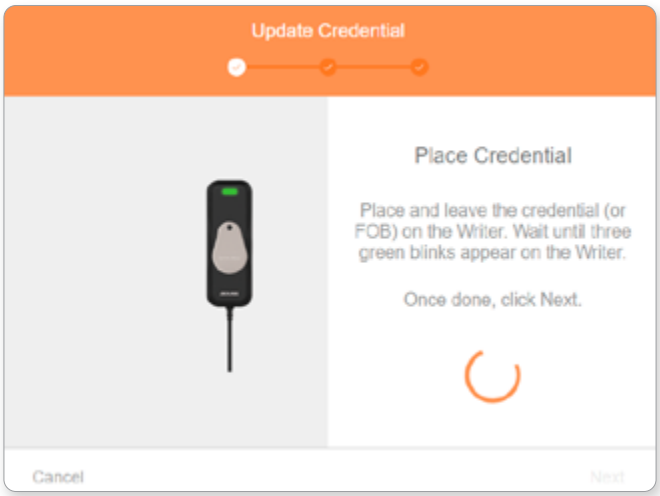


Fig. 11.2: Update Credential

7. The new credential information will be retrieved and when complete, the credential will be updated successfully.

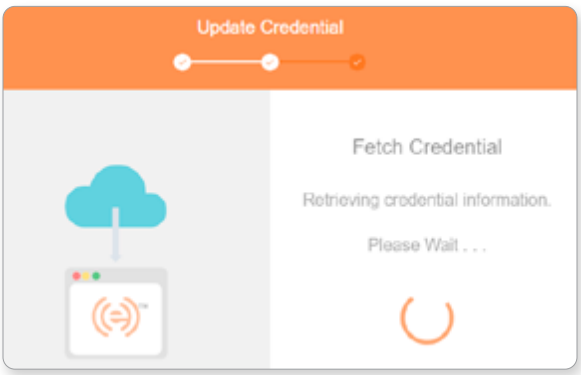


Fig. 11.3: Retrieving Information

8. Click Finish and remove the credential from the reader. The user's credential and User account have now been updated.

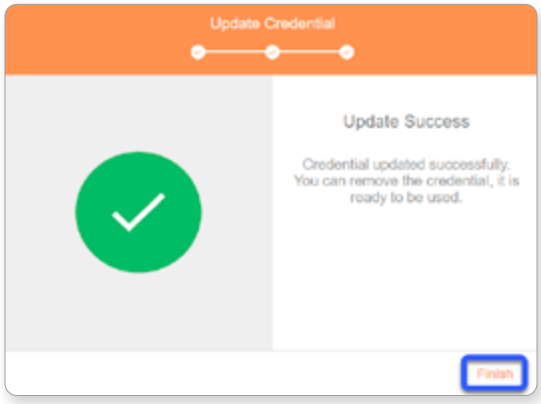


Fig. 11.4: Update Success

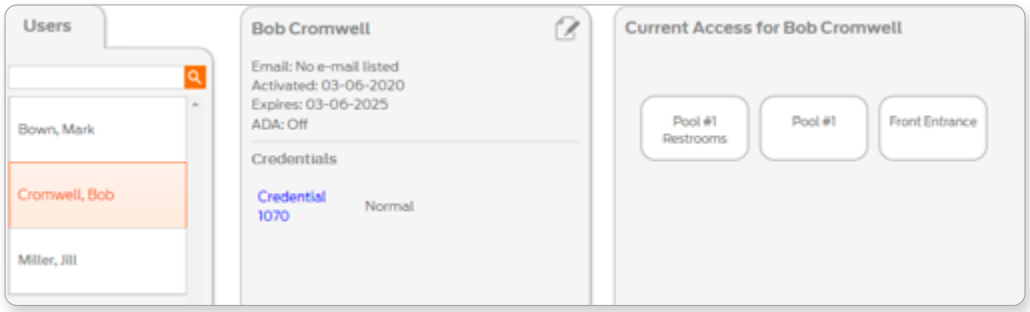


Fig. 11.5: Updated User Account

WARNING: The No-Tour feature will make the access changes at the door when the credential is presented by the user. No special action is needed by the user other than just present the credential to gain normal access. When the User credential is not available, the Administrator can always use the Schlage Mobile Application to Sync and make changes without using No-Tour.

Mobile Credentials

➔ **Note:** Use of Mobile Credentials requires the latest versions of Schlage Mobile Access application and the latest lock firmware. Schlage Mobile Access application may not automatically update.

1. Update the user's access rights. See **Assign Access** and **Remove Access**.
2. Updating a Mobile Credential only requires the mobile application to be closed and reopened to receive any new access programming.

   ➔ **Note:** Mobile Wi-Fi or data connection is required for cloud access.

No-Tour Temporary Maintenance Access

When Temporary or Maintenance Access is needed, it is recommended for the No-Tour Administrator to manipulate User Activation or Expiration settings, along with a limited User (Maintenance) Schedule.

This allows the Administrator to use a User Activation / Expiration setting to specify the day (or days) maintenance access is needed, and then use a pre-defined maintenance User Schedule to specify the specific "Time-Of-Day" access is to be allowed.

NOTES:

- User Schedules MUST first be saved in ENGAGE and then each device must Sync before the new schedule is available at the door.
- User Activation / Expiration settings are programmed on the credential and are immediately available when presented at the door.

Here is one example of a Temporary Maintenance Access setup:

1. Define a USER "Maintenance Shift" schedule in the ENGAGE Web Application that limits a sub-contractor to first shift hours for access.
   - In the example below, we chose Weekdays from 8:30AM to 4:00PM as our Maintenance Daily Schedule.
2. Tour the property, perform nightly Wi-Fi updates, or commission new devices to save the new "Maintenance Shift" schedule into each device.
   - A new or updated User Schedule requires Sync before the newly defined Maintenance Shift is honored at the door.

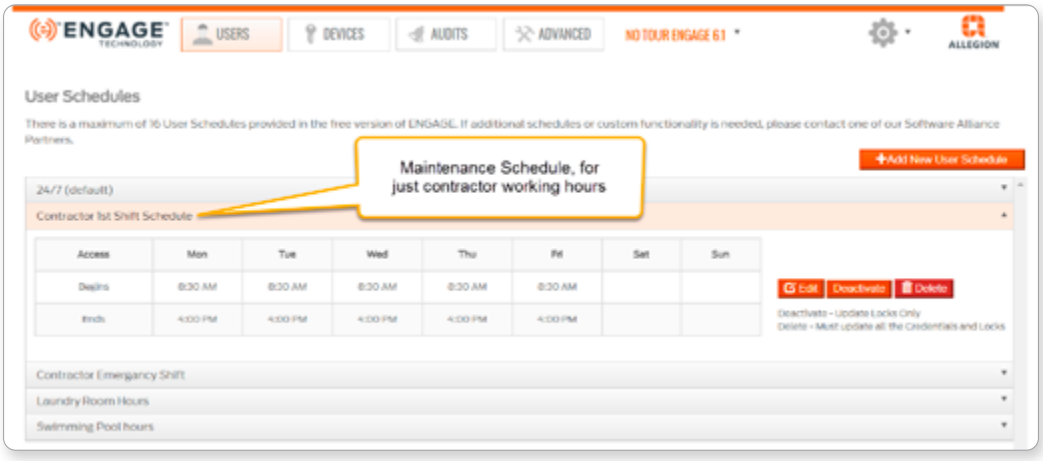


Fig. 11.6: Maintenance Shift Schedule

3. When the sub-contractor needs maintenance access, the Administrator can now follow these steps:
   - Program a credential with the contractor's name.
   - Set the Expiration for one (or more) days of access (as needed).
   - Select the scheduled "Maintenance Shift" to limit the daily hours of access to be provided for only those doors assigned.

   ➔ **Note:** A maximum of 11 doors or combination of individual doors and Door Groups can be assigned at one time to a physical No-Tour credential. Mobile credentials do not have this limitation.

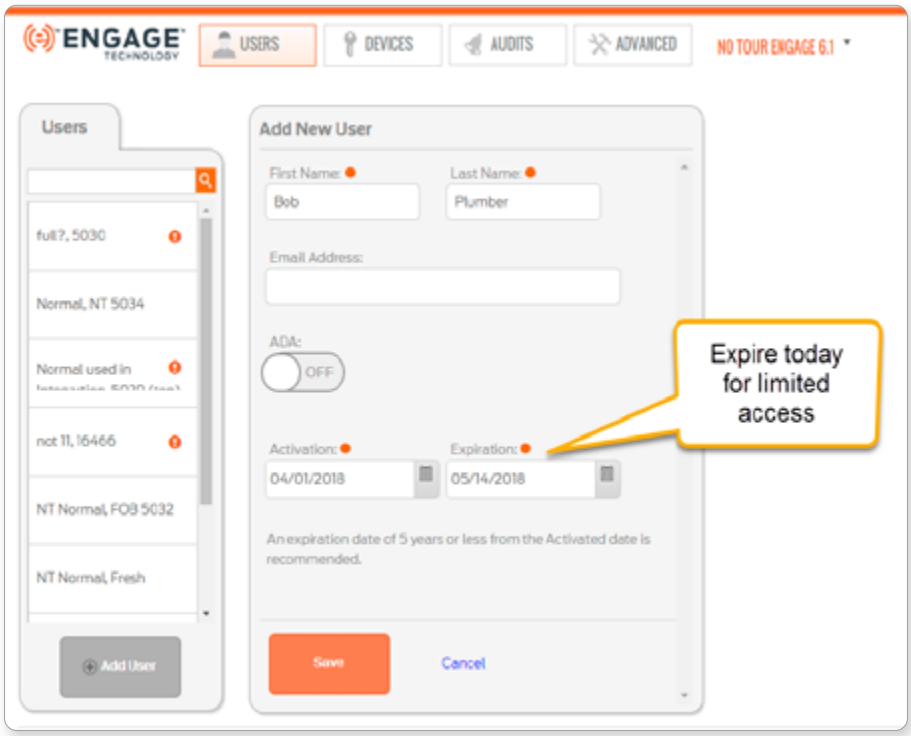


Fig. 11.7: Set Expiration for Today to Limit Access

4. When a Maintenance Contractor access expires per its Expiration setting
   - The credential can be reused as if new again.
   - Reprogram expired credentials
     i. new set of doors and/or Door Groups,
     ii. new expiration date,
     iii. different Username

PACS Managed Properties

Introduction

Our Physical Access Control Software (PACS) partners integrate and support our portfolio of electronic hardware to provide solutions that securely and efficiently control access for openings throughout a facility.

Using a PACS software system provides a broader set of features and capabilities to meet the most demanding security needs.

- The network system is managed by PACS software and a service provider
- A self-management system is operated by the property owner
- Real-time device and system updates (where applicable)
- Expanded capacities for credential management and door openings
- Additional features such as video capabilities and enhanced security

PACS managed properties have limited functionality within ENGAGE. The differences are outlined in this section.

Users

Users are people who need to gain access to an opening in your site. They must also be assigned a Credential before access can be granted.

Fig. 12.1: Users Tab

Table 12.1 Users Properties

Property	Description	Required	Default
First Name	enter the first name of the user	yes	none
Last Name	enter the last name of the user	yes	none
Email	enter user email address	no	none

Table 12.1 Users Properties			
Property	**Description**	**Required**	**Default**
Notes	can be used to capture additional information about the user (e.g. resident ID, employee ID, memo)	no	none

Add User

1. **Log In** and open the **Users Tab**.
2. Select Add User.

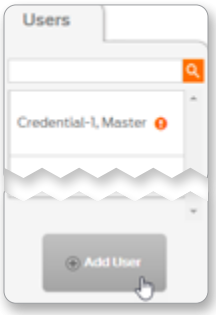


Fig. 12.2: Add User Button

3. From the Add New User screen, complete the fields:

   ➔ **Note:** See **Table 12.1 Users Properties** for details.

4. Select Save.

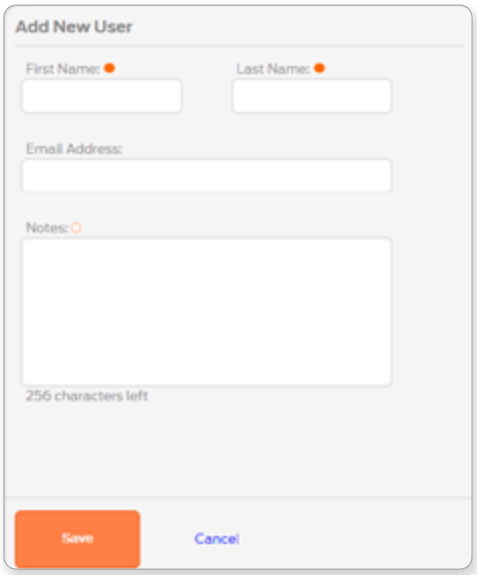


Fig. 12.3: Add New User

5. The User added banner is displayed and the user information screen displays.

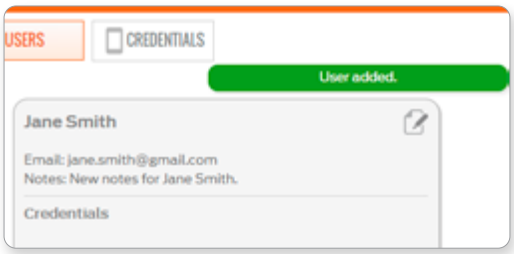


Fig. 12.4: New User Added

Edit User

1. **Log In** and open the **Users Tab**.
2. Select a current user.

Fig. 12.5: Select a User

3. Select the edit user button.

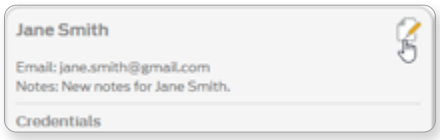


Fig. 12.6: Edit User Button

4. From the Edit User screen, make changes to the fields:

   ➔ **Note:** See **Table 12.1 Users Properties** for details.

5. Select Save.

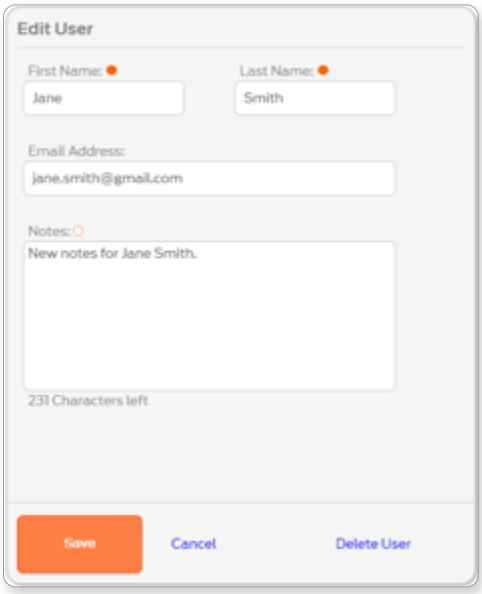


Fig. 12.7: Edit User

6. The User info updated banner is displayed and the user information screen displays.

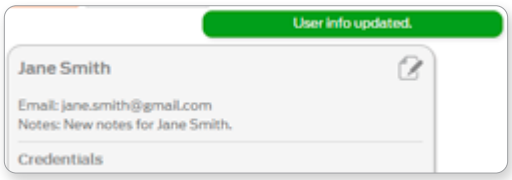


Fig. 12.8: User Info Updated

Delete User

1. **Log In** and open the **Users Tab**.
2. Select a current user.

Fig. 12.9: Select a User

3. Select the edit user button.

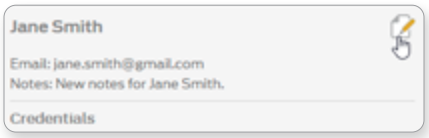


Fig. 12.10: Edit User Button

4. Select Delete User.

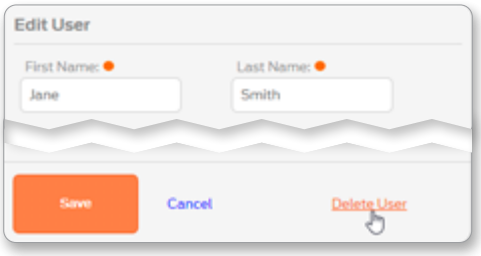


Fig. 12.11: Delete User Button

5. Type DELETE into the Confirm: box. Then select the Delete button.

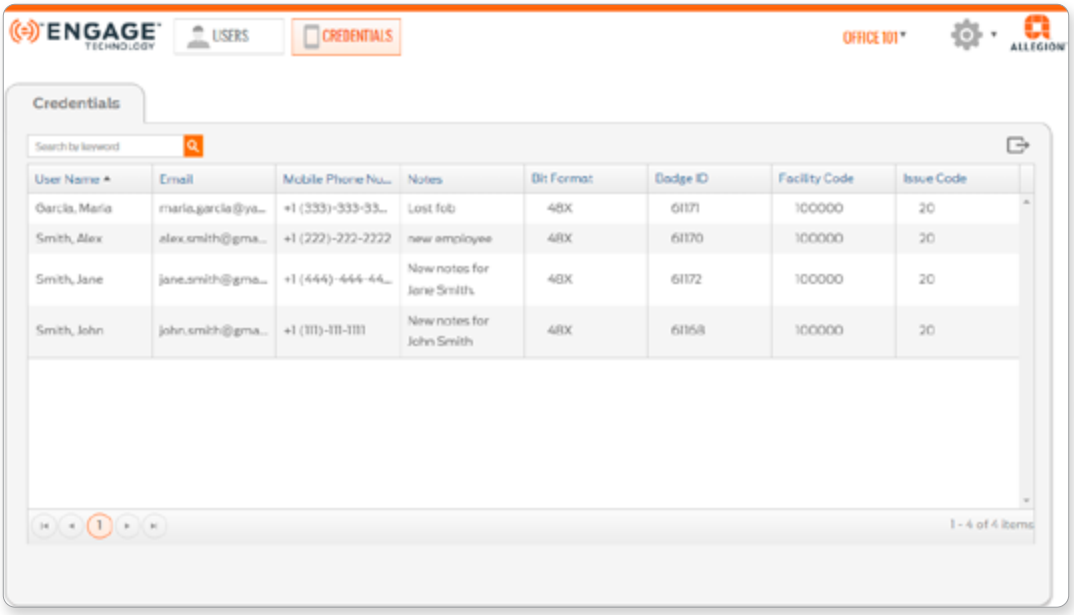
Fig. 12.12: Confirm User Deletion

6. The User deleted banner is displayed.

Fig. 12.13: User deleted

Credentials

The CREDENTIALS tab shows all the credentials registered in the site. Click the headings of User Name, Bit Format, Badge ID, Facility Code, or Issue Code to sort the list by the heading.



Bluetooth communication is required for Mobile Credential use and must be turned ON when using a Mobile phone. The Schlage Mobile Access application will warn the user anytime Bluetooth is turned OFF. Bluetooth is required for this application. Android devices will require Locations Services to be enabled whenever Bluetooth is turned ON although the Schlage Mobile Access application will never track the user's location.

Add a Credential to a User

Adding a credential to a user connects the credential to the specific user. This process identifies the user in both the ENGAGE Audits and in the ENGAGE Device databases. Only one credential can be added per user.

1. **Log In** and open the **Users Tab**.
2. Select a current user.

Fig. 12.14: Select a User

3. From the Users card, select Add Credential.

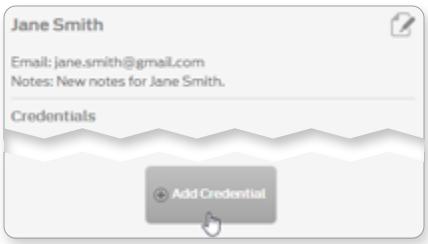


Fig. 12.15: Add Credential Button

4. Type the mobile phone number into the Mobile Phone Number box.

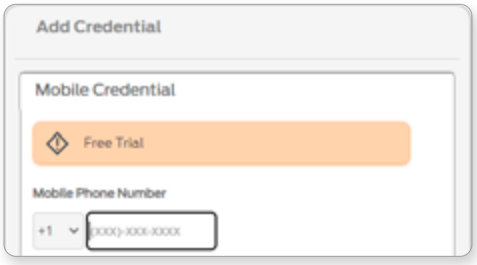


Fig. 12.16: Add Credential

5. To change the bit format, click Change and then select the desired bit format. Then click Done.

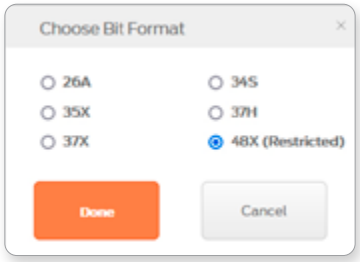


Fig. 12.17: Change bit format

6. Select Save.

   ➔ **Note:** The user's mobile phone will receive an automated text with additional instructions.

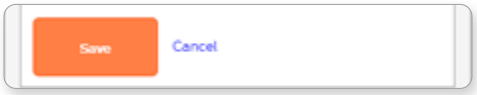


Fig. 12.18: Save Button

7. The Credential added banner is displayed and the new credential is displayed.

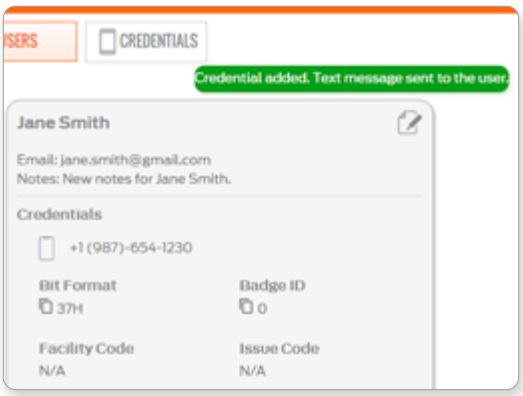


Fig. 12.19: New Credential Added

Delete a Credential

1. **Log In** and open the **Users** tab.
2. Select the user whose credential needs to be deleted.

Fig. 12.20: Select a User

3. Select Delete this credential.

Fig. 12.21: Delete this credential

4. Type DELETE into the Confirm: box.
5. Select Delete.

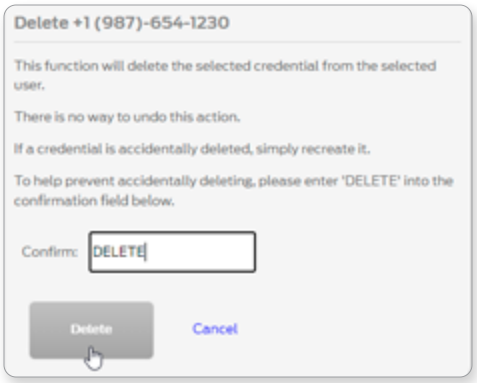


Fig. 12.22: Delete Credential

6. The confirmation message will be displayed.

> ⚠ **CAUTION:** Devices that had access with the credential must be programmed before the deleted credential will be denied access. ❗ is shown next to doors that require programming.

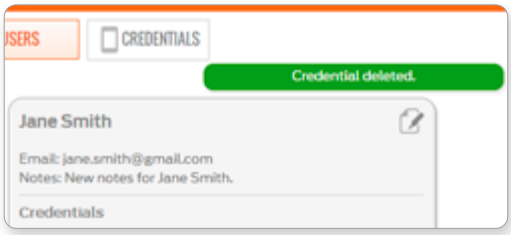


Fig. 12.23: Credential deleted

Resend Text Message

1. **Log In** and open the **Users** tab.
2. Select the user to whom you want to resend the text message.

Fig. 12.24: Select a User

3. Select Resend text message.

Fig. 12.25: Resend Text Message

4. The confirmation message will be displayed.

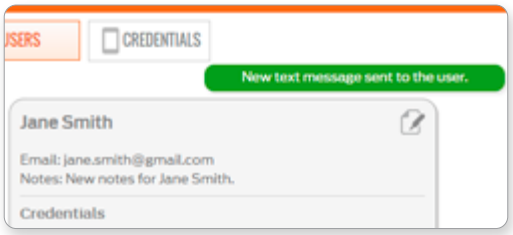


Fig. 12.26: Text message confirmation

View and Export Credentials

1. **Log In** and open the **Credentials** tab.
2. Click the headings of User Name, Bit Format, Badge ID, Facility Code, or Issue Code to sort the list by the heading.
3. Click the export button to export the list to a .csv file. The file will be generated and downloaded automatically.

Fig. 12.27: Export credentials

Credentials

⚠ CAUTION:
Construction Mode: BE467 and FE410 Control devices require the 9651 Schlage MIFARE Classic® Smart 8K bit credential to be used for Construction Mode access. All other ENGAGE devices may use any normally valid credential.

There are three types of User Access credentials supported by ENGAGE.

Table 13.1 Credential Types

Type	Description	Enrollment	Notes
Smart	A physical credential that is contactless and is available in ISO card, thick fob, and thin fob formfactors. Read/write capable. Encrypted and secure. Based on open-architecture NXP MIFARE standards and ISO14443.	Enroll quickly into a credential pool via the MT20W (bulk or individual use) or directly at the lock. Credentials directly enrollment at the lock cannot be used for No-Tour.	Supports No-Tour with a limit of 11 doors or groups of doors.
Proximity (Prox)	A physical credential that is contactless and is available in ISO card, thick fob, and thin fob formfactors.	Enrolled individually as needed via the MT20 or directly at the lock.	DOES NOT support No-Tour functionality.
Mobile	A digital credential that is issued to a user's smart phone.	Generated individually from the ENGAGE Web App. User receives a text message invitation to download the Schlage Mobile Access app and start using their credential.	Supports No-Tour functionality without the 11 door or door group limitation

The Administrator must manage the enrolled credentials and match each individual credential ink stamp number when actual User assignments are made.

Enroll Smart Credentials in Bulk

Bulk physical credential enrollment is the recommended credential enrollment process. This will allow faster initial property setup and streamline the credential assignment processes later. An MT20W reader is used to complete enrollments. When a new credential is presented to the reader, it will be added to the Select Existing Credential tab on the Add Credential menu.

Fig. 13.1: Ready MT20W

Using Wi-Fi Connectivity:

1. Make sure the MT20W is commissioned and ready.

   ➔ **Note:** See **Commissioning the MT20W** for more information.
2. Present a new credential to the MT20W. The MT20W will turn GREEN and beep one (1) time when the credential is accepted.
3. Wait a few seconds for the MT20W to return to “Ready” with the BLUE LED illuminated.
4. Repeat steps 2 and 3, presenting new credentials, one-at-a-time until all credentials have been enrolled.

Using USB connectivity:

1. Make sure the MT20W is commissioned and ready.

   ➔ **Note:** See **Commissioning the MT20W** for more information.
2. Go to the ENGAGE Web application and **Log In** to your account.
3. Ensure the ENGAGE Desktop Application is running on the computer.

   ➔ **Note:** See **Installing the ENGAGE PC Desktop Application** for more information.
4. Plug the MT20W into a computer for power and communication with the computer. Wait a few seconds for the MT20W boot up process to complete and for the ENGAGE Desktop Application to connect with the MT20W.
5. Present a new credential to the MT20W. The MT20W will turn GREEN and beep one (1) time when the credential is accepted.
6. Wait a few seconds for the MT20W to return to “Ready” with the BLUE LED illuminated.
7. Repeat steps 5 and 6 presenting new credentials, one-at-a-time until all credentials have been enrolled.

To verify and view the recently enrolled credentials:

1. Select a new or existing User, select the Add Credential button.
1. Select the Select Existing Credential tab.
2. View each of the recently enrolled and available credentials. The recently added and unassociated bulk credentials will appear.

   ➔ **Note:** If the credentials do not appear in the list, wait a few seconds and select the Refresh List button to try again.

Fig. 13.2: Select Existing Credential

Enroll a Smart Credential Individually

An administrator must enroll a new credential whenever a new user is added or a credential needs to be replaced.

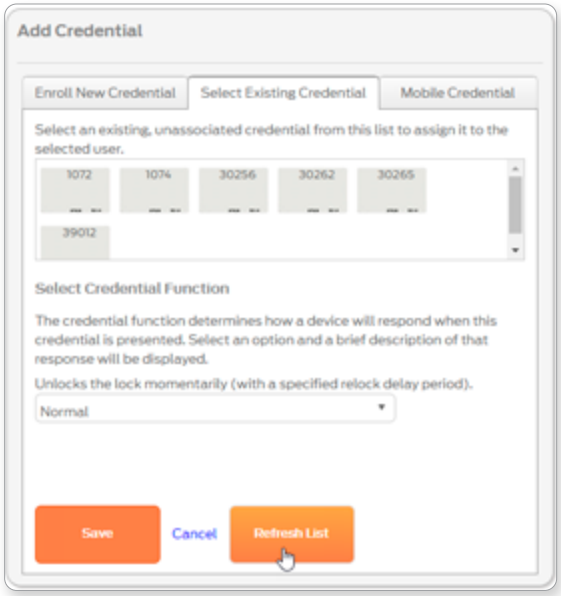


Fig. 13.3: Individual Credential 1070 Enrolled

1. Plug the MT20W credential enrollment reader into the computer's USB port. Wait a few seconds until the reader boots up and begins communication. The LED will light solid BLUE when ready.

   ➔ **Note:** If the MT20W LED is solid RED after power is applied and the boot process is completed, the MT20W is not commissioned or communicating and/or the ENGAGE desktop application is not running (USB communication mode).

2. **Log In**.
3. Hover over the Users menu and then select Users from the pull-down.
4. Select the appropriate user.
5. From the user's card, select Add Credential.
6. Select the Select Existing Credential tab.
7. Present the new credential to the MT20W.
   The MT20W turns GREEN and beeps 1 time when the credential is accepted.
8. Wait a few seconds and then select Refresh List. The "Ink Stamped" number on your credential will appear in the Select Existing Credential list.

   ➔ **Note:** If the credential number does not appear in the list, wait a few seconds and select Refresh List again.

   ➔ **Note:** Once the individual credential has been enrolled, it is now available for immediate assignment to a User. If credentials are enrolled into stock, be sure to label the credential with the Ink Stamp # for reverence and User assignment, later.

When using multi-technology credentials and ENGAGE locks with multi-technology credential readers as your credential enrollment reader, disable the card technology in the credential reader (lock) that is not wanted before attempting credential enrollments. Otherwise the credential technology (Smart or Proximity) desired may not be the credential technology that is actually enrolled.

Enrolling a Credential at a Door

It is possible to assign a credential to a User in ENGAGE using the ENGAGE Mobile Application and an installed device.

This credential assignment method allows the Administrator additional flexibility for quick credential enrollment and assignment.

➔ **Note:** This method is NOT recommended because some functionality normally available in ENGAGE is not available.

WARNING: ENGAGE cannot track these credentials because the "Ink Stamp" is not known when using this enrollment process. Badge Searches and credential identification by the "Ink Stamp" is not possible.

1. **Log In** to the mobile application.
2. Locate any nearby and commissioned ENGAGE device to use as an enrollment reader.
3. Select the Users menu and the specific user to be assigned a new credential.

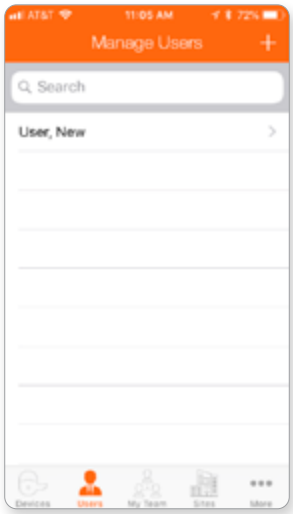


Fig. 13.4: Manage Users

4. Select the Credentials Menu.
5. Select the + sign to identify devices in-range that can be used as an enrollment reader.
   - In this case five (5) devices are in-range. We will use the lock named Storage as our enrollment reader.

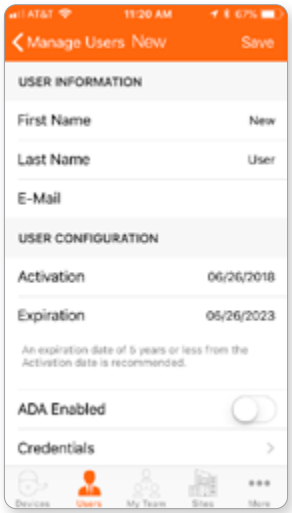


Fig. 13.5: User Profile

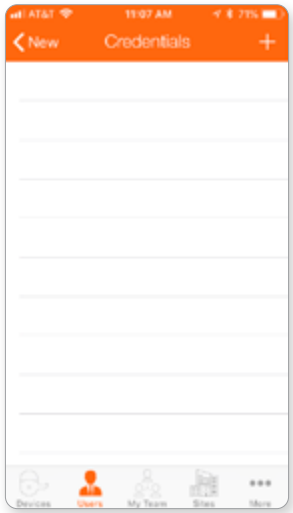


Fig. 13.6: Credentials

6. Select a specific device from the Available Enrollment Readers list.

➔ **Note:** After selection, the selected device LED flashes RED.

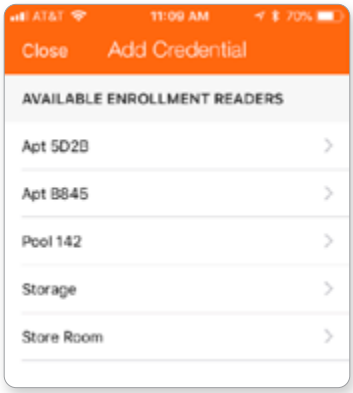


Fig. 13.7: Add Credential

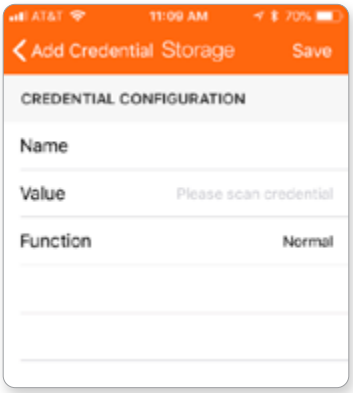


Fig. 13.8: Credential Configuration

The process times out after 20 seconds.

When the device reads the credential, the credential value recorded is displayed with asterisks ********. The default credential NAME is Credential 1.

7. Present the new credential to the nearby storage device.
8. Select Save.
9. VERIFY SUCCESS: See the Credential Enrolled Successfully! Message.
10. Select Ok.

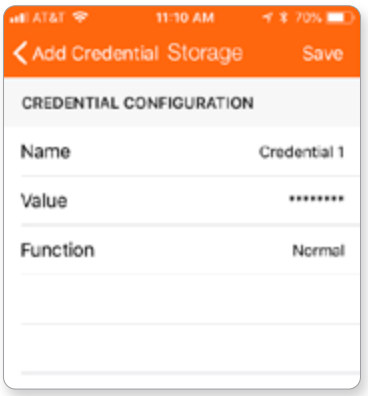


Fig. 13.9: Credential Enrolled

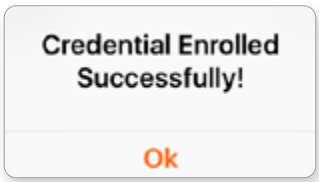


Fig. 13.10: Credential Enrolled Successfully

Resend Mobile Credential Invitation

1. **Log In** to the mobile application and open the **Users Tab**.
2. Select the appropriate user.

Fig. 13.11: Select a User

3. Select the mobile credential.

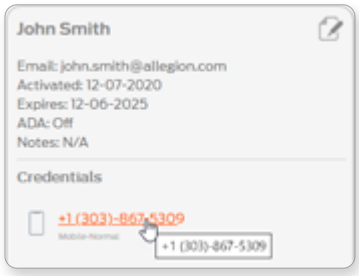


Fig. 13.12: Select Mobile Credential

4. Select Resend Text Message.

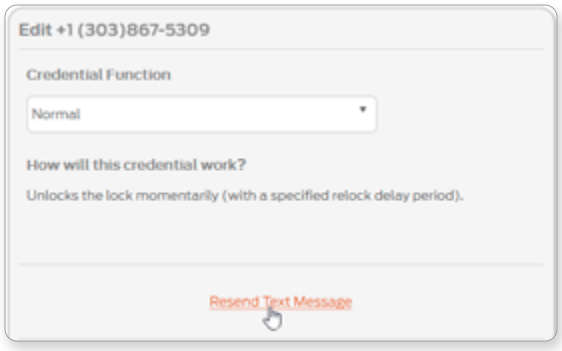


Fig. 13.13: Resend Text Message

5. The user will receive a text message. The screen shows New text message sent to the user.

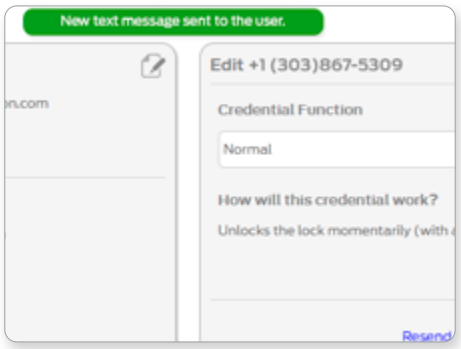


Fig. 13.14: Text Message Resent

See **No-Tour Feature** for more information.

No-Tour Credential Programming

The ENGAGE No-Tour feature allows Administrators to assign and change access rights without visiting the lock or performing **Synchronization**.

The Administrator can program a physical Smart credential and/or Mobile credential in their office with new or changed access rights and have that credential make the changes at the affected door(s) when the credential is presented by the credential holder for normal access.

Search for Credentials in ENGAGE

A badge ID search can be performed to identify the owner of a found credential using the Ink Stamp number to locate its owner.

For example, search for the owner of a found ID number S26A74678-01070.

1. **Log In** to the web application.
2. Select Advanced menu, then the Credentials tab.

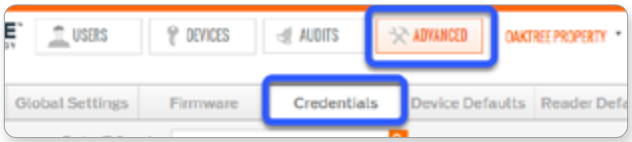


Fig. 13.15: Advanced > Credentials

3. In the Badge ID Search field enter the numbers after the dash located on the credential.
4. Click the magnifying glass icon.

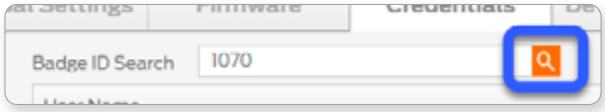


Fig. 13.16: Badge ID Search

5. If found, name of owner will appear.

Fig. 13.17: ID Found

If a credential is enrolled at a door, the credential is NOT searchable. Only credentials enrolled individually or in bulk using the MT20W or MT20 credential enrollment readers are searchable.

6. If not found, error message appears. Click OK and try again.

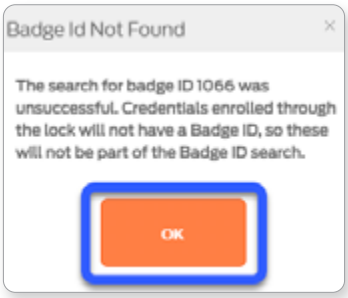


Fig. 13.18: ID Not Found

Physical Credential Reuse: Best Practices

Physical smart credentials can be reused and reassigned many times. There is no limitation on how many times a credential may be issued and reassigned.

To reuse a credential you can either delete it or expire it. Once deleted or expired you need to perform **Synchronization** on each lock that credential was assigned to or wait for a Wi-Fi sync. Using only no tour will not work. Locks must be synced to complete the process.

First, there are a few things to remember about No-Tour physical credentials.

- Each credential will allow up to 11 door, and Door Groups assignments at one time
- Multiple doors can be grouped together into **Device Groups** to allow multiple doors to occupy only one door assignment on the credential. This allows for the credential to have access to as many doors as necessary (exceeding the 11 individual door assignment limit)
- Individual door access and device group assignments that are “Deleted” will continue to occupy a door assignment on the credential. A Deleted door assignment is labeled as “Blocked” on the credential and will be denied access.
- Credentials that are merely “Deleted” from the system will retain the previously assigned access assignments.
- Credentials that “Expire” due to the User expiration setting, will free up the 11 available door assignments and again allow up to 11 new individual and Door Group assignments.

WARNING:
Be aware that ENGAGE devices were not initially Mobile Enabled. The devices on your property may need to be updated to include Mobile Credential support. The original wall mounted MT readers used with CTE cannot be upgraded for Mobile Enabled MTB compatibility.

Mobile Credentials

Mobile Credentials are available for both iOS and Android devices and require a free application to be used to manage the credential.

Users may be assigned ONLY one Mobile Credential at a time. Mobile Credentials enrolled into an ENGAGE property CANNOT be assigned and used in any another ENGAGE property.

Both physical and mobile credentials may be assigned to the same user, if desired.

Mobile credentials must have a license as of September 5, 2023. Three (3) free licenses are available with each site. Additional licenses can be purchased and managed using the License Manager in the Allegion 360 Portal. See **License Type** on page **125** for more information.

Fig. 13.19: Mobile Credential

License Type

License Type	Expiration*	Mobile No-Tour	Renewal	Reassign	Description
Free Trial	none	??	n/a	No	• Assigned to all existing Mobile Credentials. • Any change will prompt an upgrade to a free or paid license, or change to a physical credential.
Free	none	Yes	n/a	Yes	• Three (3) per site. • Only one free license can be assigned to a credential.
One Year Flexible	one (1) year	Yes	• When more than one license is assigned, the next license automatically replaces the expired license. • Up to three (3) One Year Licenses can be added to a Credential.	Yes	Can be reassigned indefinitely until expiration.
Reusable					A One Year Flexible License that has been unassigned from a credential.
Five Year Fixed	five (5) years	No	Add new license within 30 days of expiration. New replaces old after expiration.	Yes	Expires when unassigned from a credential.

* Expiration countdown starts the when the license is assigned the first time. Countdown runs even if the license has been unassigned from a credential.

View Mobile License Inventory

1. **Log In** to the web application.
2. Select the Licenses tab.

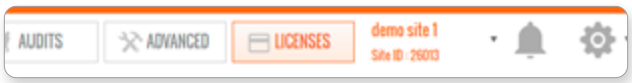


Fig. 13.20: Licenses

3. All currently available mobile licenses are displayed.
4. To be notified about licenses that are expiring, select the slider below Email Notifications (on by default).
5. To change the frequency of the notifications, select one of the radio buttons below Email Frequency.

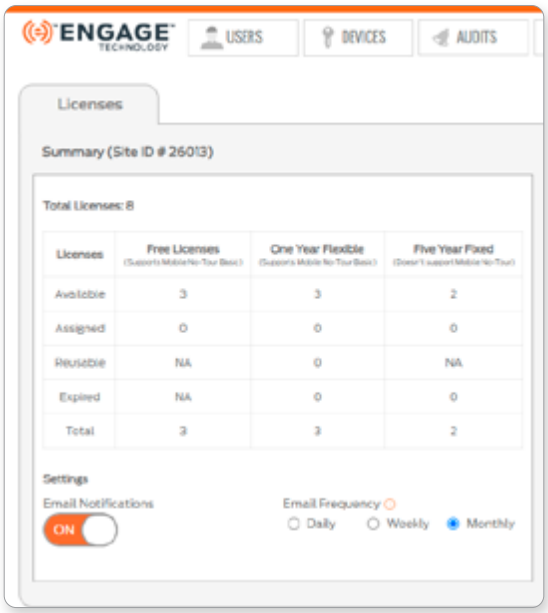


Fig. 13.21: Mobile licenses summary

6. The right side of the screen shows the Expiring soon and Expired licenses tabs.

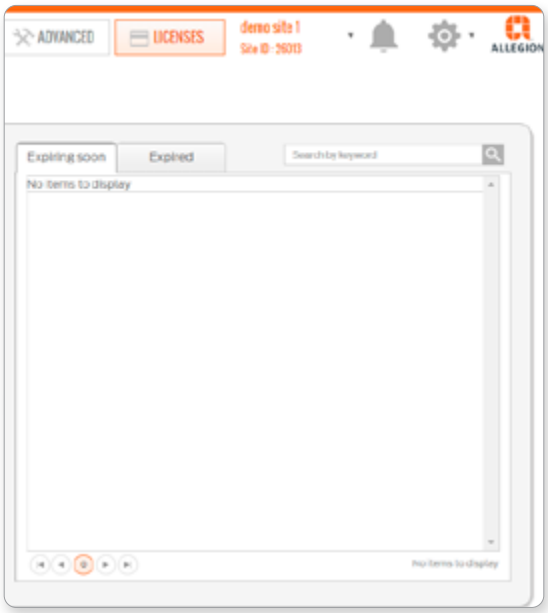


Fig. 13.22: Expiring soon and expired mobile licenses

Renew an Existing License

1. **Log In** to the mobile application and open the **Users Tab**.
2. Select the appropriate user.

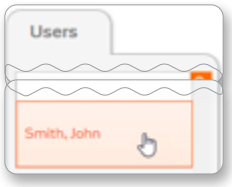


Fig. 13.23: Select a User

3. Select the mobile credential.

   ➔ **Note:** The current license is displayed below the credential.

Fig. 13.24: Select Mobile Credential

4. Select Renew license.

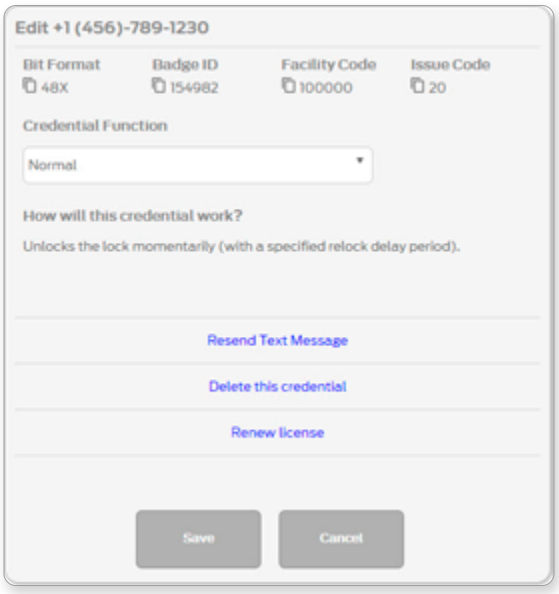


Fig. 13.25: Renew license

5. Choose the desired License Type from the drop-down box.

   ➔ **Note:** The license types will depend on the type of license that was already assigned. You may not be able to edit this field.

6. Choose the No. of Licenses from the drop-down box.

   ➔ **Note:** The number of available licenses and license types will depend on the licenses that have been purchased in the License Manager. See **View Mobile License Inventory** on page **126** for more information.

7. Click the Renew button.

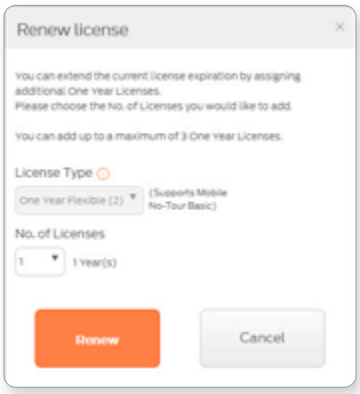


Fig. 13.26: Renew button

Assign a Mobile Credential

See **Commissioning the MT20W**.

Delete a Mobile Credential

When a mobile credential is deleted from a user, the license for that credential may be available to be assigned to another mobile credential, depending on the license type that was originally assigned. See **License Type** on page **125** for more information.

To delete the credential, see **Delete Credential**.

Change Starting Badge ID for Mobile Credentials

See **Set or Modify the Starting Badge ID**.

Exporting Mobile Credentials

Mobile credentials can be exported from ENGAGE to a .csv file, so they can be enrolled into a PACS system.

1. **Log In.**
2. Select the ADVANCED menu.
3. Select the Credentials tab.

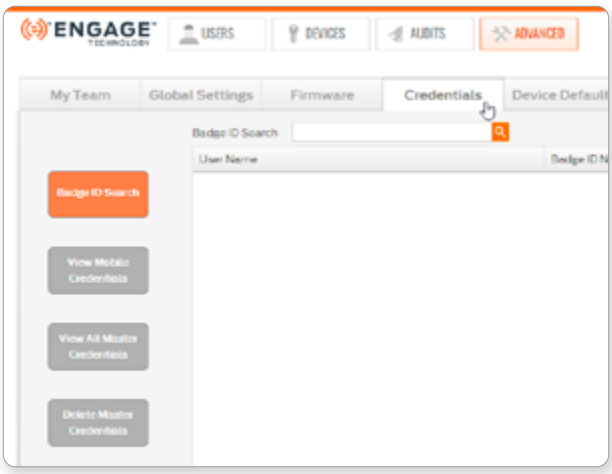


Fig. 13.27: Advanced > Credentials

4. Select the View Mobile Credentials button.

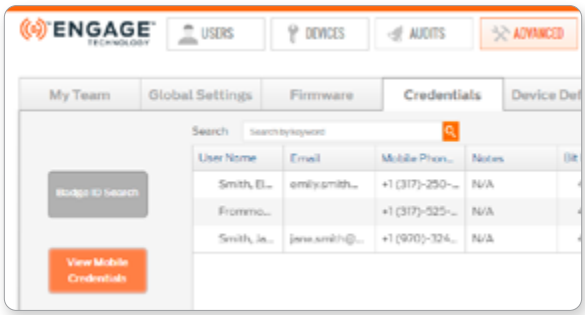
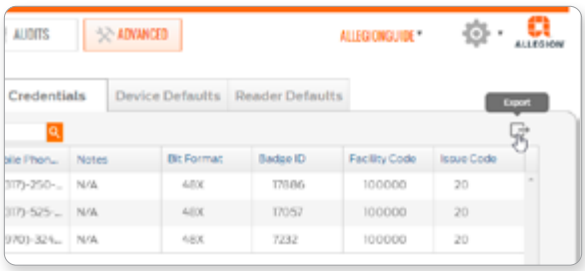


Fig. 13.28: View Mobile Credentials

5. Select the export icon to export all mobile credentials. A .csv file will be generated.

➔ **Note:** If you have any questions about importing credentials into PACS, PropTech, or any other access control system, contact your representative for directions on how to enter, save and activate Schlage Mobile Bluetooth credentials.



Schlage Mobile Access Application

Once a valid user Mobile phone number is entered and saved within the ENGAGE system, a text message is issued to the user with instruction to download the Schlage Mobile Access application.

User will receive a text message and instructed to download the application from the App Store or the Google Play Store.

Internet access is needed for these steps.

1. Download the Schlage Mobile Access application.
2. Accept the terms and conditions.
3. Set up your security authentication.

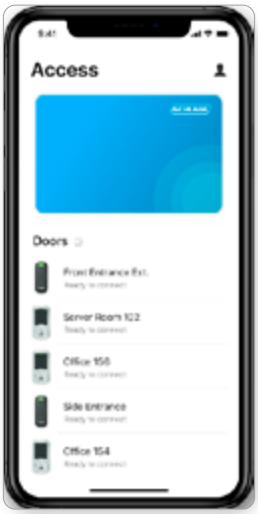


Fig. 13.29: Schlage Mobile Access Application

Use the Mobile Access Application to access a Door

After users have downloaded, installed and setup the Schlage Mobile Access application, they can begin to access assigned doors using their new Mobile Credential.

1. Open the Schlage Mobile Access application on a mobile phone.

   ➔ **Note:** Notice one level of security is required.

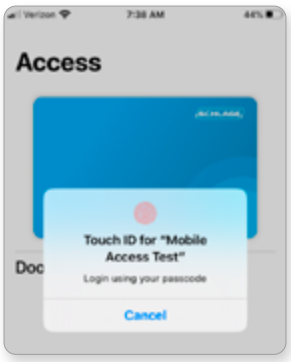


Fig. 13.30: Schlage Mobile Application Security

If no doors are displayed, refresh the screen.

2. Stand close to an assigned door.
3. View the available mobile enabled devices (doors) that are nearby.
4. Select the desired device.
5. Wait a moment for the door to momentarily unlock and enter.

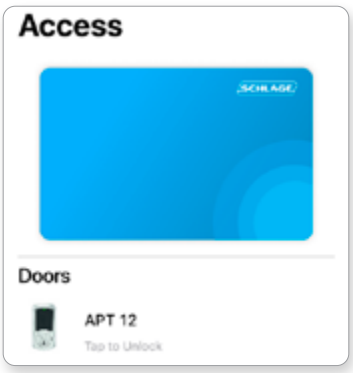


Fig. 13.31: Available Doors

6. Access is granted.

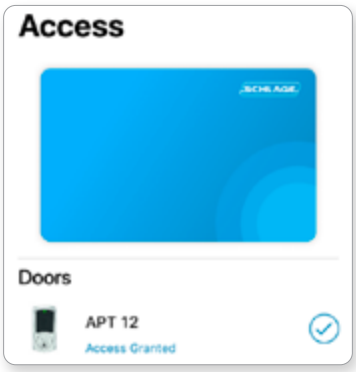


Fig. 13.32: Access Granted

WARNING: A LOST credential is still valid at previously programmed doors until the lock is presented with the replacement No-Tour credential or a new device Sync (door file update) is performed.

Replace a Credential

Replacing a credential swaps one credential for another. The new credential carries the same access assignments as the original credential and blocks or deletes all access from the original (damaged/broken or lost) credential.

This feature is most useful when credentials are damaged/broken or when the original credential is lost.

1. **Log In** to the web application.
2. Select Users > Users.
3. Select the appropriate user from the Users list.
4. From the Users card, Select the enrolled blue credential to open the Edit Credential card.

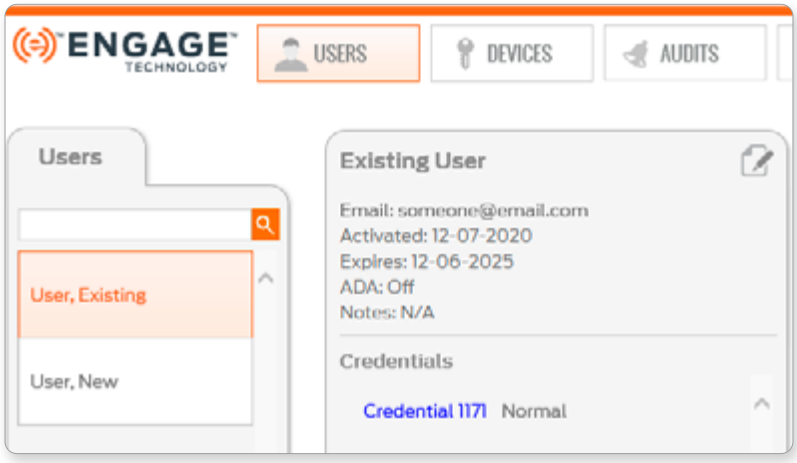


Fig. 13.33: Select Credential

5. Select Replace this credential.

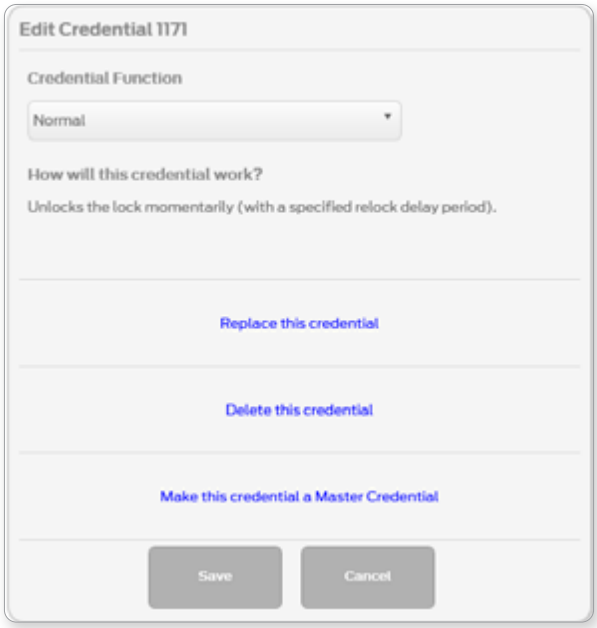


Fig. 13.34: Edit Credential

WARNING:
Physically locate the credential in your Credential Stock and verify the ink stamp matches the assigned credential from the stock list before Confirming the Replacement.

6. Select a Replacement Credential from stock list.
   - If no credentials are available for replacement, you must enroll a credential now.

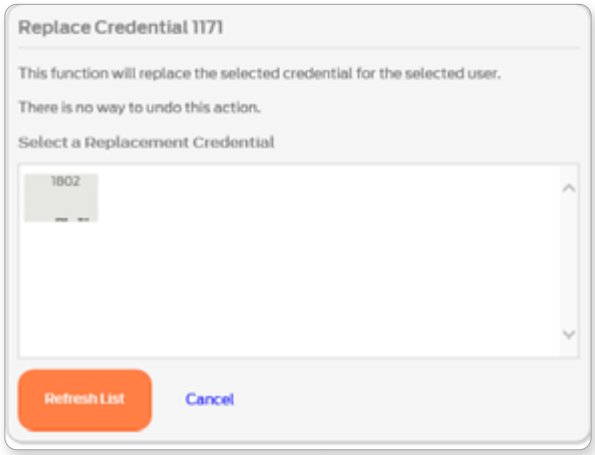


Fig. 13.35: Replace Credential

7. Select Confirm.
8. View the momentary Credential Replaced Successfully message.

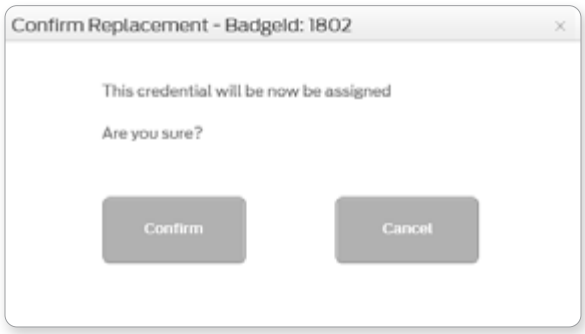


Fig. 13.36: Confirm Replacement

9. The new is now listed under the Existing User Credentials and the old replaced credential has been removed from the list.

Fig. 13.37: Credential Replaced Successfully

10. The credential now needs programming with the Schlage MT20W.

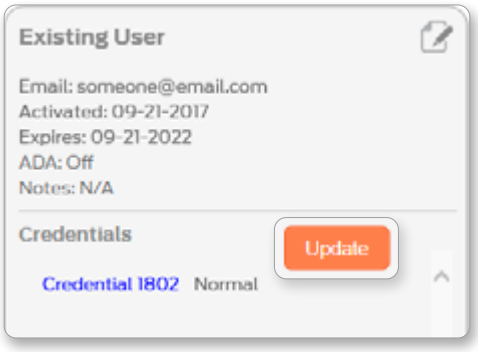


Fig. 13.38: Credential needs programming

Master credentials may not be reused.

Using Master Credentials

Overview

Serious consideration and consultation with local authority should be done BEFORE enabling and generating Master Credentials. Master Credentials may not be allowed for your property. Verify with your Authority Having Jurisdiction (AHJ) before proceeding. Read and understand the Important notes below before proceeding.

WARNING: Each ENGAGE site can have no more than thirty (30) Master Credentials. Exceeding this number may cause commissioning errors when adding new locks. Delete unused Master Credentials where necessary.

IMPORTANT NOTES:

1. Master Credentials are generally used for Property Maintenance, local Fire Department and emergency access to all openings on the property

BEST PRACTICE: Enable this setting before commissioning any devices.

2. The ENGAGE Master Credential feature is DISABLED by default and may be enabled after consultation with local jurisdiction.
3. Best Practice is to ENABLE Master Credentials when setting up the site for the first time.
   - Device commissioning is required to install the defined Master Credentials.
   - Any device commissioned before the Master Credential feature is enabled will require Sync, overnight update (Door File update) to enable the feature at the door.
4. A Master Credential allows PASS THROUGH credential function access.
5. No-Tour updates cannot be used to Enable or Disable the Master Credential function at a door. Sync or commissioning is required.
6. No-Tour programming can ADD Master Credentials. However, to DELETE a Master Credential, the credential must be deleted in the ENGAGE database and every lock must Sync.
7. Any valid User credential type can be assigned as a Master Credential.
8. Multiple Master Credentials can be generated for the same property.
9. Lost Master Credentials require every originally programmed device to be re-programmed to remove the lost Master Credential.
10. No-Tour updates can enroll a new Master Credential and block an old (lost) Master Credential, however it is RECOMMENDED that Master Credential replacements and deletions be accomplished via the Sync process (Door File updates) across the whole property.
11. DELETED Master Credentials are permanently DELETED and can never be used again in the same ENGAGE account – ever.

BEST PRACTICE: Destroy any Deleted Master Credentials.

Enable Master Credential

WARNING: Each ENGAGE site can have no more than thirty (30) Master Credentials. Exceeding this number may cause commissioning errors when adding new locks. Delete unused Master Credentials where necessary.

1. **Log In**.
2. Select the ADVANCED menu and Global Settings tab.
3. Slide the Master Credentials button to ON to enable the generation of Master Credentials. The Master Credentials Setting Updated message will appear.
4. You **must** sync all devices (update Door file) that were commissioned before enabling the Master Credential.

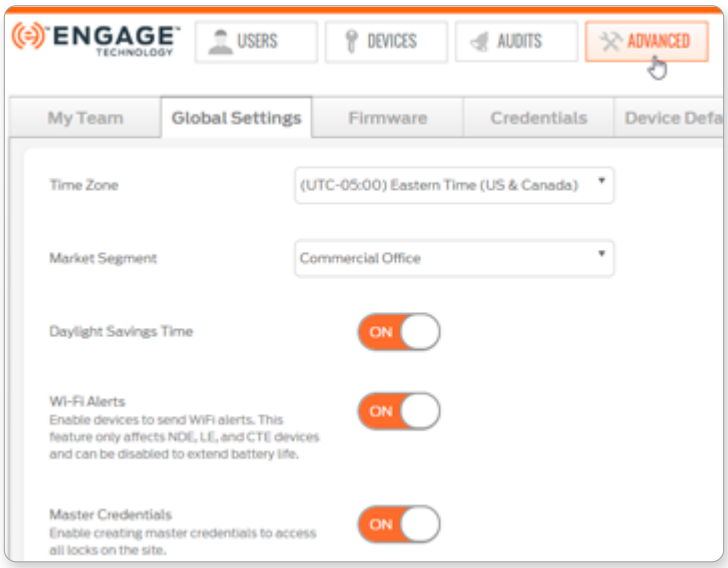


Fig. 13.39: Master Credentials ON

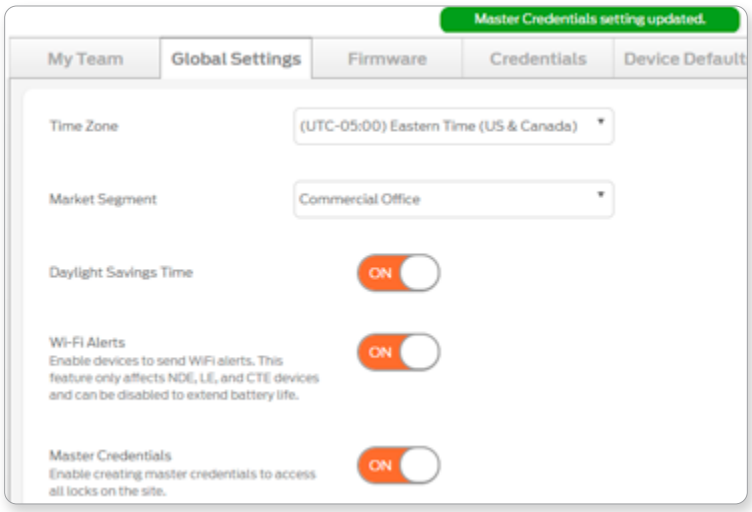


Fig. 13.40: Master Credentials Setting Updated Message

Any type of credential can be a Master Credential, including mobile credentials.

Assign a Credential as Master

1. **Log In**.
2. Select USERS > Users tab and the User intended to receive a MASTER CREDENTIAL.
3. Select a currently assigned credential that is to become a MASTER CREDENTIAL.

BEST PRACTICE: Give the User a name that identifies them as a Master Credential holder in Device Audits. In this case we picked the current User, **Master Credential-1** with Credential 39012 already assigned.

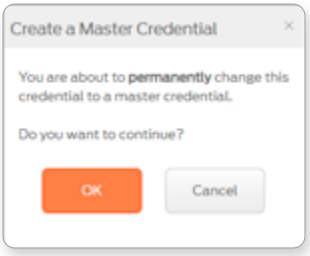


Fig. 13.41: Create a Master Credential Warning Message

If the Make this credential a Master Credential is NOT available, the feature has not been enabled yet. **Enable Master Credential** first and then try again.

4. Select Make this credential a Master Credential.

   ➔ **Note:** There is no need to select Credential Function from the Pull-Down menu. All Master Credentials are automatically programmed with the "PASS THROUGH" credential function.

5. Select OK to acknowledge the WARNING message.

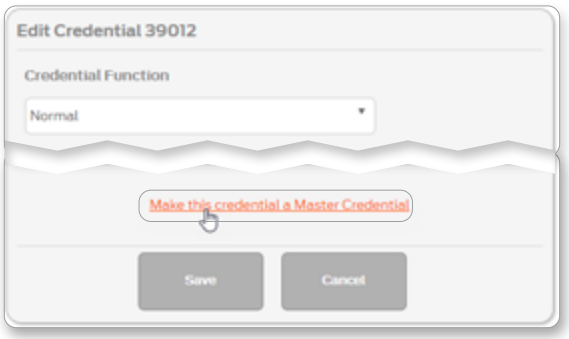


Fig. 13.42: Make this credential a Master Credential

6. The User's assigned credential will now have the Master Credential ICON next to the credential indicating it is programmed as a MASTER CREDENTIAL with the PASS-THROUGH function assignment on every lock.

   Select Update in the Credentials screen.

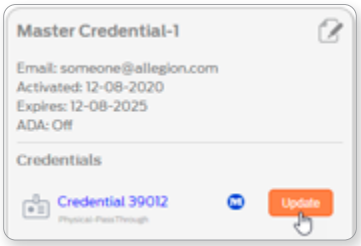


Fig. 13.43: Update Master Credential

7. Follow the instruction provided on screen, then select Next.
8. Select Finish.

➔ **Note:** Every Device now has the Device Update ICON displayed to inform the Administrator that door updates are needed. The Master Credential itself and all devices are required to be updated before these changes are honored. The Administrator must ensure all doors on the property are updated with No-Tour or Sync (Door Files updated) to add the new Master credential.

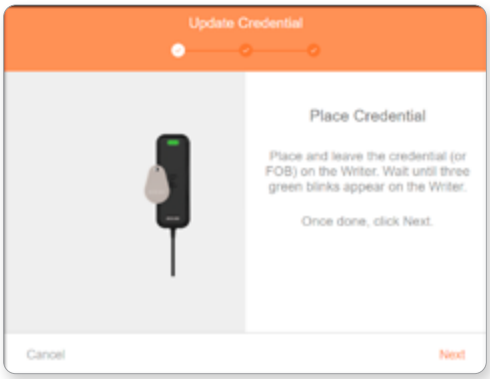


Fig. 13.44: Update Credential

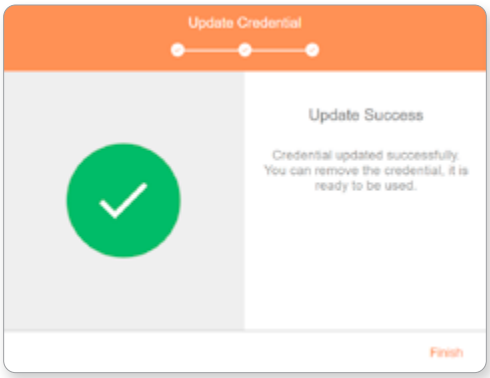


Fig. 13.45: Update Success

View and Delete Master Credential

WARNING: Each ENGAGE site can have no more than thirty (30) Master Credentials. Exceeding this number may cause commissioning errors when adding new locks. Delete unused Master Credentials where necessary.

1. **Log In**.
2. Select the ADVANCED menu and then select the Credentials tab.
3. Select the View All Master Credentials button. All Users with Master Credential assignments are displayed.

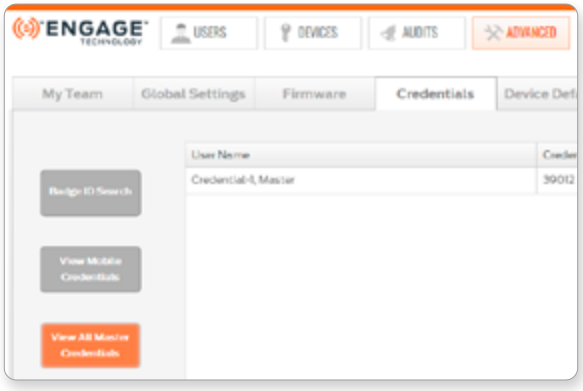


Fig. 13.46: View All Master Credentials

4. To delete Master credentials select Delete Master Credentials button.
5. Select the checkbox for each Master Credential to be deleted.
6. Select Delete.

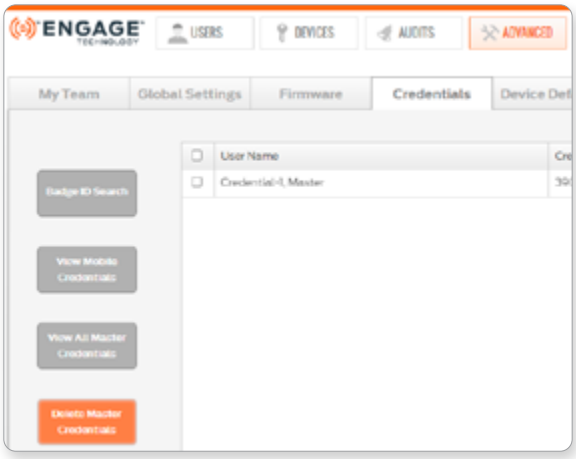


Fig. 13.47: Delete Master Credentials

7. Select OK to accept the Delete the Master Credential WARNING message.
8. Verify that the selected Master Credential has been removed.

➔ **Note:** This process removes the Master Credential from the ENGAGE database and schedules the changes needed for the property. All devices in the now show the Device Update ICON when an update is required.

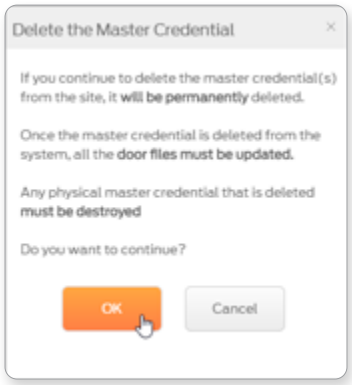


Fig. 13.48: Delete Master Credentials Warning

Credential Functions

Credential Function	Definition
Normal	Unlocks the lock momentarily. Relock delay period is 3 seconds, by default. Relock delay setting can be changed per device, as desired.
Toggle	Changes the state of the lock from locked to unlocked or unlocked to locked. Schlage Control **does not** support Toggle credentials. When a Toggle credential is programmed into a Control, the lock engages the thumb turn for the defined relock delay period.
Freeze	Freezes the lock in its current state (locked or unlocked). Lock remains frozen until a Freeze credential is presented again. The Freeze credential used to “unfreeze” a lock can be the same credential or a different Freeze credential.
One Time Use	Allows only one attempt with Normal Access granted. Schlage Control **does not** support One Time Use credentials and denies access anytime a One Time Use credential is presented.
Pass Through	Unlocks a lock momentarily. Gains access to a lock in Freeze and Lock Down states. Gains access during scheduled Holiday lockouts. Attempts to unlock a device that is in “Critical Battery Mode”.
Lock Down	Changes the state of the lock to locked and disables all normal user credentials. Pass Through credentials gain access when Lock Down is enabled. Freeze credentials must be used to return locks to normal state, from Lock Down
Block	Denies normal access to the lock and records the access attempt as an audit.

Control Mobile Enabled Smart Lock Installation and Commissioning

The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

Introduction

Go to https://commercial.schlage.com/en/products/electronic-locks/schlage-control-mobile-enabled-smart-locks.html for the full installation instructions.

BEST PRACTICE: Before installing, record the serial number and the intended location. This information is required for the Administrator to commission the device and entry into the ENGAGE account.

Tools Needed:

Phillips screwdriver and tape measure.

Optional - flathead screwdriver and a Torx™ driver.

Prepare to Install the Device

Interconnect

Verify the **Door thickness**, the **lock backset**, proper **hole dimensions**, and the proper **bore-to-bore** dimensions specified in the installation instruction. The center lines of the drilled cross bore holes and centered door alignment MUST be accurate for proper bolt and latch retraction.

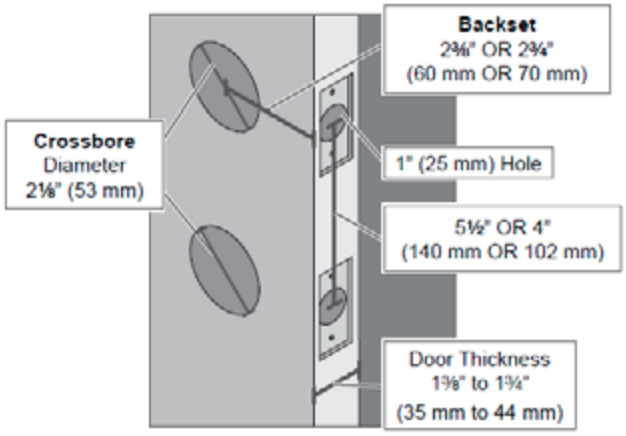


Fig. 14.1: Interconnect Door Prep requirements

Install the Device

Install the Schlage Control Mobile Enabled Smart Lock as directed in the installation instructions provided in the box.

WARNING: DO NOT USE A POWER DRILL for installation. Power tools may damage the product.

Pay special attention to the following items during the installation process.

For best results, ensure the following:

1. The bolt is **ALWAYS** retracted during installation.
   - If the deadbolt is not retracted when power is applied, the handing of the door and the electronic operation of the bolt is reversed.
2. The through door cable is routed from the exterior side **OVER** the top of the latch body and through the door.

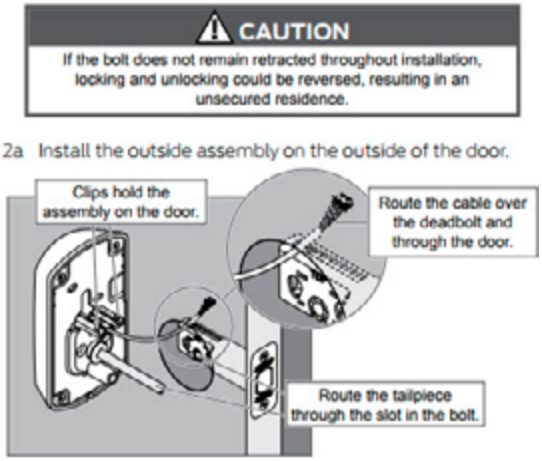


Fig. 14.2: Outside Assembly

3. Verify the CAM is in the correct vertical position with the switch lever contact pressed as shown above during installation. The CAM contacts the switch when in the correct vertical position.

Fig. 14.3: Cam Position

4. When plugging in the cable, be sure to connect with the RED wire on the bottom. The connecter is designed to fit in only one orientation. DO NOT FORCE THIS CONNECTION as connector damage is possible.

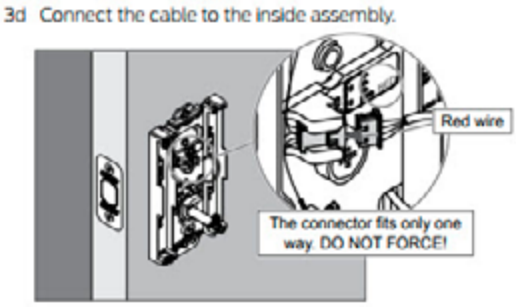


Fig. 14.4: Electrical Connection

5. When working with **INTERCONNECTED** units (FE410), pay attention that the “Handing Plate” and “Handing Screw” are installed properly. Verify the lever catch is in the correct orientation to allow proper lever installation (Handing) as shown.
6. Once the Control Mobile Enabled Smart Lock is properly installed:
   - The thumb turn should physically move the bolt in and out of the closed door and frame smoothly without resistance.
   - The outside thumb turn should spin freely until a valid credential is presented.
   - Interconnected lock smoothly retracts the bolt whenever the inside lever is used with no restrictions.
   - Upon Power-up the Control Lock boots up, flashes the **GREEN** LED and beeps 3 times. This is the indication that it is ready for Commissioning or Construction Mode operation.

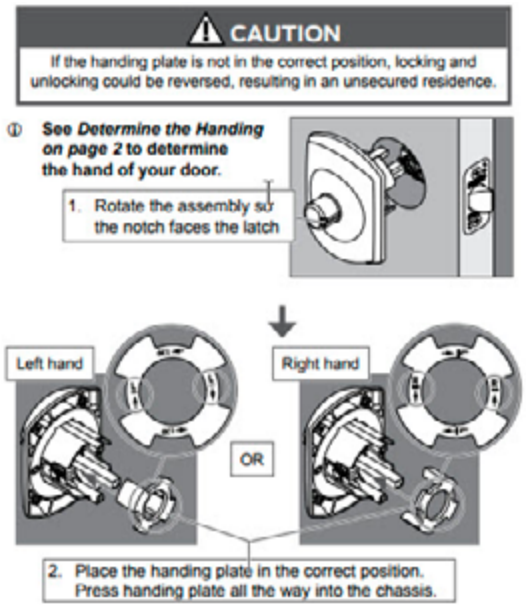


Fig. 14.5: Handing Plate

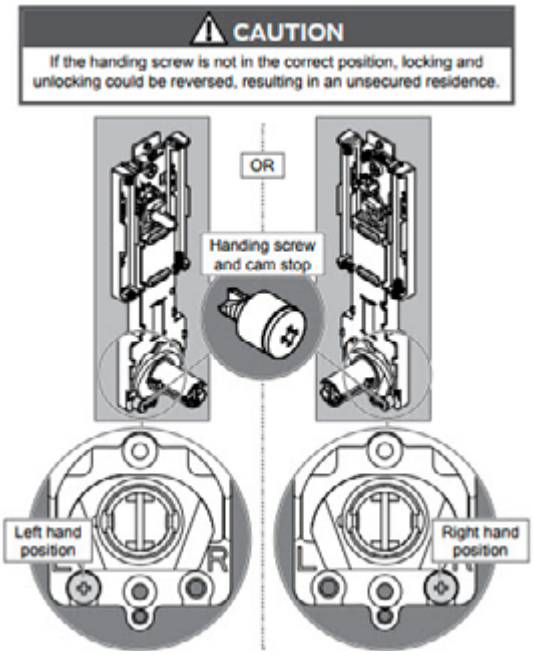


Fig. 14.6: Handing Screw

Factory Default Reset (FDR)

A Factory Default Reset (FDR) will return the Control Mobile Enabled Smart Lock to its original settings as shipped from the factory.

Additionally, the following will occur.

- The device will beep once when the inside lever is turned.
- Removes any non-default device settings, deletes any construction or user credentials, and allows construction mode to be entered again.
- Does **NOT** have any effect on the firmware currently on the device.
- Does **NOT** remove the Control Mobile Enabled Smart Lock from your ENGAGE account.

Images show the older version of Control, but the FDR process remains the same.

Perform a Factory Default Reset (FDR)

1. Remove inside cover.
2. Disconnect at least 1 battery for 10 seconds.
3. Reconnect batteries.
4. Wait for the lock to beep and flash GREEN 3 times.
5. Within 10 seconds, rotate the interior tailpiece back and forth 2 times.
   a. The lock flashes 1 long GREEN flash and beeps 1 long beep to indicate success.

Fig. 14.7: Interconnect

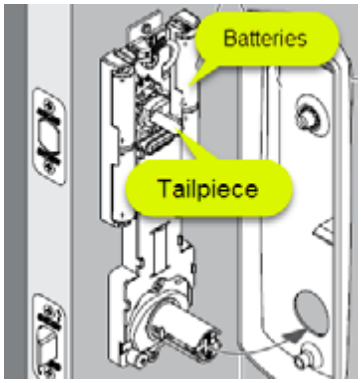
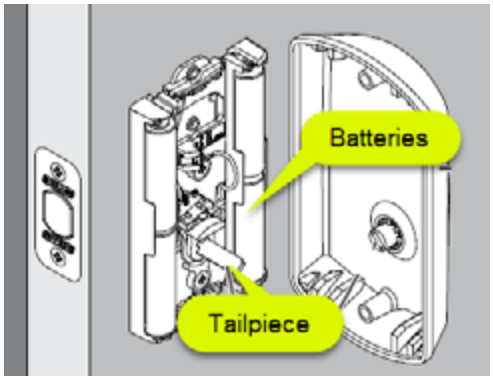


Fig. 14.8: Deadbolt



Verify Success of the FDR

The Control Mobile Enabled Smart Lock will “advertise” its presence via Bluetooth communication after FDR.

When properly reset, the Control Mobile Enabled Smart Lock will advertise its presence via its Bluetooth radio and is available for commissioning again.

Construction Mode

The Construction Mode is used to allow access before the lock is commissioned or during testing before commissioning.

- Construction Mode is a temporary mode of operation and is NOT required to be used.
- Construction Mode is enabled by default and after a successful Factory Default Reset (FDR).
- The lock will remain in Construction Mode until the mode is cancelled by a Factory Default Reset (FDR) or the device is commissioned into ENGAGE.
- No access audits are captured while the lock is in Construction Mode because the lock does not track time or credential numbers.
- Control devices will use the credential “Facility Code” as the Construction Credential ID.
- All credentials with the same Facility Code as the originally presented credential, will be allowed access during Construction Mode.

Create a Normal Construction Credential for Control

Enter Construction Mode:

- Control Mobile enabled Smart Locks will accept he first valid credential presented to set the “**Facility Code**” for all Construction cards to be used at the door.
- Any credential with the **SAME** Facility Code will be subsequently granted NORMAL access.
- Construction mode operation provides NORMAL Credential function.
  - Valid construction credentials allow the user to momentarily rotate the thumb turn to retract or extend the deadbolt.

Exit Construction Mode:

- To exit construction mode, retract the bolt and then use the Mobile application to commission the Control Mobile Enabled Smart Lock.
- All construction credentials are no longer valid once the lock is commissioned and exits construction mode.
- Construction mode can be cancelled by Commissioning or by performing an FDR.
- All previously valid Construction Credentials no longer function at the door after Commissioning or an FDR.

Verify Success - Construction Credential

1. Start with a Control just out-of-the box or recently reset.
2. Present a valid credential type with the Facility Code the Administrator wants to use as the construction code to the device.
3. Present the original credential or any other credential with the same Facility Code.
4. The device will unlock, while the lock is flashing GREEN, turn the outside thumb turn to lock and unlock door.
   - Locking and unlocking the deadbolt must be complete within the time the LED is flashing GREEN.
5. If device is not locked or unlocked while the LED is flashing a timeout will occur.
   - Repeat steps 1-2 to try again.

Review the **Wi-Fi Network Requirements** before you begin.

WARNING: **Before commissioning a device, Administrators should create any needed Schedules and review Property-Wide Settings.**

CAUTION: When commissioning a Control Mobile Enabled Smart Lock, the **No-Tour Feature** is automatically enabled.

Commissioning

Commissioning a device enrolls the device into ENGAGE, defines the device name, and prepares the device for later setup steps.

To commission a Control Mobile Enabled Smart Lock, follow these steps.

1. Apply power or cycle power by installing the batteries or temporarily remove an installed battery, wait a few seconds, then replace or install the battery(s).
2. Retract the deadbolt. Retracted bolt is required for Bluetooth "Advertising" to allow for Commissioning.
3. **Log In.** Stand near the device you want to commission.
4. All devices currently commissioned into the account will be displayed. A blank Devices Screen is displayed here, because no devices have been commissioned yet
5. **Select** the "+ "sign to begin the commission process.
   - **iOS Mobile device**: + sign in the upper right-hand corner.
   - **Android Mobile device**: + sign in the lower right-hand corner.
6. **Select** the Control Lock in the "Select a device type" screen.

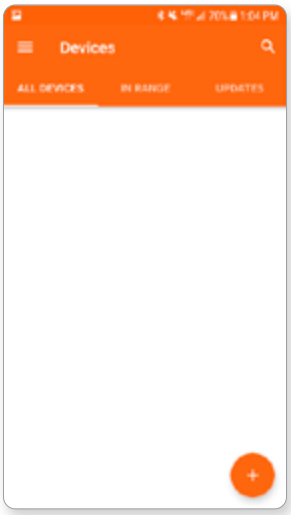


Fig. 14.9: Android Device Menu

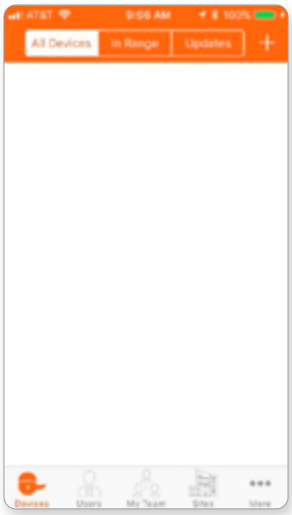


Fig. 14.10: iOS Device Menu

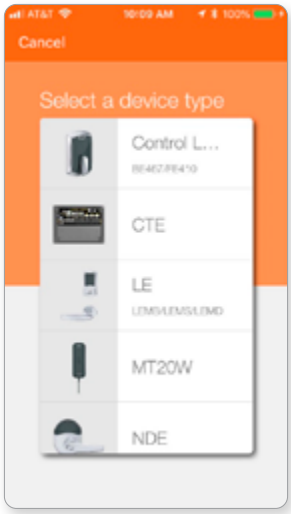


Fig. 14.11: Control Lock Screen

7. The next screen displays:
   - Only once per property
   - Only once for each Administrator
   - Only once for each product type

   ➔ **Note:** This is the ONLY reminder to think about and use the predefined **Property-Wide Settings** before setting up several devices. Administrators can use the currently defined default ENGAGE settings for this device or elect to modify the Property Wide settings now.

   ➔ **Note:** Administrators may modify individual device settings at any time, using the Customize Settings option also provided.

8. Select Use Default Settings to continue

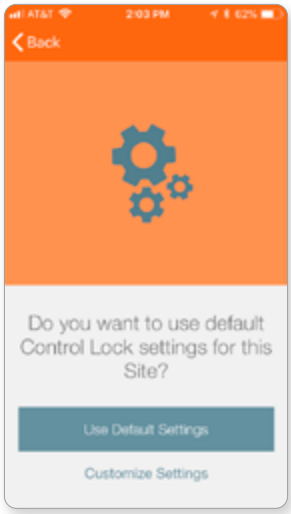


Fig. 14.12: Default or Customize

All nearby Control Mobile Enabled Smart locks with RETRACTED deadbolt and available for commissioning are displayed.

The Device serial number can be found on the sticker on the front of the Schlage Control Mobile Enabled Smart lock or on the inside plate.

When multiple Control locks are present, select the appropriate device by serial number, or just pick one and see which begins flashing.

9. Select the specific Schlage Control Mobile Enabled Smart lock to be commissioned from the list of new or recently Factory Default Reset (FDR) devices displayed.
10. Select the desired Schlage Control Mobile Enabled Smart lock for commissioning.

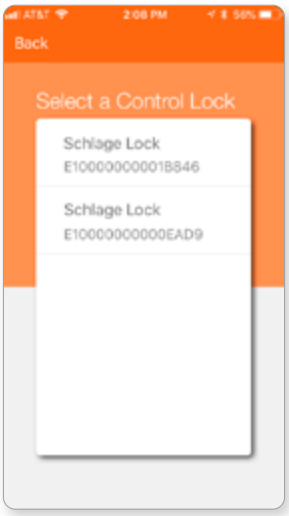


Fig. 14.13: Select a Lock Screen

11. Verify that the selected device LED is flashing RED.
12. Select YES to continue.
13. Enter a descriptive Lock Name for this Lock.
    - In this case we entered Storage Room.
14. Select Next.

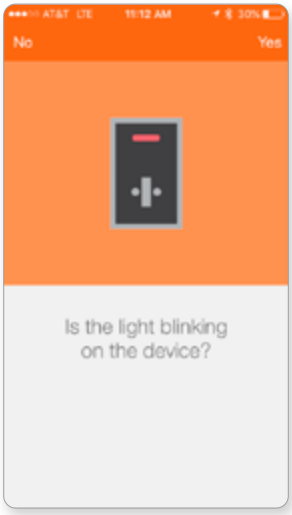


Fig. 14.14: Light blinking screen

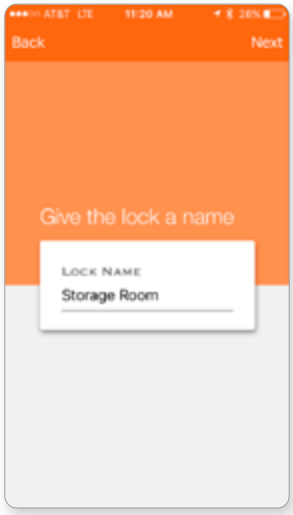


Fig. 14.15: Name Lock

15. View the Schlage Control device commissioned successfully **Check Mark** message.
16. Select Finish to complete the commission process or, select Add another Control device to continue enrolling additional Schlage Control devices.

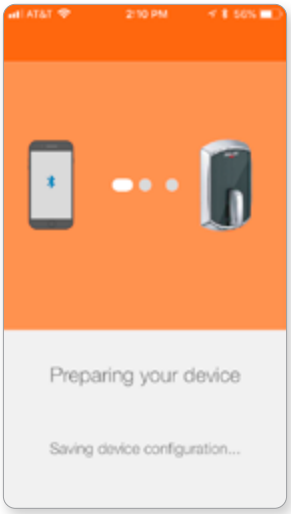


Fig. 14.16: Preparing your device

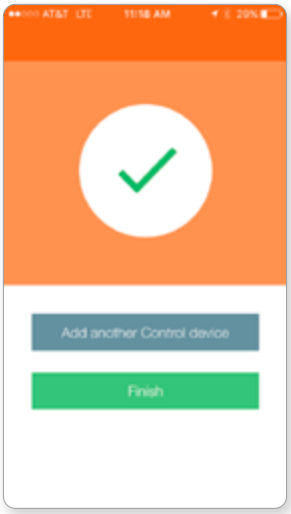


Fig. 14.17: Commission successful

17. The newly commissioned Schlage Control Mobile Enabled Smart Lock is now shown in the ENGAGE Mobile Application All Devices screen and the In Range screen, when nearby the device.

Fig. 14.18: In Range screen

XE360 Devices Installation and Commissioning

The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

Introduction

Before installing the device, review the Installation Instructions for the Schlage XE360 lock contained within the box.

Commissioning in the box

This lock series can be commissioned prior to installation. This is useful when a large number of locks need to be commissioned, and will then be physically installed by another person or at later time.

1. Remove and unwrap both the interior and exterior assemblies.
2. Connect the interior assembly's through-door cables to the exterior assembly.
3. Unwrap the battery pack and install the batteries.
4. Connect the battery pack to the interior assembly.
5. Follow the instructions for **Commissioning the Device** on page **152**.
6. Write the name of the lock and the intended location on the box.
7. Remove power and disconnect cables. Carefully replace the assemblies in the box.

   ➔ **Note:** The lock will retain the commission information even when power is removed.

Prepare for Installation

Tools Needed: Phillips screwdriver, pin wrench, tape measure

T-15 Torx screwdriver (optional).

1. Verify the door and jamb are properly prepared before attempting to install.
   - Each lock comes with a paper template in the box. Use this template to prepare the door for the lock you received.
   - When using DPS (door position switch), make sure to also prepare a hole in the jamb exactly opposite the hole in the door edge, when the door is closed.
   - The DPS wire routing hole on the face of the door is on the **interior of the door.**
   - The DPS wire routing hole is ONLY halfway through the door.

⚠ **CAUTION:** The centerline of the latch bore hole and the centerline of the though door bore MUST be accurate for proper latch retraction.

Install the Device

Use the instructions that came with the device for installation. Additionally, consult the online interactive instructions for further detail.

alle.co/XE360

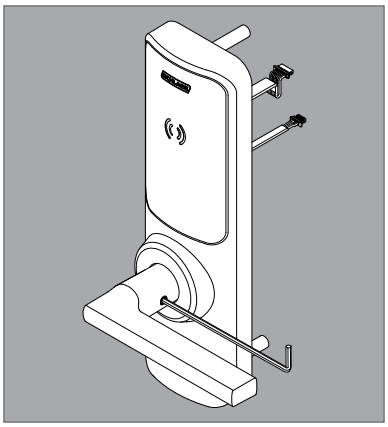
CAUTION: DO NOT USE A POWER DRILL for installation. Power tools may damage the product.

BEST PRACTICE: Record the serial number and final lock location prior to installation. The serial number is located on the sticker on the product, or the sticker on the box, or on the mobile app (MAPP) when connected to the lock.

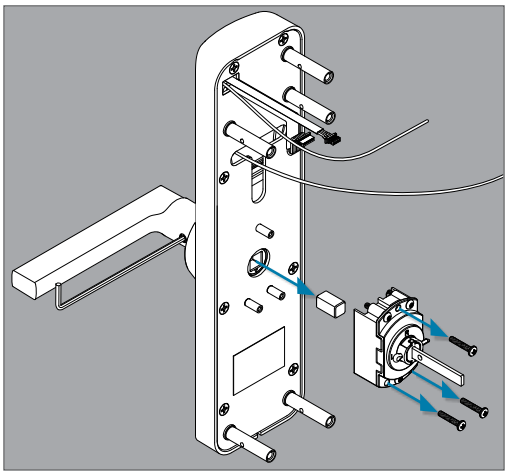
Lock Handing

➔ **Note:** Check handing before installation. Handing requires removal of the lock from the door.

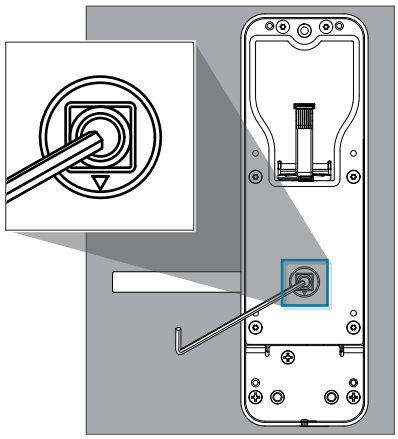
1. Loosen set screw.



2. **Exit:** Remove tailpiece assembly and spindle, as shown.



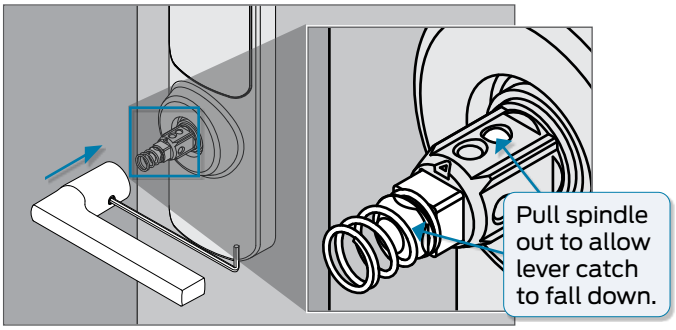
3. Use hex wrench to press center of assembly to release the lever.



4. See **Lever installation** on page **149** to reinstall levers.

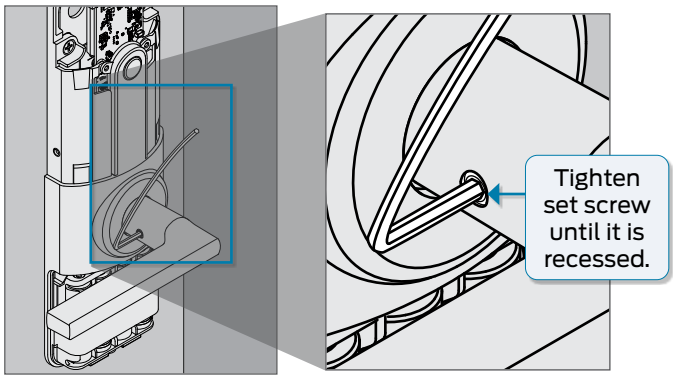
Lever installation

1. When installing levers, make sure to pull the spindle out first, to release the lever catch. This will allow the lever to fully seat onto the spindle.



2. Tighten the set screw, using the long end of the hex wrench, until is recessed below the surface of the lever.

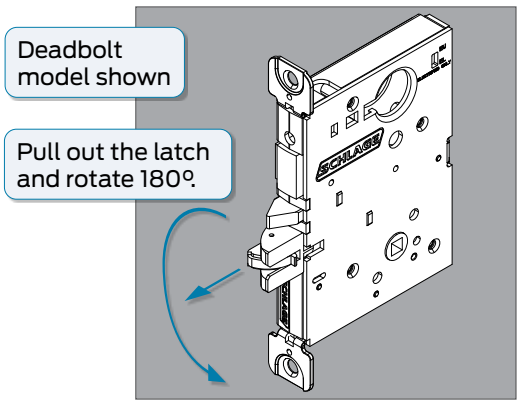
⚠ CAUTION: Do not over-tighten the set screw. This will permanently damage the set screw and prevent tightening. Repeated lever removal may lead to failure of the set screw.



Mortise notes

There is no handing screw on the mortise case. To rehand, simply pull the latch out and rotate.

➔ **Note:** Check handing before installation.



The ENGAGE Mobile Application Advanced settings may be used to “Block” Construction Mode after commissioning.

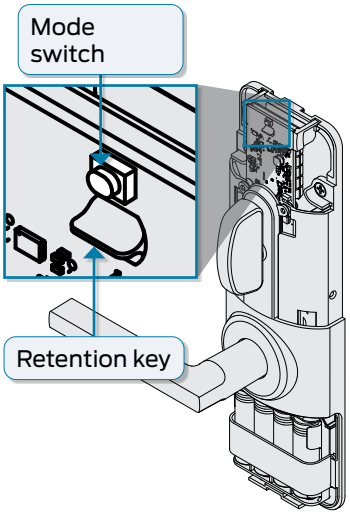
When “Blocked”, Construction Mode cannot be entered again after FDR. The Master Credential enrollment is denied. To enable Construction Mode again, use the ENGAGE Mobile Application Advanced menu to “Unblock” the Construction Mode setting and SAVE. An FDR is required to begin again.

Factory Default Reset Overview

Factory default reset (FDR)

Factory Default Reset (FDR) will return the device to the original, factory settings. Factory Default Reset (FDR) can be entered from any mode. The FDR event removes configurations, user and schedule databases, and requires the lock to re-commissioned. The FDR event does not remove a device from the MAPP site.

➔ **Note:** If there is a timeout or a failure during this process, 2 (two) red lights will light and 2 beeps will sound.



Steps	Lights		Beeps
	Interior	Exterior	
1. Remove the electronic cover.	—		—
2. Press and hold the mode switch for five (5) seconds.	2 green		2
3. Rotate and release the interior lever or depress exit device three (3) times within 20 seconds of FDR requence.	1 red for each turn		1 for each turn
4. FDR in process.	solid red		-
5. FDR completes.	1 green		1
6. Replace the electronic cover.	—		—

Lock Modes

Normal mode

The open architecture design of the XE360 allows it to be managed by an access control system, or be integrated into popular physical access control and Proptech systems through our PACS Alliance program. This enables customers to choose what best fits their requirements now and transition to another solution at any time.

Multi-family construction mode

When in multi-family construction mode, the lock may be unlocked by presenting any credential with the same 48X-type and facility code.

Steps	Lights		Beeps	Action
	Interior	Exterior		
1. While the lock is in **Factory default reset (FDR) (pg 150)**, present a 48X-type credential wth a valid facility code, to the lock.	5 green		1	Lock unlocked.
2. The lock will now operate in multi-family construction mode. Present anyh 48X-type credential with the same facility code as above to operate the lock.				

Commercial construction mode

When in commercial construction mode, the lock may be unlocked by presenting a registered credential.

Steps	Lights		Beeps	Action
	Interior	Exterior		
1. Register a master credential. ➔ **Note:** While the lock is in **Factory default reset (FDR) (pg 150)**, press and hold the mode/REX switch and present a card within five (5) seconds.	5 green		1	Master credential registration successful.
2. Present the master credentail.	solid green		1	
3. Within 20 seconds, present another credential to add as a user credential.	5 green		1	User credential registration successful.
4. Present user credential to operate the lock.				

Review the **Wi-Fi Network Requirements** before you begin.

Commissioning the Device

Commissioning a device enrolls the device into ENGAGE, defines the device name, and prepares the device for later setup steps.

WARNING:
Any setting changes or updates made to an installed and previously commissioned device will require Sync or Over-night call-in updates.

- Administrators should define all **Schedules** and all **Device Defaults** before commissioning locking devices.
- All default Device Settings and defined Schedules are initially programmed into each locking device when it is commissioned.
- If a device setting or schedule is added or updated, a **Synchronization** is required for every device that is affected or was previously commissioned before an update was performed.

The iOS and Android devices have slightly different screens however the functions are the same.

1. Install the batteries.
2. While near the device to be commissioned, **Log In** to the mobile application.
3. The Devices menu will appear.

➔ **Note:** The menu may be blank if no other devices have been commissioned, or previously commissioned devices may be displayed.

4. Tap the + sign.
   - iOS Mobile device: + sign in the upper right-hand corner.
   - Android Mobile device: + sign in the lower right-hand corner.
5. Select XE360.

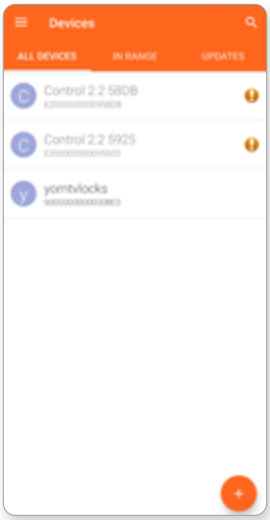


Fig. 15.1: Android Device Menu

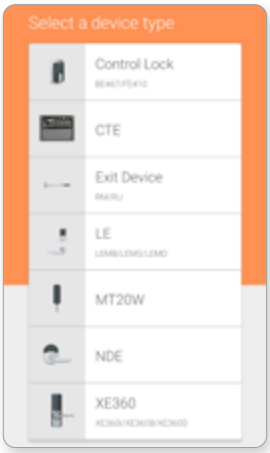


Fig. 15.2: Device Type

Administrators may modify individual device settings at any time, using the Customize Settings option also provided.

6. The next screen displays:
   - Only once per property
   - Only once for each Administrator
   - Only once for each product type

➔ **Note:** This is the ONLY reminder to think about and use the predefined **Property-Wide Settings** before setting up several devices. Administrators can use the currently defined default ENGAGE settings for this device or elect to modify the Property Wide settings now.

7. Select Use Default Settings.

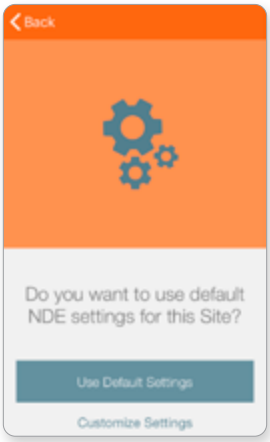


Fig. 15.3: Use Default Settings

The mode switch is located unter the interior cover, as shown in the image on the MAPP.

8. Turn and release the XE360 inside lever, or press the mode switch for exits. This will cause the lock to advertise its presence with its Bluetooth (BLE) radio.
9. Select Next.

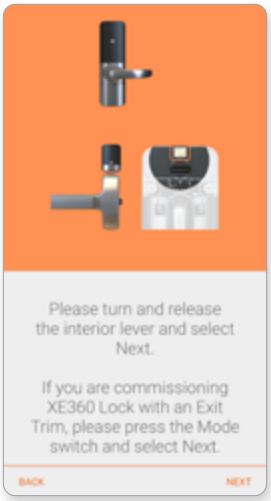


Fig. 15.4: Advertise Presence

When no device information is displayed, ensure the following:

- The battery cover is properly installed. The device cannot “advertise” when the battery cover is not fully installed.
- The lock is Out-Of-The-Box or has recently been Factory Default Reset.
- The Mobile device has Bluetooth turned ON.
- The Mobile device is within Bluetooth communication (BLE) range (<10 ft).

Select Back, to try again.

10. Select the XE360 device to be commissioned.
    - Only devices with a recent inside lever turn will be displayed.
    - The device advertises for 2 minutes to allow selection in this step.
    - When the lock appears in this screen, the number is the serial number.

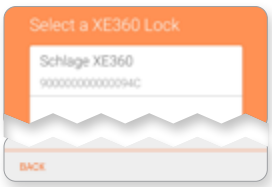


Fig. 15.5: Select the XE360 Device

11. Select Yes, after verifying the device LED is blinking.

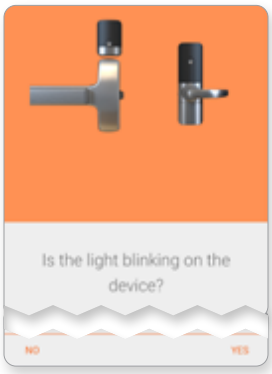


Fig. 15.6: Light Blinking

Typically, the device name would be the device’s physical location.

12. Provide a descriptive name under Device Name.
13. Select Next.

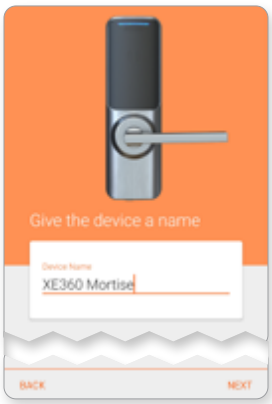


Fig. 15.7: Name Device

14. Select the lock function desired at this opening.

    ➔ **Note:** Notice, when a lock function is selected, a description function is provided.

15. Select NEXT.

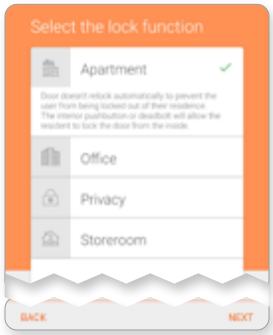


Fig. 15.8: Select the lock function

16. Select Finish or, Select Add another XE360 device.

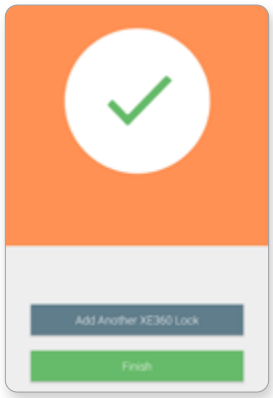


Fig. 15.9: Commissioning Complete

17. The Schlage NDE lock is shown in the devices screen with its new descriptive name.

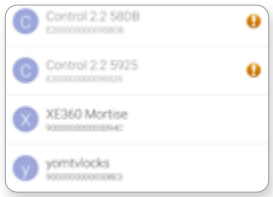


Fig. 15.10: New Lock Displayed

LE and LEB Devices Installation and Commissioning

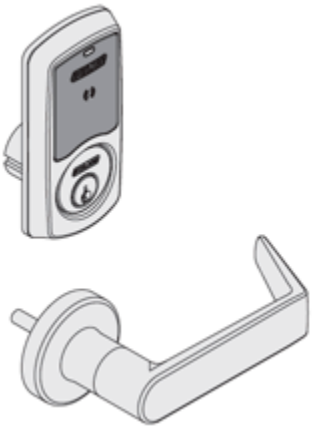
The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

The installation instructions outlined here are excerpts from the Installation Instructions found in the box and highlight the most common issues encountered when installing the device.

Introduction

Before installing the device, review the Installation Instructions for the Schlage LE or LEB lock contained in the box: https://commercial.schlage.com/en/products/electronic-locks/le-mobile-enabled-wireless-mortise-locks.html.

BEST PRACTICE: Before installing, record the serial number and the intended location. This information is required for the Administrator to commission the device and entry into the ENGAGE account.



Sectional Trim

Escutcheon Trim

Fig. 16.1: LE Wireless Mortise Lock

There are no installation differences for the LE and LEB locks.

An LE may be updated to an LEB with replacement components, however, no additional door preparation is required.

Tools Needed:

Phillips screwdriver (#1, #2)

pin wrench

needle-nose pliers

tape measure

Prepare for installation

1. Verify the door is properly prepared before installation
   - Verify the **Door thickness**, the **Mortise pocket size**, and **mounting hole locations** specified in the installation instruction. The mortise pocket is slightly deeper due to additional wire clearance requirements for the Request to Exit (RTE) switch wire routing
   - It is **RECOMMENDED** you dry fit the chassis into the mortise pocket to verify final fit and adequate wire clearance.
   - External wiring for the Request-To-Exit (RTE) switch requires the mortise pocket to be slightly deeper (3/8") into the door than other standard door preparations.

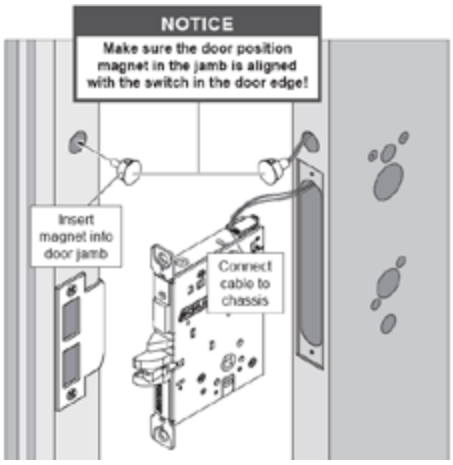


Fig. 16.2: LE/LEB external DPS with Deadbolt

2. The LE and LEB Wireless Mortise Locks are normally provided with an internal Door Position Switch (DPS). However, when these devices are ordered with a deadbolt there is no room for the DPS. LE products with a deadbolt will require additional DPS door preparation needs.
   - Carefully connect the DPS sensor to the chassis as shown.
   - Pay special attention to the small connector while inserting.
   - LE and LEB without a deadbolt will have the DPS integrated into the chassis and will not require the external DPS door prep or wire routing

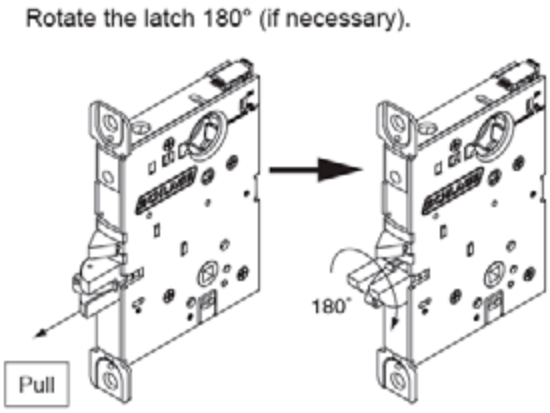


Fig. 16.3: Latch Direction

For best results, ensure the following:

- Verify the chassis can be dry fit into the mortise pocket before final installation, without damaging external wiring.
- The Request-To-Exit (RTE), Door Position Sensor (DPS) and other wiring should be verified.
- Ensure the latch is in the correct direction with the latch bevel towards the door opening.

WARNING: DO NOT USE A POWER DRILL for installation. Power tools may damage the product.

- The Spring Cage Arrow direction is mounted properly with the arrows pointing in the lever down direction.

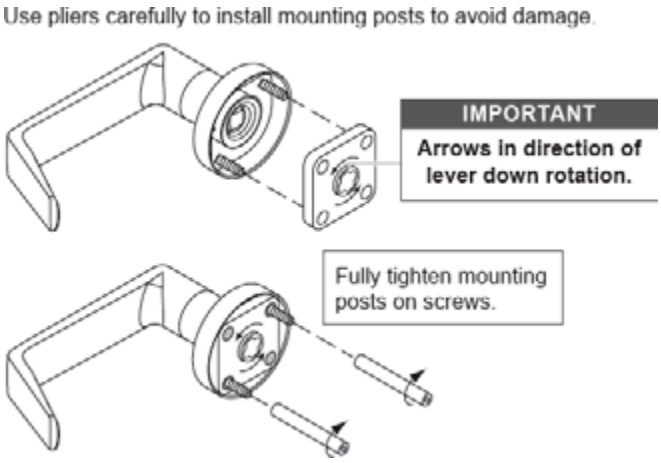


Fig. 16.4: Spring Cage Arrow Direction

- The RX module switch and Handing Screw is on the SECURE side of the mortise chassis (inside).

WARNING: If you are changing the handing direction, be VERY careful not to damage the RX microswitch during the handing process.

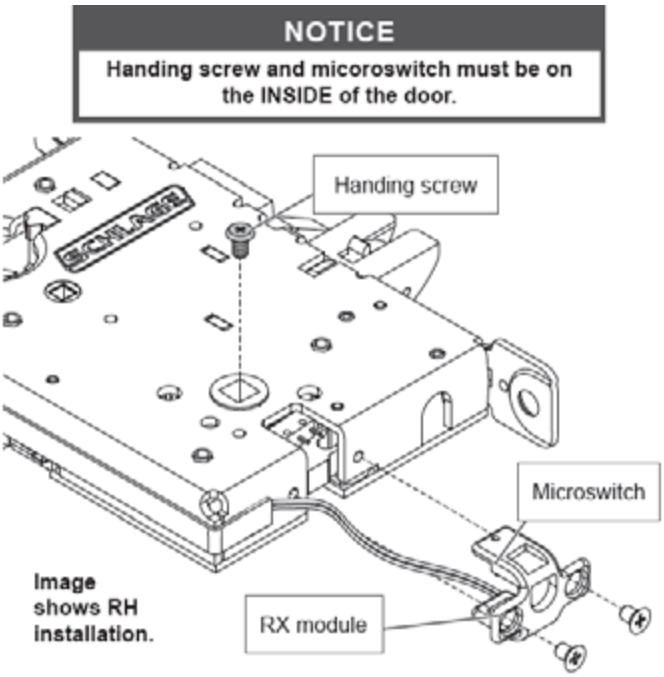


Fig. 16.5: Handing Screw & Microswitch

Verify Success of Installation

Once the lock is properly installed:

- The inside lever moves the latch in and out of the door and frame smoothly and without resistance.
- If the lock is a deadbolt version the thumb turn, and deadbolt also move in and out of the door and frame smoothly without restriction.
- The door closes properly, and the lever handing is correctly installed.
- Upon power-up, the lock performs a Power-On-Self-Test (POST).
  - A few seconds after power is applied, the lock indicates successful POST with 5 GREEN flashes and beeps indicating it is ready for Commissioning or Construction Access Mode operation.

Factory Default Reset

A Factory Default Reset (FDR) will return the LE/LEB to its original settings as shipped from the factory. Additionally, the following will occur.

- Causes the device to beep once when the inside lever is turned.
- Removes any non-default device settings, deletes any construction or user credentials
- Does NOT have any effect on the firmware currently on the lock.
- Does NOT remove the LE or LEB from your ENGAGE account.
- May allow construction mode to be entered again.

➔ **Note:** Construction Mode may be blocked in the default site settings. See **Device Defaults** on page **77** for more information.

Perform an FDR

1. Remove the LE or LEB battery cover.
2. Press and HOLD the FDR button for 5 seconds.
   a. The lock beeps and blinks 2 times.
3. Turn the inside lever **3 times within 20 seconds**.
   a. The lock blinks **RED** and beeps on each lever turn; then provides 2 **GREEN** flashes and beeps to indicate success.

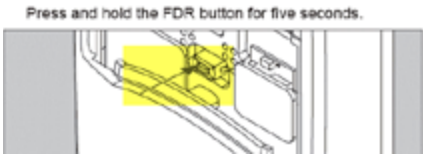


Fig. 16.6: FDR Button

Verify Success of the FDR

1. Turn the inside lever; it will beep once to indicate success.
   - The lock now “advertises” via Bluetooth communication and can be seen in the Select a LE screen as available for commissioning in the **Mobile Application**.

➔ **Note:** Bluetooth (BLE) communication requires the lock battery cover to be properly installed. A loose battery cover may not allow the lock to “Advertise” when connecting.

Construction Access Mode

The Construction Access Mode provides temporary access prior to commissioning the device. Construction mode is a temporary mode of operation used before the ENGAGE account is setup and temporary access is desired.

LE and LEB Wireless Mortise locks Construction Access Mode requires the Administrator to enroll a credential as the Master Construction credential, then use that credential to add additional User Access credentials that can be used for access.

There is only one Master Construction credential so keep it safe, however any number of Access Construction credentials can be added.

➔ **Note:** Construction Mode may be blocked in the default site settings. See **Device Defaults** on page **77** for more information.

- The Construction Access Mode is enabled by default out of the box.
- Construction Mode is a temporary mode of operation and is NOT required to operate lock.
- The lock will remain in Construction Access Mode until the mode is cancelled via FDR or Commissioning of the device.
- No audits are captured while the device is in Construction Access Mode.

➔ **Note:** Construction Mode may be blocked in the default site settings. See **Device Defaults** on page **77** for more information.

Master Programming Credential:

- The Master Programming Credential is used to add additional Construction Access credentials to each installed lock.
- The Master Programming Credential will not grant access.
- The Master Construction credential is ONLY used to add additional User Construction credentials.
- Best Practice; Use the same Master Programming Credential for all the locks in the facility.
- If the Master Construction Credential is lost or destroyed, no additional construction credentials can be added to the lock.

Remove Construction Credentials:

- The only way to remove Construction Access Credentials from a lock is to perform a factory default reset (FDR) on the lock or commissioning.
- After an FDR or commissioning, all previously valid Construction Credentials are no longer valid.
- To enter the Construction Access Mode again, a new Master programming Credential must be created, and additional user access credentials will need to be enrolled.

Create a Master Construction Credential

Start with a new LE or LEB new, out of the box or after a Factory Default Reset with the “Block Construction Mode” ENGAGE Mobile Application setting not selected.

1. Turn and HOLD the inside lever Request-to-Exit (RTE) and present a new credential to become the property Master Construction Credential.
2. The lock acknowledges the credential presentation with 5 GREEN flashes and enrolls the credential as the Master Construction Credential.
3. Present the newly added Master Construction Credential to the LE or LEB lock.
4. The lock LED lights GREEN for 20 seconds waiting for another credential to be presented for enrollment as a Construction Access Credential.

➔ **Note:** The next credential presented will be enrolled as a Construction User Access Credential. Construction User Access Credentials allow NORMAL (momentary) access when presented

Create Construction User Access Credentials

To enroll construction credentials that allow User access.

1. Present the previously enrolled Master Construction Credential.
2. While the lock LED is solid GREEN, present the credential intended to become a Construction User Access Credential.
   - The lock beeps after successfully enrolling the presented credential.
3. Repeat the Master Construction Credential presentation followed by a new Construction Access Credential for each Construction Access Credential that is needed.
4. Present the newly added Construction Access Credential(s).
5. Verify momentary access is granted.

Review the **Wi-Fi Network Requirements** before you begin.

Commissioning

Commissioning enrolls the device into ENGAGE, defines the device name, and prepares the device for later setup steps.

WARNING: Any setting changes or updates made to an installed and previously commissioned device will require Sync or Over-night call-in updates.

- All **Device Defaults** and defined **Schedules** are initially programmed into each locking device when it is commissioned.

1. Install the batteries in the LE or LEB Lock.
2. While near the device to be commissioned, login to the ENGAGE Mobile Application.
3. The initial blank Devices Screen will appear. Depending on your Mobile device (Android or iOS), one of the following screens is presented.

➔ **Note:** When devices have been commissioned, this screen will display the name of the commissioned devices.

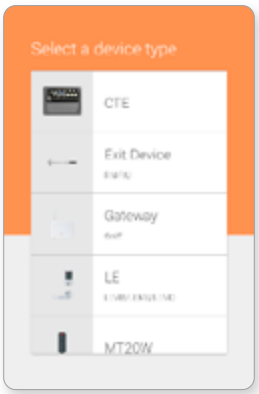


Fig. 16.7: Device Type

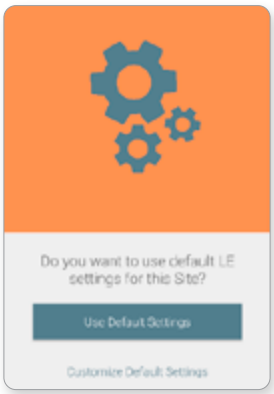


Fig. 16.8: Site Settings

- iOS Mobile device: + sign in the upper right-hand corner.
- Android Mobile device: + sign in the lower right-hand corner.

4. Select the + sign to select the nearby LE or LEB lock being commissioned,
5. Select the LE device type for commissioning.
6. Select Use Default Settings to continue.

➔ **Note:** This is the ONLY reminder to think about and use the predefined **Property-Wide Settings** before setting up several devices. Administrators can use the currently defined default ENGAGE settings for this device or elect to modify the Property Wide settings now.

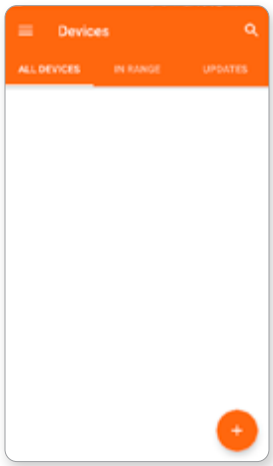


Fig. 16.9: Android Device Menu

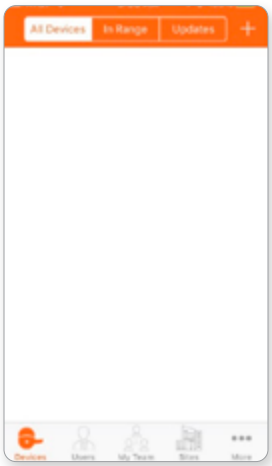


Fig. 16.10: iOS Device Menu

7. Turn and release the inside LE lever to cause the lock to “advertise” its presence with its Bluetooth (BLE) radio.
8. **Select Next**.

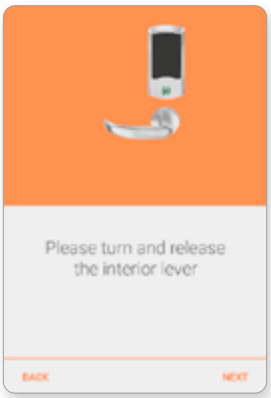


Fig. 16.11: Advertise Presence

If no device information is displayed, ensure the following:

- The battery cover is properly installed. The Schlage LE/ LEB does not “advertise” when the battery cover is not installed properly.
- The LE/LEB is Out-Of-The-Box or recently had a Factory Default Reset.
- The Mobile device has Bluetooth turned ON.
- The Mobile device is in Bluetooth communication (BLE) range of the Schlage LE/LEB (<10ft).

Select Back to try again.

9. **Select** the **LE device** to be commissioned.

   ➔ **Note:** Only devices with a recent inside lever turn will be displayed. The device “advertises” for 2 minutes to allow selection in this step. In this screen, the number shown is the device serial number.

Fig. 16.12: Select LE Device

10. After the lock has been selected
    - The Mobile Device will connect to the lock
    - And ask to verify that the actual lock being commissioned is blinking it’s LED RED.
11. **Select Yes** After verifying the LED is blinking.

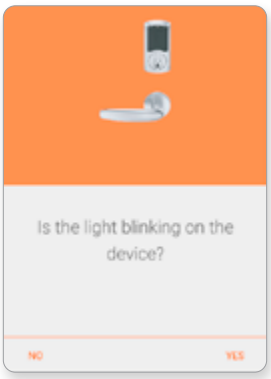


Fig. 16.13: Light Blinking

12. Enter a descriptive name for your device under Device Name.
    - **Storage** is used here

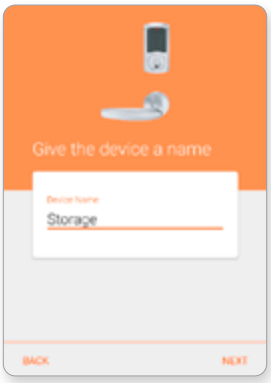


Fig. 16.14: Name Device

13. Select the lock function.
    - See **Lock Function Definitions** on page **7** for more information.
14. Select Next.

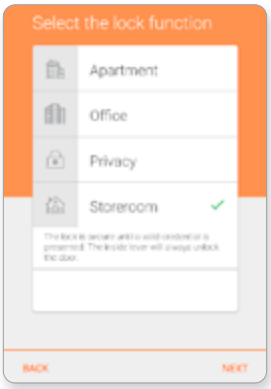


Fig. 16.15: Lock Function

WARNING: The Apartment, Office, and Privacy lock functions require the Inside Push Button (IPB) or deadbolt thumbturn to be available for proper operation.

Only select a SAVED network if the network is available at the physical door location.

15. Enable the Wi-Fi network connection capabilities of the LE/LEB device.
    - To enable or edit a Wi-Fi network later OR if the Wi-Fi is not available or needed, select Skip.
    - Android Devices: To enable a Wi-Fi network now, select the desired Wi-Fi from the currently available networks and follow the prompts.
    - iOS Devices: To add a new network now, select Add a new network and follow the prompts.

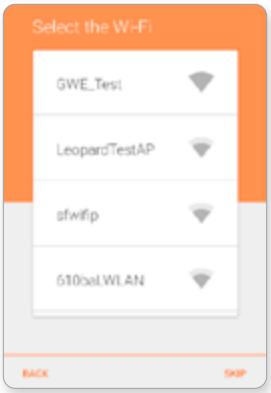


Fig. 16.16: Android Wi-Fi Screen

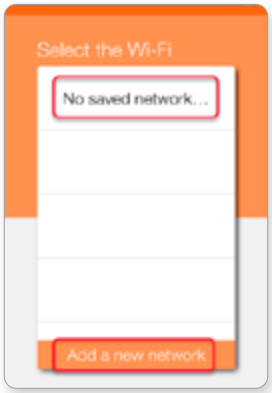


Fig. 16.17: iPhone Wi-Fi Screen

➔ **Note:** The Property Administrator may enable or edit a Wi-Fi network connection setting at any time using the ENGAGE Mobile application. See **Device Wi-Fi Network Setup** for setup requirements when a Wi-Fi network is available, and the Administrator wants to take advantage of the Nightly Call-In feature.

16. Your device is being prepared.

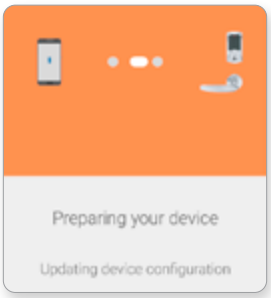


Fig. 16.18: Device Configuration

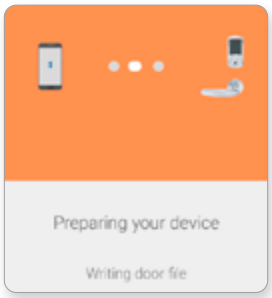


Fig. 16.19: Writing Door File

17. Select:
    - Finish to complete the commission process.
    - Add Another LE Device to continue enrolling LE or LEB locks.
18. When Finish is selected, the newly commissioned device is shown in the ENGAGE Mobile Application Devices screen with its new name.

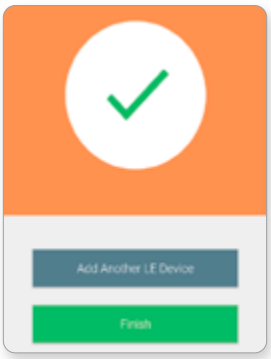


Fig. 16.20: Finish or Add Another

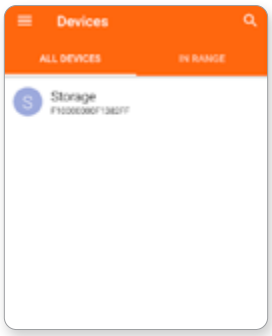


Fig. 16.21: Newly commissioned device

NDE80 and NDEB Devices Installation and Commissioning

The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

Introduction

Before installing the device, review the Installation Instructions for the Schlage NDE80 and NDEB lock contained within their respective boxes.

➔ **Note:** NDE80 and NDEB locks have very similar installation requirements. NDEB locks will include a standard magnetic DPS switch and will require additional installation door preparation. NDE80 locks can be upgraded to NDEB with an upgrade kit

NDE Standalone Wireless: https://commercial.schlage.com/en/products/electronic-locks/nde-mobile-enabled-wireless-cylindrical-locks.html

NDE Networked Wireless: https://commercial.schlage.com/en/products/electronic-locks/nde-mobile-enabled-wireless-cylindrical-locks.html

Tools Needed: Phillips screwdriver, pin wrench, tape measure

T-15 Torx screwdriver (optional).

Prepare to Install the NDE80 or NDEB Wireless Locks

Before installing, record the serial number and the intended (or installed) location. This information is required for the Administrator to commission the device and entry into the ENGAGE account.

WARNING: DO NOT USE A POWER DRILL for installation. Power tools may damage the product.

1. Verify the door is properly prepared for the Schlage NDE80 or NDEB installation before attempting to install.
   - The Schlage NDE80/NDEB and the mechanical ND locks use the SAME basic door preparation template, which comes in the box with the product.
   - Mechanical cylindrical lock (ND) updates to NDE80 or NDEB are easily performed.
   - Schlage NDEB locks will have additional DPS installation door preparation requirements compared to mechanical ND and NDE80 locks.
2. Verify these **critical items** before attempting to install the Schlage NDE80 or NDEB.
   - Through door bore backset = 2 or 2 inches
   - Through door bore diameter = 2 inches
   - The two 5/16 inch through door bolt holes are properly located
   - Latch Bore hole diameter = 1.0 inch and the hole is centered in the door
   - Latch bore hole centerline and the Door bore hole centerline is in alignment.
   - For NDEB only:
     - The additional DPS door edge and frame hole locations are made based on the door material (wood/metal)
   - The DPS wire routing hole on the face of the door is on the **interior of the door**
   - The DPS wire routing hole is ONLY halfway through the door

WARNING: The Centerline of the Latch Bore Hole and the Centerline of the though Door Bore MUST be accurate for proper latch retraction.

Install the Device

1. Install the NDE or NDEB as indicated in the Installation Instructions.

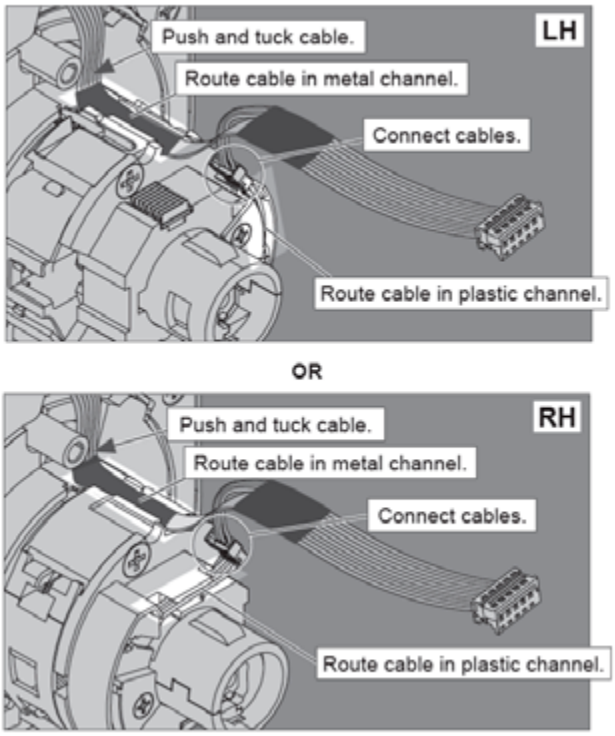
WARNING: Ensure cable is routed with no pinching and with both cable connections properly seated in the proper channels.

CAUTION: Ensure the installed latch and chassis are properly aligned and fully engaged.

WARNING: For non-standard door thickness, carefully follow the door thickness adjustment steps outlined in the Door Thickness Adjustment section.

1c Connect chassis cable. Route cables.

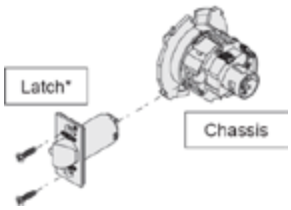
The cable should be routed on top of the chassis! Connect cable from outside assembly to connector in chassis.



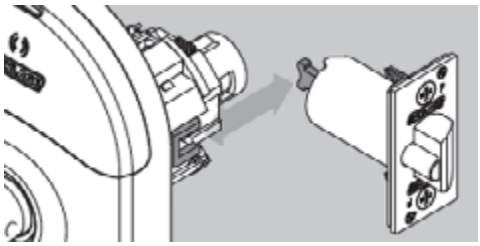
Tuck connected chassis cable into appropriate channel.

Fig. 17.1: Connect Chassis Cables

2. Insert the chassis into the installed latch.



3. Check the Latch prongs and the Retractor Slide engagements are properly connected.



4. Align latch prongs and chassis slide.

WARNING: The latch prongs MUST fully engage the top and bottom chassis slides. The installed latch MUST be centered in the chassis and door.

NDE80 ONLY: Install the Magnet and Strike

Depending on the door frame requirements, ANSI and T-Strike DPS sensor options are available.

Install the provided standard DPS magnet or install the magnet tray along with the appropriate strike.

➔ **Note:** ANSI Strikes with the Magnetic Tray are recommended. T-Strikes with a separate magnet is provided as an alternate. When the T-Strike and standard door position magnet are used, additional door prep is required to install the magnet into the frame.

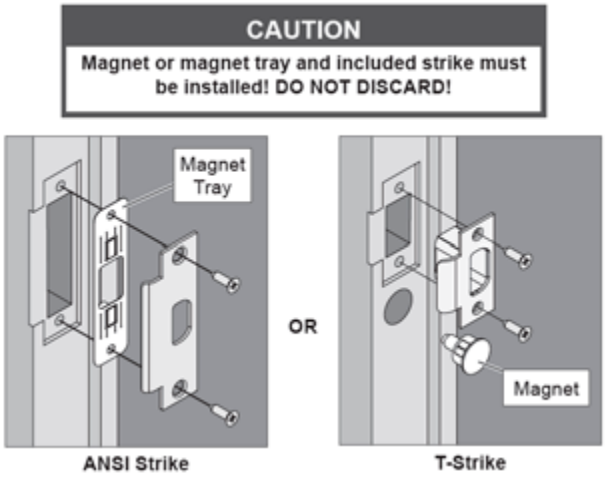


Fig. 17.2: NDE80 Magnet and Strike options

WARNING: The Door Position Sensor magnet tray or T-Strike magnet MUST be installed for proper Door Position sensing and proper calibration during commissioning

Install the DPS sensor NDEB ONLY

When working with NDEB Wireless Locks, a separate DPS magnet and standard wiring through the door to the NDEB circuit board is required.

WARNING: The Door Position Sensor magnet MUST be installed properly. Pay attention when connecting (or removing) the cable the DPS cable connector. This connector is very small and can be easily damaged. Ensure the DPS wires will not be pinched when the battery holder and battery cover are fully installed

With the DPS door drill preparation accomplished and the NDEB inside escutcheon properly installed, the DPS may be fully installed.

- Feed the wires through the interconnected drill holes to bring the wires to the interior side of the door
- Fully seat the DPS magnet into the door edge
- Route the wires under tabs as shown below (2), ensuring that any excess wires are tucked into the door (3) and out of harms' way.
- Securely attach DPS connector (1) to the NDEB printed circuit board.

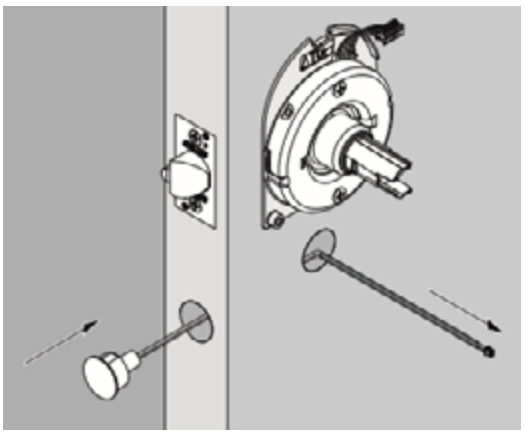


Fig. 17.3: NDEB DPS Sensor

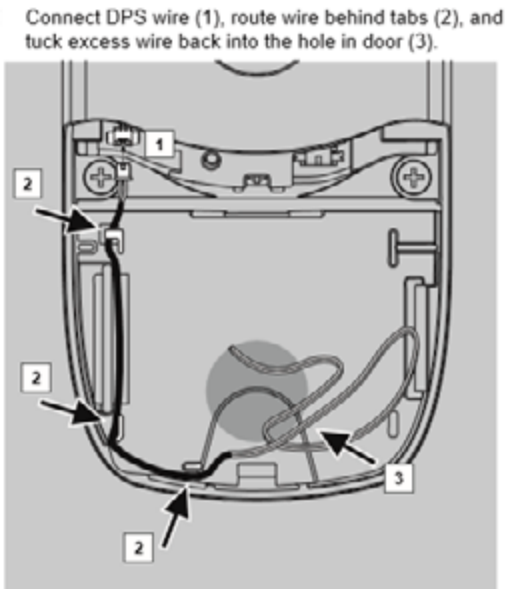


Fig. 17.4: NDEB DPS wire routing

The ENGAGE Mobile Application Advanced settings may be used to "Block" Construction Mode after commissioning.

When "Blocked", Construction Mode cannot be entered again after FDR. The Master Credential enrollment is denied. To enable Construction Mode again, use the ENGAGE Mobile Application Advanced menu to "Unblock" the Construction Mode setting and SAVE. An FDR is required to begin again.

Factory Default Reset Overview

A Factory Default Reset (FDR) will return the NDE80 or NDEB to its original settings as shipped from the factory. Additionally, the following will occur.

- The device to beep once when the inside lever is turned.
- Removes any non-default device settings, deletes any construction access credentials.
- Does NOT have any effect on the firmware currently on the lock.
- Does NOT remove the NDE80 or NDEB from your ENGAGE account.
- May allow construction mode to be entered again.

Perform an FDR

1. Remove the NDE80 or NDEB battery cover.
2. Press and HOLD the FDR button for 5 seconds. The lock beeps and blinks 2 times.
3. Turn the inside lever 3 times within 20 seconds.
   a. The lock blinks RED and beeps on each lever turn; then provides 2 GREEN flashes and beeps to indicate success.

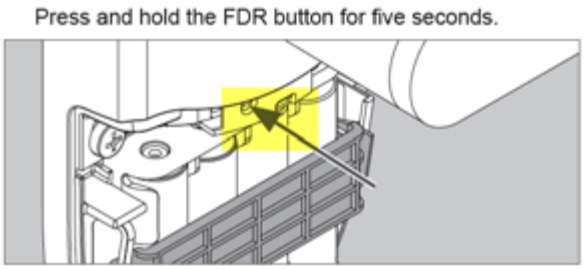


Fig. 17.5: NDE80 or NDEB FDR Button

Verify Success of the FDR

4. Turn the inside lever; it will beep once to indicate success.
   a. The lock now "advertises" via Bluetooth communication and can be seen in the Select an NDE/NDEB screen as available for commissioning in the ENGAGE Mobile application.
   b. When "Block Construction Mode" has been disabled, prior to the FDR, a new Master Construction Credential can now be created.

➔ **Note:** Bluetooth (BLE) communication requires the lock battery cover to be properly installed. A loose battery cover may not allow the lock to "Advertise" when connecting.

Construction Access Mode Overview

Construction Access Mode provides temporary access prior to commissioning the device and requires an electronic credential (see the Master Programming Credential section below).

Construction Access Mode: The Construction Access Mode is enabled by default and may be after a Factory Default Reset (FDR).

- Construction Mode is a temporary mode and is NOT required to operate lock.
- The lock will remain in Construction Access Mode until the mode is cancelled.
- No audits are captured while the lock is in Construction Access Mode.
- To exit Construction Access requires commissioning with the ENGAGE Mobile application or Factory Default Reset (FDR)

Master Programming Credential: The Master Programming Credential is used to add additional Construction Access credentials to each installed lock.

- The Master Programming Credential will not grant access.
- Master Programming Credential is ONLY used to add additional Construction Access credentials.
- Administrators will use the same Master Programming Credential for all the locks in the facility.
- If the Master Construction Credential is lost or destroyed, no additional Construction Access credentials can be added to the lock

Remove Credentials: To remove credentials from the Construction Access Mode, perform a Factory Default Reset (FDR) on the lock.

- After an FDR, all previously valid Construction Credentials are no longer valid.

Create a Master Construction Credential

Start with a new NDE80 or NDEB, out of the box or after a Factory Default Reset with the "Block Construction Mode" ENGAGE Mobile Application setting not selected.

1. Turn and HOLD the inside lever Request-to-Exit (RTE) and present a new credential to become the property Master Construction Credential.
2. The lock acknowledges the credential presentation with five (5) GREEN LED flashes and enrolls the credential as the Master Construction Credential.

➔ **Note:** If the lock does not accept the Master Construction credential enrollment and provides two (2) **RED** LED flashes. Construction Mode has been Disabled. Use a Mobile Device to connect to the device and **Disabl**e the "Block Construction Mode". Then perform a new FDR to try again.

Verify Success of the Master Construction Credential

1. Present the newly added Master Construction Credential to the NDE80 or NDEB Wireless lock.
2. The Schlage NDE or NDEB LED lights GREEN for 20 seconds waiting for another credential to be presented for enrollment as a Construction Access Credential.

➔ **Note:** The next credential presented is enrolled as a Construction Access Credential and is allowed momentary access to the lock when presented again.

Create Construction Access Credentials

1. To enroll construction credentials that allow access, present the previously enrolled Master Construction Credential.
2. While the lock LED is solid GREEN, present the credential intended to become a Construction Access Credential.
3. The lock beeps after successfully enrolling the presented credential.
4. Repeat the Master Credential presentation followed by a new Construction Access Credential for each Construction Access Credential that is needed.
5. Present the newly added Construction Access Credential(s).
6. Verify momentary access is granted.

Review the **Wi-Fi Network Requirements** before you begin.

Commissioning the Device

Commissioning a device enrolls the device into ENGAGE, defines the device name, and prepares the device for later setup steps.

WARNING: Any setting changes or updates made to an installed and previously commissioned device will require Sync or Over-night call-in updates.

- Administrators should define all **Schedules** and all **Device Defaults** before commissioning locking devices.
- All default Device Settings and defined Schedules are initially programmed into each locking device when it is commissioned.
- If a device setting or schedule is added or updated, a **Synchronization** is required for every device that is affected or was previously commissioned before an update was performed.

1. Install the batteries in the NDE80/NDEB device.
2. While near the device to be commissioned, **Log In** to the mobile application.
3. The blank Devices menu will appear.

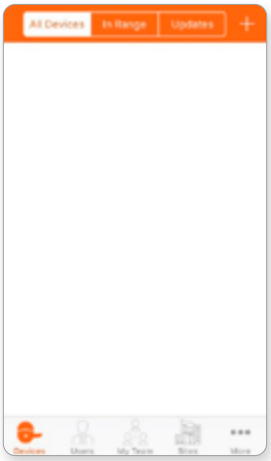


Fig. 17.6: iOS Device Menu

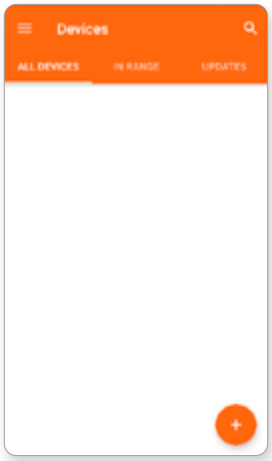


Fig. 17.7: Android Device Menu

The iOS and Android devices have slightly different screens however the functions are the same.

4. To Select the nearby NDE/NDEB device being commissioned, tap the + sign.
   - iOS Mobile device: + sign in the upper right-hand corner.
   - Android Mobile device: + sign in the lower right-hand corner.
5. Select NDE.

➔ **Note:** Select the NDE device type for commissioning either NDE80 or NDEB device types.

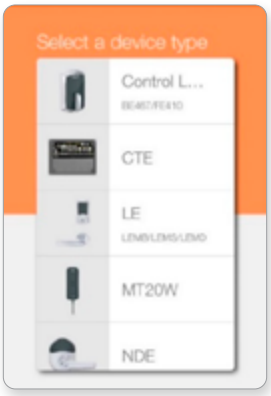


Fig. 17.8: Device Type

Administrators may modify individual device settings at any time, using the Customize Settings option also provided.

6. The next screen displays:
   - Only once per property
   - Only once for each Administrator
   - Only once for each product type

➔ **Note:** This is the ONLY reminder to think about and use the predefined **Property-Wide Settings** before setting up several devices. Administrators can use the currently defined default ENGAGE settings for this device or elect to modify the Property Wide settings now.

7. Select Use Default Settings.

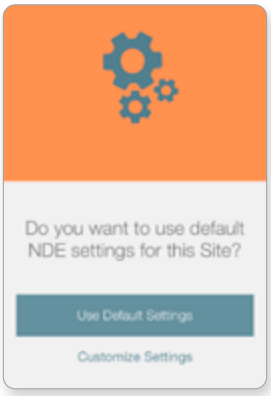


Fig. 17.9: Use Default Settings

8. Turn and release the NDE inside lever. This will cause the lock to “advertise” its presence with its Bluetooth (BLE) radio.
9. Select Next.

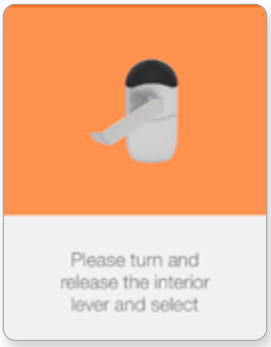


Fig. 17.10: Advertise Presence

10. Select the NDEB device to be commissioned.
    - Either NDE80 or NDEB devices are selectable here.
    - Only devices with a recent inside lever turn will be displayed.
    - The device “advertises” for 2 minutes to allow selection in this step.
    - When the lock appears in this screen, the number is the serial number.
11. Select Yes, after verifying the device LED is blinking.

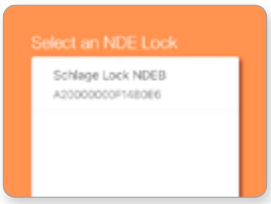


Fig. 17.11: Select the NDEB Device

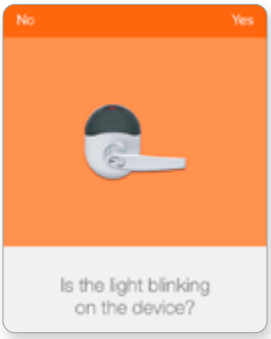


Fig. 17.12: Light Blinking

12. Provide a descriptive name (Main Office) under Device Name.
13. Select Next.

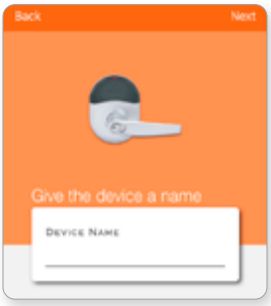


Fig. 17.13: Name Device

When no device information is displayed, ensure the following:

- The battery cover is properly installed. The device cannot “advertise” when the battery cover is not fully installed.
- The lock is Out-Of-The-Box or has recently been Factory Default Reset.
- The Mobile device has Bluetooth turned ON.
- The Mobile device is within Bluetooth communication (BLE) range (<10 ft).

Select Back, to try again.

14. Select the lock function desired at this opening.

    ➔ **Note:** Notice, when a lock function is selected, a description function is provided. NDE80 locks are ALWAYS 80 Function (Storeroom) and this menu, Selecting a Lock Function is not presented for NDE80 devices.

15. Select NEXT.

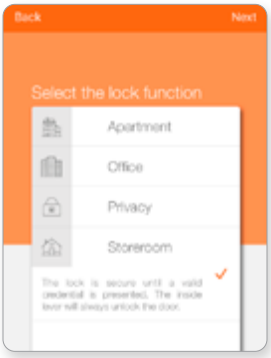


Fig. 17.14: Select the lock function

➔ **Note:** The NEXT step in the commissioning process can enable the Wi-Fi network connection capabilities of the Schlage NDE locks. Administrators may also elect to skip setup of the Wi-Fi network when a network is not available or not needed by selecting Skip. The Administrator may enable or edit a Wi-Fi network connection setting at any time using the Mobile application.

16. Select Skip Let's assume that the propertied local Wi-Fi network has not been set up yet and there are no local Wi-Fi network connections available.

    ➔ **Note:** See **Device Wi-Fi Network Setup** for setup requirements when a Wi-Fi network is available, and the Administrator would like to take advantage of the Schlage NDE "Nightly Call in" feature.

Fig. 17.15: Select the Wi-Fi

17. Select Finish or, Select Add another NDE device.

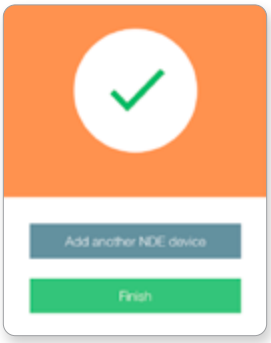


Fig. 17.16: Commissioning Complete

18. The Schlage NDE lock is shown in the ENGAGE Mobile Application Devices screen with its new descriptive name.

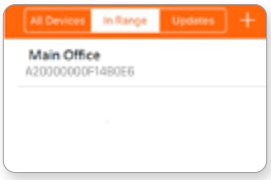


Fig. 17.17: New Lock Displayed

CTE Controller and MTB Readers Installation and Commissioning

The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

Introduction

Before installing the device, review the Installation Instructions for the Schlage CTE contained in the box. Additionally, review all accessory details for the power supply, credential reader, and the installation instructions of the locking device to ensure their interconnection and mounting requirements.

CTE:

https://commercial.schlage.com/en/products/reader-controllers/cte-single-door-controller-with-mtb-reader.html

MTB Mobile Enabled Multi-Technology Readers

https://commercial.schlage.com/en/products/readers.html

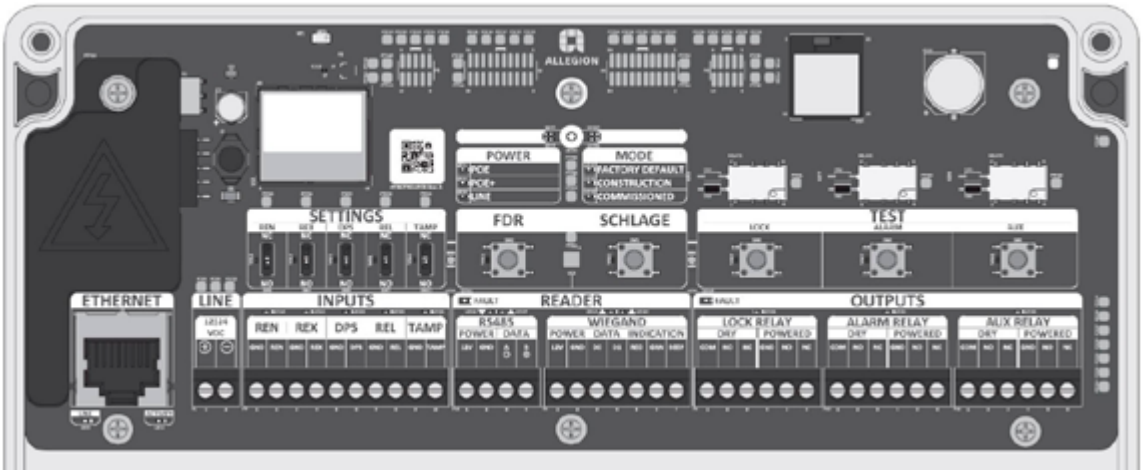


Fig. 18.1: CTE Printed Circuit Board (PCB) Diagram

Prepare to Mount the Device

Before installing, record the serial number and the intended (or installed) location. This information is required for the Administrator to commission the device and entry into the ENGAGE account.

Tools Needed: Phillips screwdriver, the credential reader, and the locking device system. Additional items may be needed depending on the power supply and accessories chosen.

For best results when installing the CTE, review the points below and the installation excerpts from the installation instructions:

- Install the CTE indoors with a temperature range of -35ºC to +66ºC (-31ºF to +151ºF).
- Install in a **secure location** that is not accessible by the public.
- Determine the location and interconnection wiring requirements for each component before installing.
- **Do not mount** the CTE on a metal surface and keep it at least 1 inch away from any metal. Wireless signals can be adversely affected
- Ensure all wiring runs are as short as possible and do not exceed recommended distances, 500 feet with 18 gauge (awg).
- Use **ONLY** stranded and appropriate wire gauge multi-conductor wire.
- Do not use any splices in any wiring connection and ensure good connections are made when using Power Hinges or Electrical Power Transfers (EPT).

- The CTE Lock Relay can be configured to fail safe (fail unlocked) or fail secure (fail locked) by wiring the door hardware to either NO or NC and selecting a failsafe or fail secure locking device.
- For best Wi-Fi network and Bluetooth (BLE) wireless communication, ensure the following:
  - Do not mount the CTE near large metal objects or inside other metal enclosures or cabinets. Wireless signal will not pass through metal walls.
  - Mount the CTE within 10 feet of the door opening.
  - Mount the CTE within communication range of the local Wi-Fi access point.

Mount/Install the Devices

Install the Schlage CTE and all accessories as directed in their respective installation instructions.

WARNING: To avoid damage to the Schlage CTE electronics during installation, use CAUTION when drilling holes for the external wiring exit/entry connector holes. The installer should use light drilling pressure so that the drill bit does not penetrate the enclosure and damages the internal Printed Circuit Board (PCB). If the PCB is to be temporarily removed for drilling connector holes and wiring, use EXTREME CAUTION to ensure the PCB is not damaged and is handled in an electrostatically safe manner.

CTE Installation

The Schlage CTE is provided in an enclosure that allows the installer multiple options when mounting in its permanent location.

The CTE is not plenum rated.

The installer should refer to the CTE Installation Instruction and use best practices to securely mount the enclosure. Generally, four screws into a solid wall are adequate for a secure mount. If the location does not adequately support the CTE, mounting anchors should be used.

The CTE enclosure provides ample room for cable routing in and out of the enclosure. Special attention is needed when drilling additional holes in the enclosure to accommodate the size and number of entry or exit connectors to be used.

Power Supply Installation

When selecting and installing a power supply, refer to that components' own installation instruction.

Use of an existing and available power supply or a Power-Over-Ethernet (POE) supply may eliminate the need for additional power supplies.

CTE does not support wall mounted readers with a keypad (MTKB15). The CTE only supports -485 readers not weigand.

Credential Reader Installation

The CTE supports one door opening and one wall mounted Credential Reader at a time.

The original MT11-485 mullion and MT15-485 single gang readers initially available have been updated to provide Mobile Credential compatibility with MTB11 and MTB15.

Fig. 18.2: Original Readers

Fig. 18.3: Mobile Enabled Readers

The CTE is completely compatible with either the original or new Mobile Enabled Wall Mounted Credential readers.

The electrical connections from the CTE to the Wall Mounted Reader require only power and data line connections. Refer to the credential reader installation instructions when installing.

Table 18.1 Reader Connections

Reader - RS485		**Description**
POWER 12V	Reader power (red wire)	12 VDC power to RS485
POWER GND	Reader power ground (black)	Electrical ground (common) for the CTE
DATA A	RS485 data A (pink)	Data A communication for RS485 reader
DATA B	RS485 data B (tan)	Data B communication for RS485 reader

Credential Reader Connection to CTE

The credential reader must be properly wired for power and communication and Paired (or linked) to the CTE for proper operation.

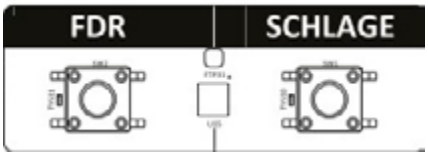


Fig. 18.4: CTE / Reader Connection Switches

- When properly connected and powered up, the attached credential reader will automatically be recognized during the initial Power-On process.
  - If the Credential Reader does not respond to credential presentations and presents a solid **RED** LED, it is not properly wired to the CTE.
- When changing the Credential Reader, the Pairing process may need to be manually repeated.
  - Follow the steps below to pair a Credential Reader with the CTE.
    - Press and release the **Schlage** button 1 time.
    - Press and release the **FDR** button 2 times.
    - The Credential Reader beeps and blinks **AMBER** 3 times to indicate success.

➔ **Note:** The CTE **does not** control the Credential Reader beeper. A Configuration Card (CE-401-133) is required to disable the credential reader beeper

Locking Device Installation

The CTE supports many different types of electronic locking devices. The installer should review the locking device installation instruction for the device they intend to install and follow its installation requirements.

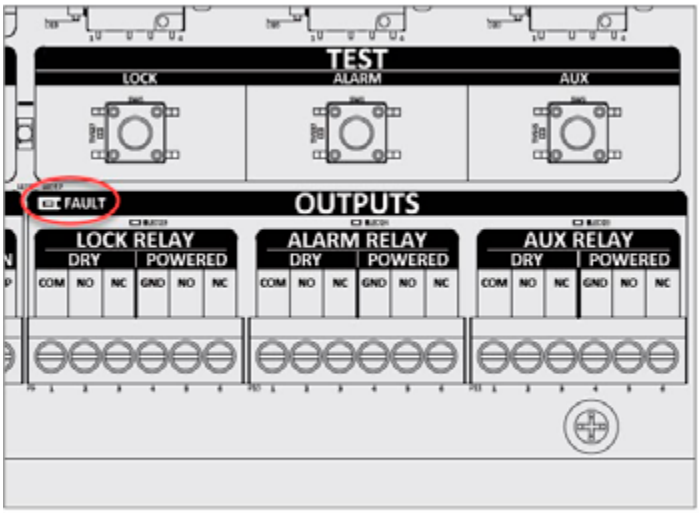
Verify Success of the Installation

Once all components have been installed, test each to ensure a successful installation.

CTE Relay Outputs Test

The CTE has built in options to test its installation quickly.

Each of the three output relays (lock, alarm, and auxiliary) has three DRY outputs and three POWERED outputs that can be manually activated using a push-button on the CTE PCB.



CTE Outputs: LOCK, ALARM, and AUX.
Located below TEST buttons.

Fig. 18.5: CTE TEST Switches

- Press and hold any of the TEST switches to manually test the LOCK RELAY, ALARM RELAY, and AUX RELAY.
  - Both the DRY and the POWERED outputs of the relays are exercised when the TEST buttons are pressed.
- The FAULT LED (circled) illuminates **RED** any time an overcurrent condition is detected at any of the relay outputs.

Factory Default Reset (FDR) Overview

A Factory Default Reset (FDR) will return the CTE to its original settings as shipped from the factory. Additionally, the following will occur.

- Removes any non-default device settings, deletes the Master Construction and User Construction Credentials, and allows construction mode to be entered again.
- Does **NOT** have any effect on the firmware currently on the CTE or the reader.
- Does **NOT** remove the CTE from your ENGAGE account.
- The STATUS LED on the PCB lights **RED** and the Factory Default MODE lights **GREEN**.

Perform an FDR

1. **Remove** the lid.
2. **Press** and **HOLD** the **FDR** button for 5 seconds, then **release**.
   - CTE will beep 2 times and the STATUS LED will blink **GREEN** 2 times at the end of 5 seconds.
3. **Press** the **Schlage** button 3 times; there is one beep for each button press.
   - CTE will beep once and the STATUS LED will light **GREEN**.

Verify Success of the FDR

The CTE STATUS LED will be solid **RED** and the MODE LED for Factory Default will be solid **GREEN**.

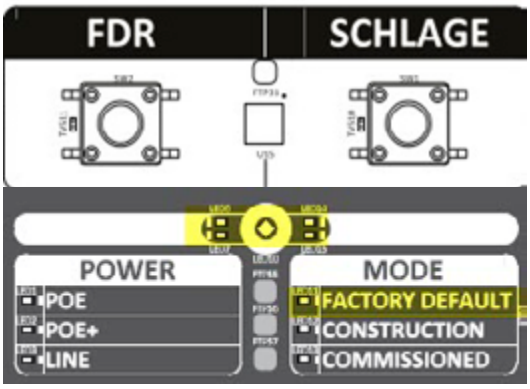


Fig. 18.7: FDR Mode

Construction Mode Overview

The Construction Mode is used to allow access before the CTE controller is commissioned and for testing purposes.

Construction Mode: The Construction Mode is enabled by default and after a Factory Default Reset (FDR).

- Construction Mode provides NORMAL Credential function and the CTE always automatically relocks after momentary access is granted.
- The CTE will remain in Construction Mode until the mode is cancelled by performing an FDR or Commissioning into an ENGAGE account.
- No access audits are captured while the CTE is in Construction Mode.

Master Construction Credential: The Master Construction Credential is used to add additional User Constructions Credentials to each installed CTE.

- The Master Construction Credential will not grant access through a door.
- The Master Construction Credential **must** be programmed before programming construction access mode with user credentials.
- The Master Construction Credential is **ONLY** used to add additional User Construction Credentials.
- Use the same Master Construction Credential for all the controllers in the facility.
- If the Master Construction Credential is lost or destroyed, no additional user construction credentials can be added to the CTE.

Cancel Construction Mode: To cancel the Construction Mode and to remove all credentials, perform a factory default reset (FDR) or commissioning.

- When Construction Mode is cancelled, the Master Construction Credential and all other added User Construction Credentials will no longer function.
- To enter the Construction Access Mode again, a new Master programming Credential must be created, and new User Access Construction credentials will need to be re-enrolled.

Create a Master Construction Credential

The CTE requires a Master Construction Credential that is used to add additional User Access Construction Credentials to each installed CTE.

1. Begin with a new CTE or after a successful FDR.
2. **Remove** lid.
3. **Press** and **hold** the **Schlage button** for 5 seconds;
   - CTE MODE indicator switch for Construction will be illuminated.
4. **Present** a credential to the reader within 20 seconds of releasing the Schlage button.
5. The CTE STATUS LED and reader's LED will blink **GREEN** 5 times **indicating success**.
   - The credential is now the Master Construction Credential.

     ➔ **Note:** CTE Master Construction Credentials do not provide access. Master Construction Credentials can only add other User Access Construction Credentials to each installed CTE. If a credential is **not presented within 20 seconds** a timeout will occur and the CTE will begin working as an access control device again. Repeat steps 1-5.

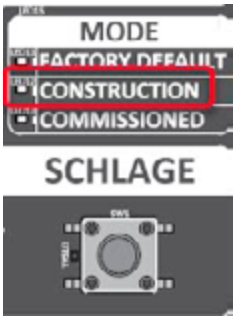


Fig. 18.8: Construction Mode

Create User Construction Credentials

Once the Master Construction Credential has been created, User Access Construction Credentials can be added to the installed CTE.

User Access Construction Credentials allow momentary (Normal) access before the CTE is commissioned.

CAUTION: The Master Construction Credential must be programmed before creating any User Access Construction Credentials.

1. Present the **Master Construction Credential** to the reader.
   - The STATUS LED on the PCB and the reader's LED will light **GREEN** for 20 seconds.
2. Within 20 seconds, present a **USER Construction Credential** to the reader.
   - The STATUS LED on the PCB and the reader's LED will blink **GREEN** 5 times.
   - To create additional User Credentials, repeat steps 1-2.
3. Present a newly created **User Construction Credential** to the reader.
4. Verify that access is granted.

Review the **Wi-Fi Network Requirements** before you begin.

Commissioning the CTE

Commissioning a CTE enrolls the device into ENGAGE, defines the device name, and prepares the device for later setup steps.

1. While near the CTE, log in to the ENGAGE Mobile application.
2. The blank **Devices Screen** will appear. Depending on your Mobile device, one of the screens is presented.

➔ **Note:** The figures show that no devices are commissioned into the property. When devices have been commissioned, this screen will display the name of the commissioned devices.

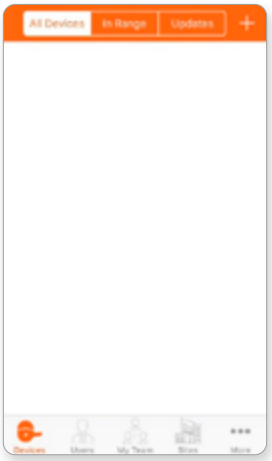


Fig. 18.9: iOS Device Menu

Fig. 18.10: Android Device Menu

- iOS Mobile device: + sign in the upper right-hand corner.
- Android Mobile device: + sign in the lower right-hand corner.

3. To select the nearby CTE device being commissioned, tap the **+ sign**.
4. Select the **CTE** device type for commissioning.

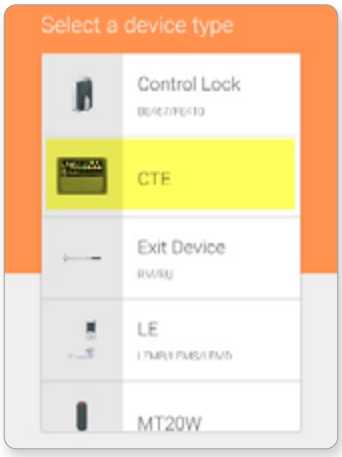


Fig. 18.11: Device Type

5. **Select Use Default Settings**
   - Only once per property
   - Only once for each Administrator
   - Only once for each product type

   ➔ **Note:** This is the ONLY reminder to think about and use the predefined **Property-Wide Settings** (pg. 77) before setting up several devices. Administrators can use the currently defined default ENGAGE settings for this device or elect to modify the Property Wide settings now. Administrators may modify individual device settings at any time, using the Customize Settings option also provided.

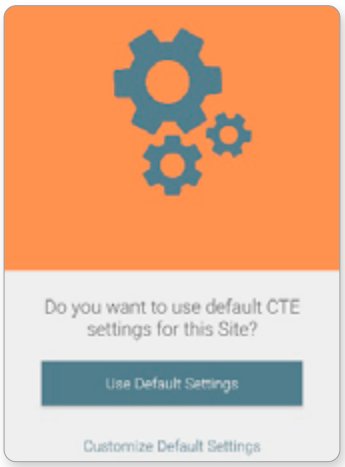


Fig. 18.12: Site Settings

6. Follow the Pop-up message instructions to enable Bluetooth "Advertising" for the desired CTE device.
   - Press and release the Schlage button inside the CTE enclosure.

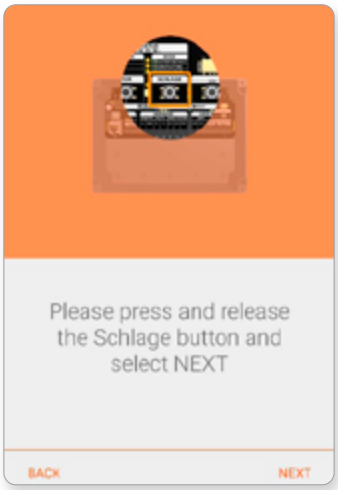


Fig. 18.13: Advertise Presence

WARNING: If no device information is displayed, ensure the following:

- **The CTE is Out-Of-The-Box or recently had a Factory Default Reset.**
- **The Mobile device has Bluetooth turned ON**
- **The Mobile device is in Bluetooth communication (BLE) range of the CTE.**
- **The CTE is "advertising" via Bluetooth (BLE)**

To try again, select Back

7. From the list of displayed devices, select the **CTE device** to be commissioned.

➔ **Note:** The CTE "advertises" for 2 minutes to allow selection. When the device appears in this screen, the number is the device serial number.

Fig. 18.14: Select CTE Device

8. After the CTE has been selected, it will connect to the device and then ask you to verify the LED is blinking **RED.**

Fig. 18.15: Connecting

Fig. 18.16: Light Blinking

9. After verifying the LED is blinking, select **Yes**. It will ask you to **Please Wait** while it processes.

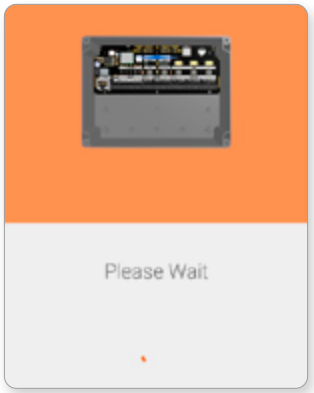


Fig. 18.17: Please Wait

10. Provide a descriptive name under **Device Name**
11. Select Next.

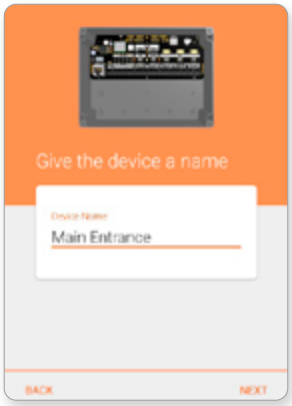


Fig. 18.18: Name Device

12. Select the **strike type** installed on the door.
    - If your strike type is not listed, select **Other**.

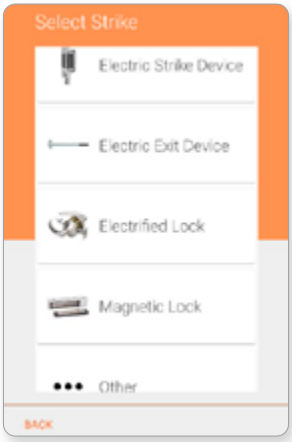


Fig. 18.19: Strike Type

13. Select the **AUX Relay** type.
    - If your AUX relay is not listed, select **Other.**
    - If there are no auxiliary relays, select **Nothing Connected**.

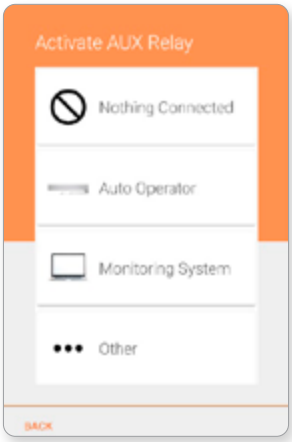


Fig. 18.20: AUX Relay

14. Select if the door has a **horn**.
    - If there is no horn, select **Nothing Connected.**

Fig. 18.21: Horn

WARNING:
The NEXT step in the commissioning process can enable the Wi-Fi network connection capabilities of the CTE. Administrators may also elect to skip setup of the Wi-Fi network when a network is not available or not needed by selecting Skip. The Administrator may enable or edit a Wi-Fi network connection setting at any time using the Mobile application

15. **Select Skip**: Let's assume that the property wide local Wi-Fi network has not been setup yet and there are no local Wi-Fi network connections available.

➔ **Note:** See **Device Wi-Fi Network Setup** for setup requirements when a Wi-Fi network is available, and the Administrator wants to take advantage of the Nightly Call-In feature.

Fig. 18.22: iPhone Wi-Fi Screen

16. Your device is being prepared.

Fig. 18.23: Device Configuration

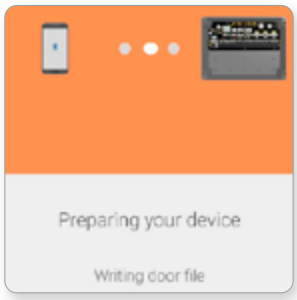


Fig. 18.24: Writing Door File

17. After the device configuration has completed, select one of the following:
    - Finish to complete the commission process.
    - Add Another CTE Device to continue enrolling CTE devices.

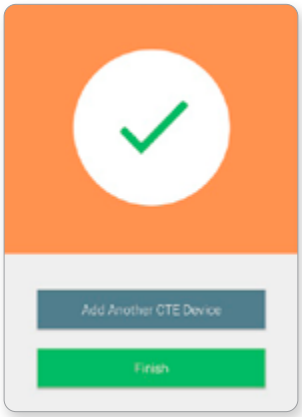


Fig. 18.25: Device Added

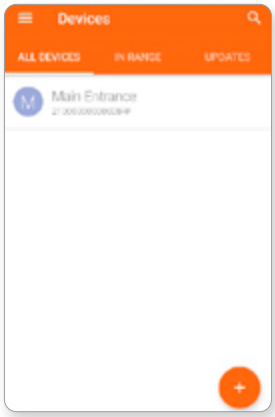


Fig. 18.26: Commissioning Successful

Configuration Cards

Configuration cards are special cards used for configuration and programming the Credential Readers.

The original Schlage family of Multi-Technology (MT11 / MT15) Wall Mounted Credential Readers require configuration card programming to disable/enable card technologies. Mobile Enabled MTB11 and MTB15 wall mounted readers can also be configured to disable and enable credential technologies from the ENGAGE Web Application when connected and linked with a CTE.

Follow these steps to **disable** the **Proximity Credential technology** in the MT or MTB family of wall mounted credential readers:

1. **Locate** the correct configuration card, part number **CE-401-101**.
2. Power cycle the credential reader.

WARNING: The reader will boot up after power is applied. Be sure to wait until the reader beeps three times before presenting the Configuration Card or it will not perform as intended.

3. Within the first 60 seconds from power up (and after Boot Up), **present** and **hold** the configuration card to the reader.
4. The reader acknowledges the configuration card by beeping 3 times; the LED flashes **RED** with each beep.
   - When the beep and LED sequence finish, the configuration update to ignore Proximity card presentations is complete.
5. Once the Proximity technology is disabled, the CTE and the credential reader must be “Paired” or linked together.
   - Remove the CTE lid.
   - **Press and release the Schlage button** once.
   - **Press the FDR button** 2 times; one beep for each button press. The credential readers’ LED will flash **GREEN** when successful.

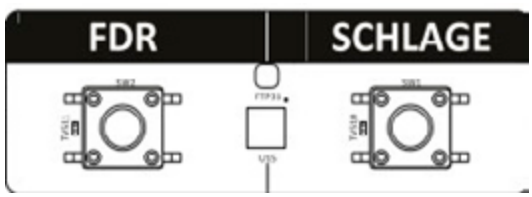


Fig. 18.27: PCB Switches

6. Present a Proximity Credential to the reader to verify the Proximity technology is now ignored when presented.
   - The reader does not acknowledge credentials with Proximity technology. No Beeps or Blinks.

MT20W Installation and Commissioning

The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

Introduction

➔ **Note:** Before you begin, review the MT20W Enrollment Reader User Guide and the Factory Reset Default Configuration card.

The MT20W multi-technology enrollment reader is designed to simplify the enrollment of smart and multi-technology credentials using the **No-Tour Feature** in multifamily applications.

The MT20W is compatible with Schlage smart credentials (MIFARE Classic®, MIFARE Plus® and MIFARE® DESFire® EV1) and supports No-Tour access control when used with supported locks.

https://commercial.schlage.com/en/products/readers.html

Fig. 19.1: MT20W

The MT20W does not read prox credentials.

MT20W initial power up

1. Plug the MT20W into the computer's USB connector. The MT20W will use the USB port for power.
2. Wait a moment while the MT20W boots-up. There will be a series of **RED** LED flashes and beeps.
3. When ready, the LED will be solid **RED** waiting for the next step in the setup process, **Commissioning the MT20W**.

Review the **Wi-Fi Network Requirements** before you begin.

Commissioning the MT20W

➔ **Note:** When commissioning a MT20W Credential Enrollment reader, the No-Tour ENGAGE feature is automatically enabled within the ENGAGE web application.

1. Connect the MT20W to the computer USB port.
2. While near the MT20W to be commissioned, log in to the ENGAGE Mobile Application.
3. The initial blank **Devices Screen** will appear. Depending on your Mobile device (Android or iOS), one of the following screens is presented. **Select** the **Plus** to begin searching for available advertising devices

➔ **Note:** No devices show as commissioned into the property account yet. Each device in the system MUST be commissioned before it is available on the **All Devices** screen.

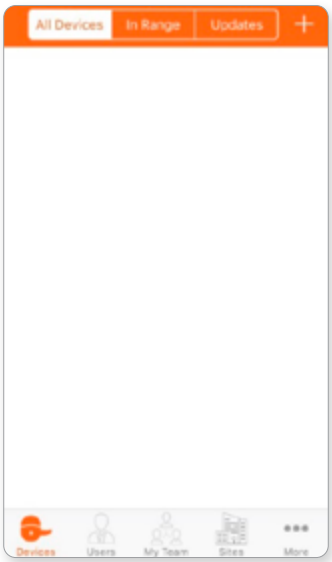


Fig. 19.2: iOS device menu

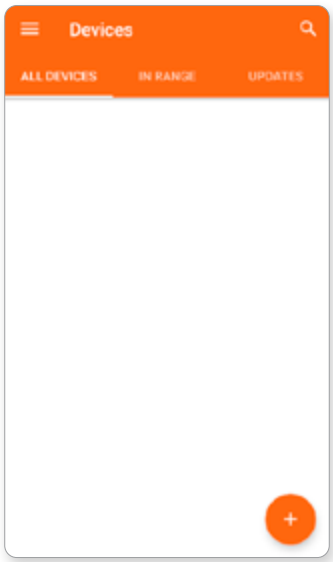


Fig. 19.3: Android device menu

4. Select MT20W device type.

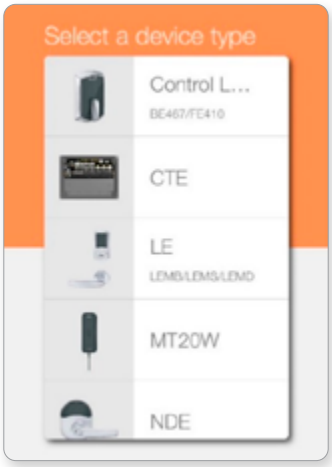


Fig. 19.4: Select MT20W device type

5. **Select** the specific MT20W device to be commissioned from the list of nearby devices.

   ➔ **Note:** More than one device may be available for commissioning.

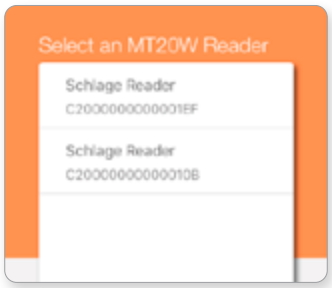


Fig. 19.5: Select the MT20W device

6. Confirm the Schlage MT20W Credential Reader selected for Commissioning. The Blue LED is blinking slowly to indicate it has been selected.
7. Select Yes.

Fig. 19.6: Confirm the MT20W device light is blinking

8. The Please wait... screen displays and is immediately followed by the data transfer method question that the Administrator must answer:
   - Which data transfer method are you using?
9. Select USB (recommended).

   ➔ **Note:** See **MT20W Wi-Fi communication mode (Optional)** on page **193** for more information.

⚠ CAUTION: When using USB communication, you must also INSTALL and RUN the ENGAGE PC Desktop Application.

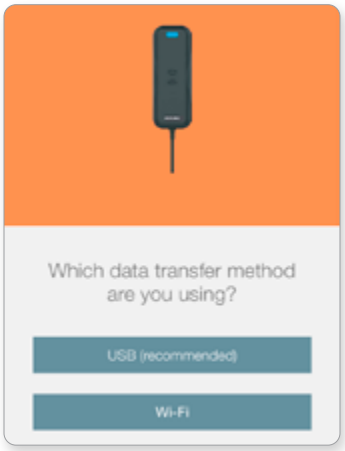


Fig. 19.7: Select data transfer method

10. Preparing your device and then confirmation checkmark screen displays.

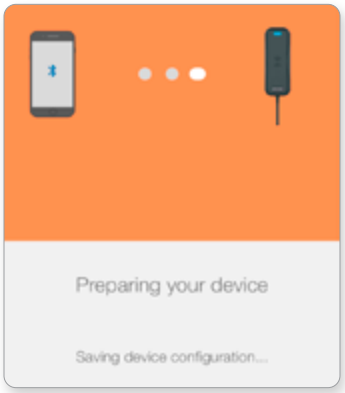


Fig. 19.8: Preparing your device

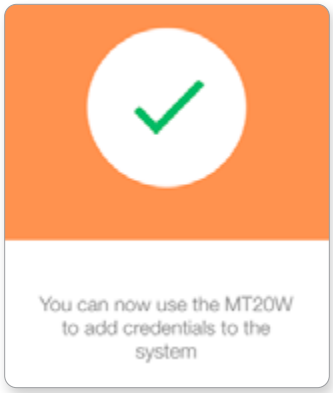


Fig. 19.9: Enrollment confirmation screen

11. Click Next in the top right-hand corner to continue.
12. Select the Send Link button.
13. An email and ENGAGE PC Desktop Application link will be sent to the Administrator's email.

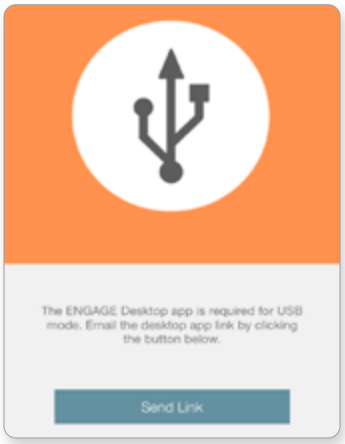
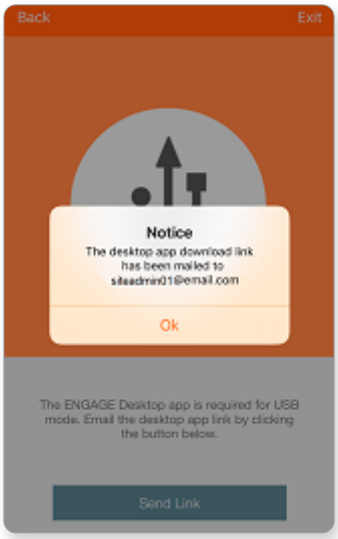


Fig. 19.10: Send link screen

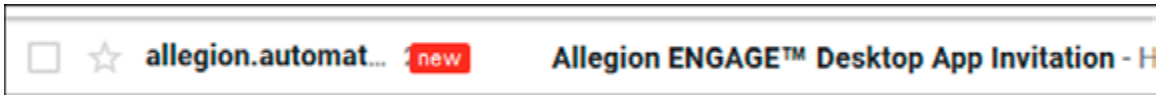
14. Acknowledge the Notice and select Ok.
15. Select Exit in the top right-hand corner to continue. The All Devices screen displays showing the recently commissioned MT20W.



⚠ CAUTION: Before using the MT20W with USB communication, you MUST complete the MT20W setup by **Installing the ENGAGE PC Desktop Application**.

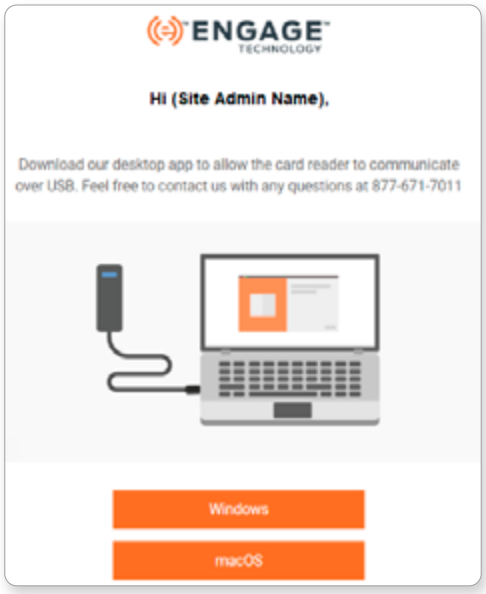
Installing the ENGAGE PC Desktop Application

1. Look for email from Allegion ENGAGE in the Administrator's email.



2. Open the email and then select Windows or macOS operating system button, to match your own operation system.
3. Navigate to the PC "Download" folder.
4. Locate the ENGAGE Setup installation application.
5. Run to install the downloaded file.

   ➔ **Note:** Contact your IT administrator if you need help installing the software.



6. When the installation is successful, and a MT20W is connected to the USB computer port. The following screens display on the desktop.

⚠ CAUTION: Do NOT use the "X" in the top right corner to close the ENGAGE Desktop Application. The application should be running in the background anytime the MT20W is using USB connectivity. When running in the background, the ENGAGE Desktop Application ICON can be seen in the computer system tray.

➔ **Note:** After the MT20W reader and Computer connection is established, the serial number and firmware version of the MT20W are shown.

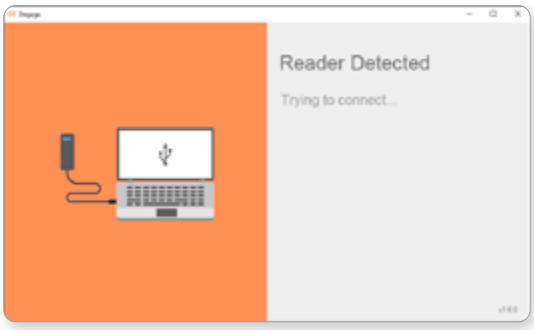


Fig. 19.11: Reader Detected

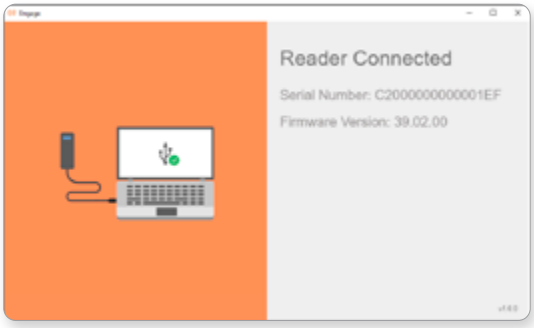


Fig. 19.12: Reader Connected

The MT20W requires a Configuration Card to perform a Factory Default Reset (FDR). This FDR configuration card is provided with the MT20W in the box, or a replacement card (CE-000-040) can be ordered separately.

MT20W Factory Default Reset

The MT20W Factory Default Reset (FDR) is normally needed when a previously used and commissioned MT20W is moved to another ENGAGE account.

Performing FDR with MT20W

Follow the steps below to perform a MT20W FDR.

1. Locate the CE-000-040 Configuration Card.
2. Power cycle the MT20W Credential Reader.
3. Wait a few seconds for the boot-up process to complete. The MT20W will beep 3 times and the LED will be solid **RED** to indicate boot up is complete.
4. Within the first 60 seconds after power up, **present** and **hold** the Configuration Card to the Reader.
5. The MT20W will beep 3 times and the LED will be solid **RED** to indicate successful completion

CAUTION: When an FDR is performed on the MT20W, the Wi-Fi network settings will be erased and decommissioned. The reader will remain in the ENGAGE account, the current MT20W firmware will not be affected.

MT20W Firmware

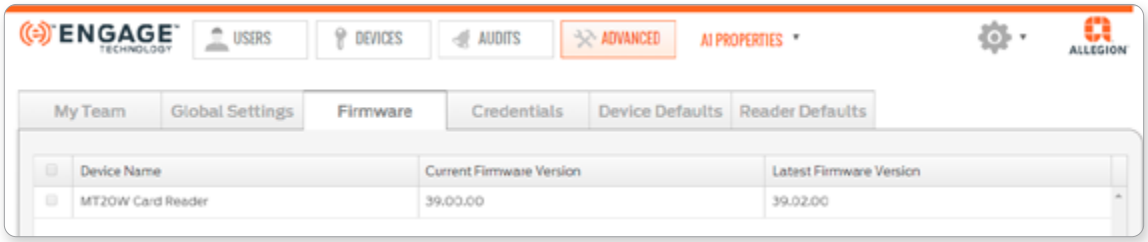
If the MT20W is already commissioned at your site, there are three ways to confirm the firmware version:

- **Web Application**
- **Mobile Application**
- **Desktop Application**

The Mobile Application and the Desktop Application may also be used to update the firmware.

Web Application

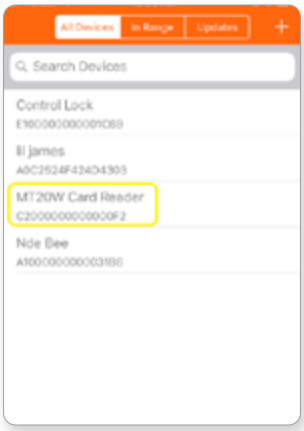
1. Open the ENGAGE Web Application on your desktop.
2. Navigate to the **ADVANCED** tab.
3. Select **Firmware**.
4. Locate the MT20W device in the Device List.
5. View the MT20W **Current Firmware Version** versus the **Latest Firmware Version**.



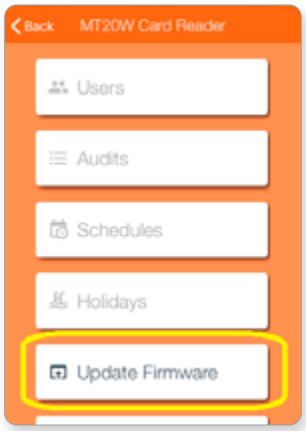
➔ **Note:** If the current MT20W firmware version is earlier than version 39.02.00, you must update the firmware before using the Mobile application to enable USB communication. USB communication is only available when the MT20W firmware is 39.02.00 or higher.

Mobile Application

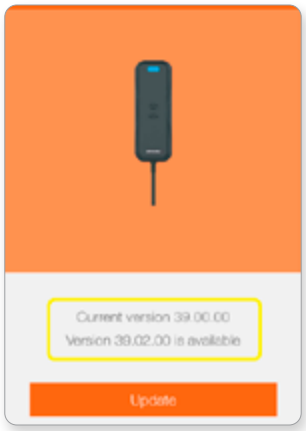
1. Connect to the MT20W.



2. Select Update Firmware.

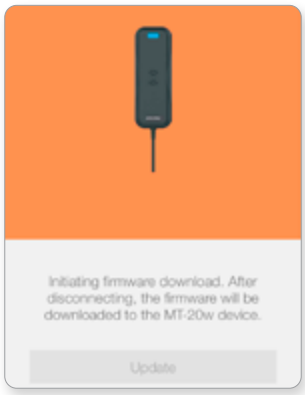


3. Is Firmware Current?

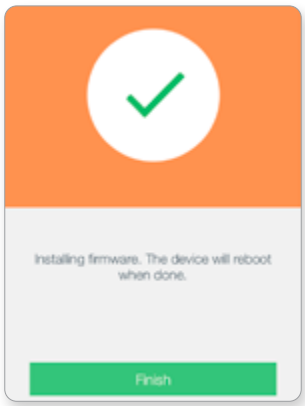


WARNING: The MT20W firmware update is ONLY possible when it is communicating over the local Wi-Fi network. When firmware updates are needed, temporarily enable Wi-Fi network communication to proceed.

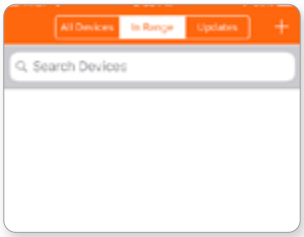
4. The Initiating firmware download screen displays.
5. The firmware is downloaded to the MT20W.
6. The Installing firmware screen displays.



7. Select Finish.

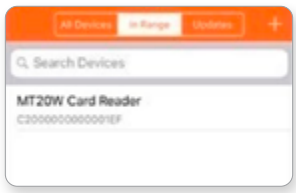


8. The **In Range** Mobile device display is shown. (currently blank)
9. The MT20W will automatically finish its firmware installation process and then it will reboot.
   - Be patient, this may take a few minutes. Wait for all LED flashing to stop.
   - The boot-up process is complete and the MT20W is communicating when a solid BLUE LED displays.



10. **Pull down** the In Range Mobile device screen to refresh the list and view the recently commissioned MT20W

➔ **Note:** The Mobile application screen does not update again until the User swipes down to refresh the screen or navigates away and comes back to the **In Range** screen.



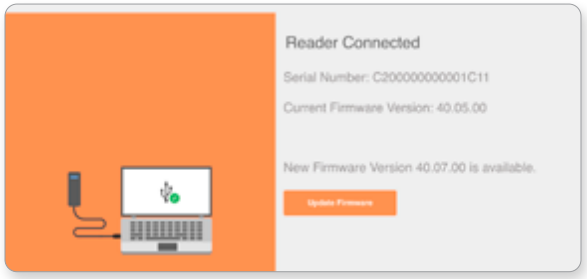
Desktop Application

1. Before beginning, download, install and launch the desktop application.

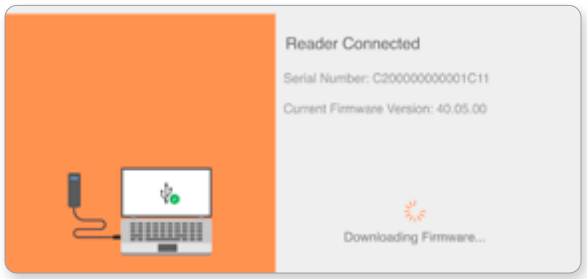
   ➔ **Note:** See **Installing the ENGAGE PC Desktop Application** on page **186** for more information.

2. Once the application is running, connect the reader to the PC using a high-quality USB cable. Wait for the reader to connect.

3. After the connection is established, the serial number and firmware version of the MT20W displays on the screen.
4. If a firmware update is available, the Update Firmware button will be displayed. Click the button to begin the update.

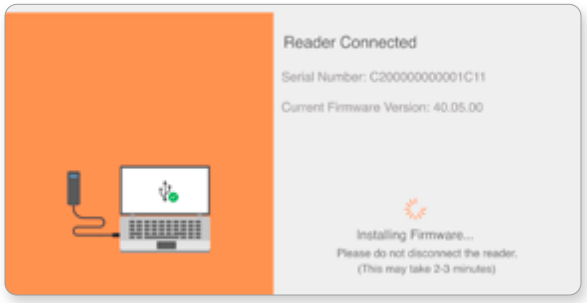


5. The firmware download will begin.

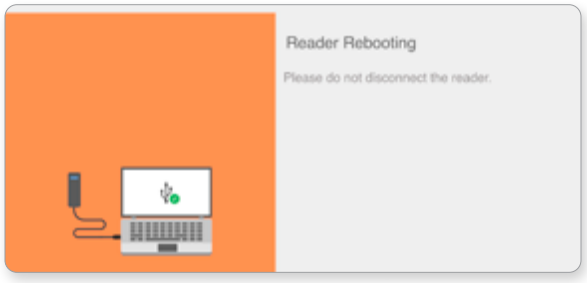


6. Once the download is complete, the update will begin.

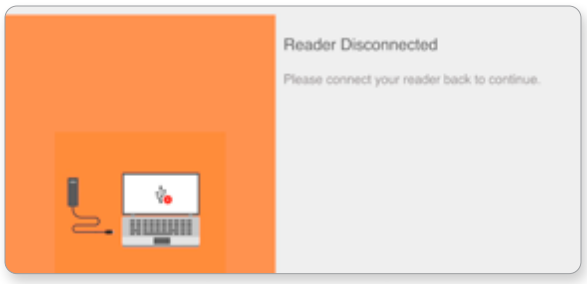
CAUTION: Do not disconnect the reader during the update.



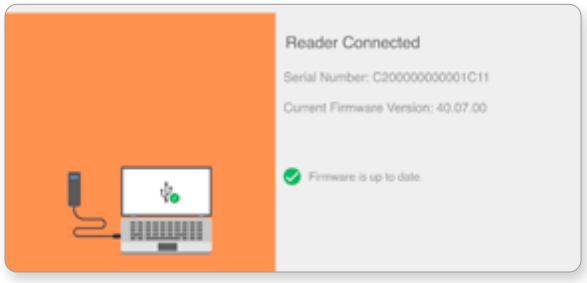
7. Once the update is complete, the reader will reboot.



8. The reader will disconnect after the reboot. Wait for it to reconnect.



9. Once the reader reconnects, it will display the new firmware version.



CAUTION: The ENGAGE Desktop Application is required to be running in the background anytime the MT20W is using USB connectivity

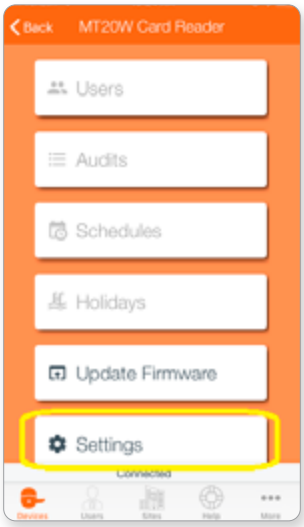
MT20W USB communication mode

The MT20W may be configured to communicate with ENGAGE via USB connection or via a local Wi-Fi network connection. USB connectivity is recommended for the most robust data connection.

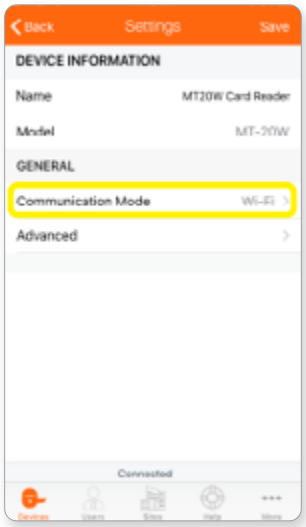
BEST PRACTICE: If the PC is rebooted unplug the MT20W and launch the desktop application, then plug the MT20W back in. This will ensure a good connection to the host.

When connected and communicating with the MT20W, follow these steps to change from a local Wi-Fi network to USB communication mode.

1. Open the ENGAGE Mobile Application on your Mobile device.
2. Select the already commissioned and nearby MT20W
3. Navigate to the Settings Menu.
4. Select Settings



5. Select Comm Mode



6. Select USB Mode

7. Select Save.

MT20W USB communication operation

The Desktop Application acts as a transmitter/receiver between the MT20W and the ENGAGE Web Application.

➔ **Note:** The MT20W LED display indications remain the same no matter which communication mode is used. Solid blue LED means the MT20W is communicating and ready for use.

1. **OPEN** the ENGAGE Desktop Application.
2. **Connect** the MT20W to the USB port.

   ➔ **Note:** Be patient; the connection may take a few seconds.

Fig. 19.13: MT20W Direct

3. After the connection is established, the serial number and firmware version of the MT20W displays on the screen.

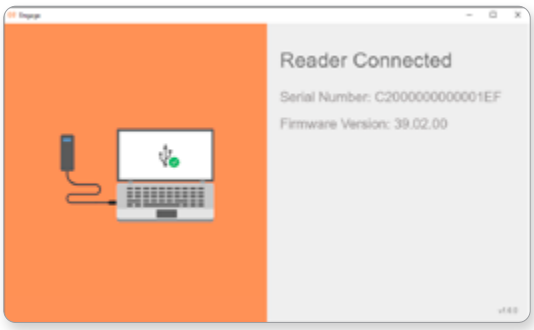


Fig. 19.14: Reader Connected

4. When a credential programming error occurs, an error message along with the error code displays on the screen along with a notification.

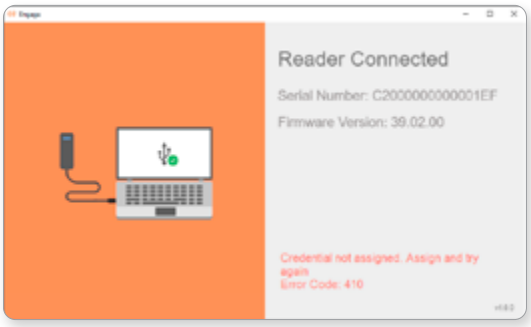


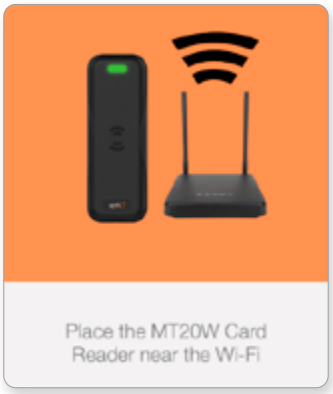
Fig. 19.15: Error Detected

Review the **Wi-Fi Network Requirements** before you begin.

MT20W Wi-Fi communication mode (Optional)

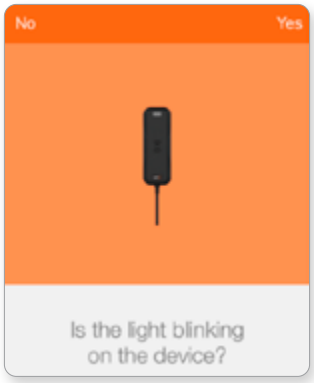
When connected and communicating with the MT20W, follow these steps to change from USB to Wi-Fi communication mode.

1. Ensure the Schlage MT20W is in signal range of the desired local **Wi-Fi** network access point.
2. **Select Next**.

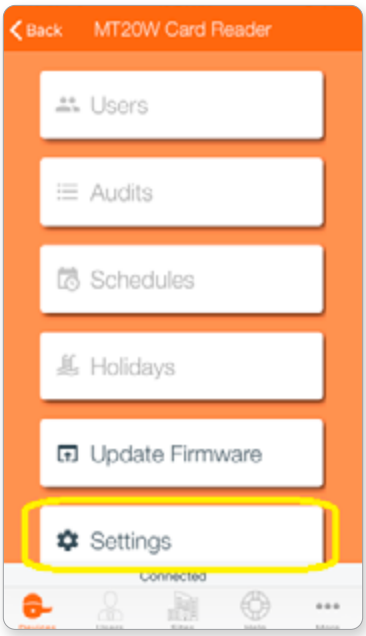


3. **Confirm** the Schlage MT20W Credential Reader selected for Commissioning.

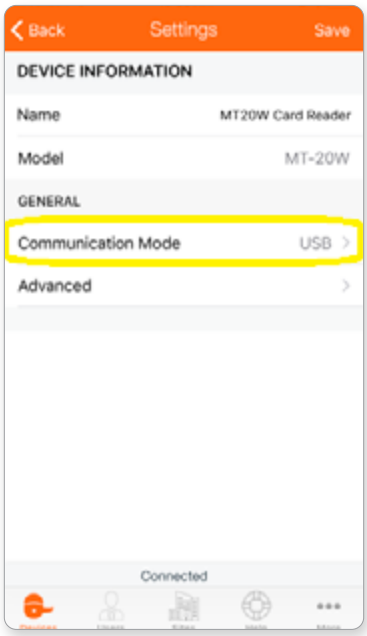
   The LED should be flashing slowly to indicate it has been selected. **Select Yes**.



4. Select Settings.



5. Select Comm Mode.



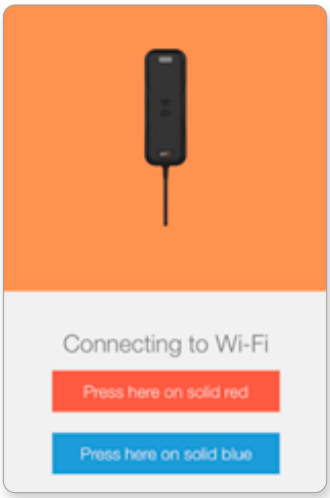
6. Select Wi-Fi.

7. Enter the Wi-Fi network details:
   - Depending on the Wi-Fi network security chosen, you will need to enter different information.
   - Both a Username and Password are required.
8. Select Next.

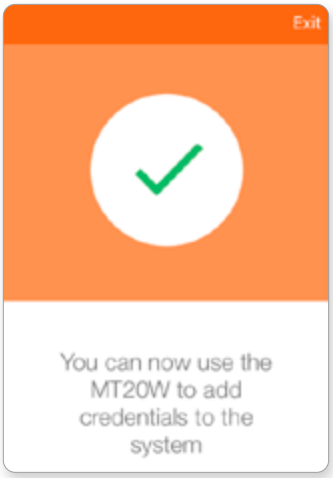
➔ **Note:** If the Schlage MT20W does not provide a solid Blue LED and tries to reconnect but fails, the Wi-Fi network settings are not entered correctly, or the local Wi-Fi network is not present. Recheck the Wi-Fi network settings and try again.

Fig. 19.16: Adding a new Wi-Fi Network

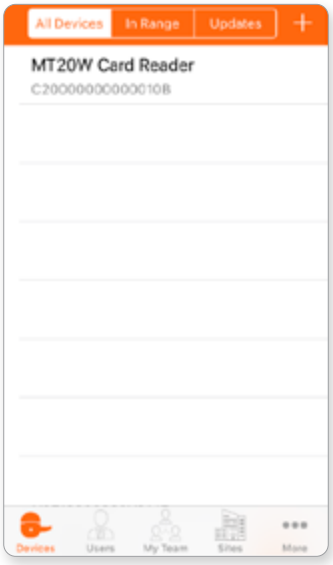
9. Select the Blue **Press here on solid blue** bar to continue.



10. Acknowledge the “Setup Complete” message. Select **Exit**.



11. The MT20W device is now shown in the ENGAGE Mobile Application All Devices menu and the In Range menu when the Mobile device is nearby the MT20W.



MT20W LED/Beep Indications

LED Indication	Beep	Meaning
Red solid 20 seconds followed by red blink	three (3)	booting, boot complete
Red solid		not commissioned
Blue solid		wifi connected and ready for use
Blue fast flash followed by blue solid		USB connected and ready for use

MT20 Installation and Commissioning

Before you begin, review the product information for the Schlage MT20 contained in the box. Also, in the box will be the MT20 Enrollment Reader User Guide and a set of output format configuration cards.

https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html

WARNING: The MT20 is not compatible with the ENGAGE No-Tour features. Administrators that want to use No-Tour must use the MT20W

The installation instructions outlined here are excerpts from the device Installation Instructions found in the box and cover the most common issues encountered when installing the device.

Introduction

The MT20 Enrollment Reader uses a Human Interface Device (HID) Keyboard Interface that requires the user to put the cursor in the desired computer data field of the ENGAGE Web Application to receive the credential data.

The MT20 is an ISO 14443 and ISO 15963 contactless credential reader, and is compatible with Schlage smart credentials, Mobile credentials, PIV credentials and most proximity credentials up to 37-bits.

Fig. 20.1: MT20

Initial Power Up

When an MT20 is plugged into a USB port, it uses the computer power and will go through a boot-up process.

Wait a few seconds for the boot-up process to complete.

The MT20 beeps and the LED will be solid **RED** when it is ready for credential enrollments.

Enrolling a Credential

After the initial boot-up is complete, the MT20 will read any valid credential when presented.

1. Go to the **ENGAGE web application** https://portal.allegionengage.com/signin and **log into your account**.
2. **Hover** over **Users** menu and select **Users** in the pull-down.
3. **Select** the appropriate user from the **Users** list.
4. **Select Add Credential.**
5. **Select** the **Enroll New Credential tab**
6. **Place** the computers 'mouse cursor in that field.
   - When presenting a valid credential to the MT20, the credential data will be stored at the cursor location.

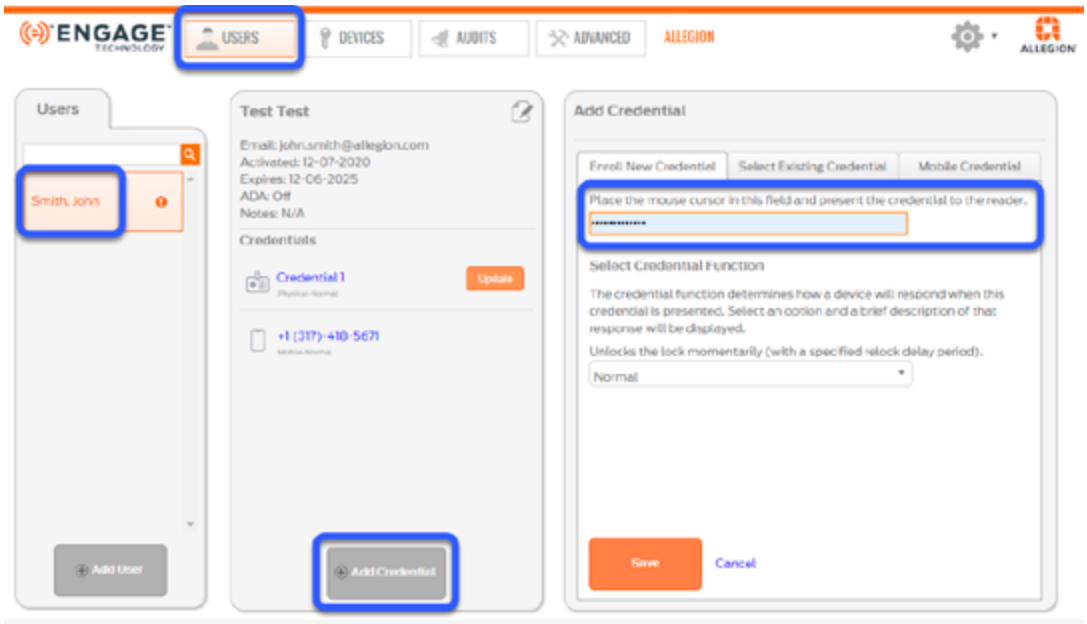


Fig. 20.2: Enroll New Credential

- The MT20 will momentarily flash **GREEN** while reading the credential data and will return to solid **RED**, waiting for the next credential enrollment presentation.
- If the MT20 **does not respond** to a credential presentation, and the LED remains **RED** with no beeps, the credential is not a valid credential type and is not supported.

7. Select **Save**
   - The newly added credential is now listed under “Credentials” for the selected User.

MT20 Output Formats

The MT20 default output format is “hexadecimal” for use with the ENGAGE system. There are additional output formats available when necessary.

To change the MT20 output format, a configuration card is needed and must be presented to the MT20 within 60 seconds after boot-up is completed.

- Default configuration card CE-401-073 required for ENGAGE (Hexadecimal)
- Configuration card CE-401-061 required for **Schlage Express** (Octal)
- Configuration card CE-401-060 required for FC/BID Output
- Configuration card CE-401-069 required for BID Only

Each of these Configuration cards are provided with the MT20 in the box.

Changing MT20 Output Formats

To change the MT20 output format configuration, follow these steps.

WARNING: The reader will boot up after power is applied. Be sure to wait until the reader beeps three times before presenting the Configuration Card or it will not perform as intended.

1. **Select** the desired output format Configuration card. (In the box)
2. Power cycle the credential reader.
3. **Present** the Configuration Card within the first minute after power is applied (and Boot Up completed) and after the MT20 boot-up process has completed
4. The MT20 will confirm the output configuration change with two short beeps and the LED will flash **RED**.
5. The MT20 will then boot-up again and after boot-up is complete, the MT20 will be ready to output the new output format.
   - The MT20 red LED will remain ON solid waiting for a new credential presentation.

Troubleshooting

Problem	Solution
MT20W does not connect to the local Wi-Fi Network.	• Verify the proper SSID and Password settings, if applicable. • Use a Mobile device to verify if the Wi-Fi network (Access Point) is present and available at the device, now. • Perform Factory Default Reset (FDR) using configuration card CE-000-040. Then commission the MT20W again.
Email invitation never arrived in the team member's email account.	• Check the team members SPAM and TRASH folders for misplaced email. • Verify the entered email address was entered correctly. • Verify your PASSWORD.
Mobile Access application Invitation Text not received.	• Ensure the user has a signal and can receive text messages. • Navigate to the Mobile credential menu to "Delete this credential". Then try the process again.
Device never shows up in the **In Range** Mobile application list.	• Does the device need Factory Default Reset (FDR)? • Is the device in Construction Mode? • Is the device already commissioned? • Is the battery cover securely installed? • For Control devices: Is the deadbolt retracted? • Are there other BLE connected dives present (Headsets, ear buds, personal devices (watches, health monitors, etc.)
Device does not allow Construction Mode.	• Devices MUST be Out-of-the-Box or recently Factory Default Reset (FDR). • Verify the Administrator has not "Blocked" construction mode using the ENGAGE Web application before resetting the device. • The device will require commissioning with the Construction Mode feature **UN-BLOCKED**, to allow Construction Mode again after FDR is completed.
Device firmware updates overnight not performed.	• Verify local Wi-Fi network was operational overnight. Was there an outage? • Verify the device Wi-Fi network settings, SSID, username and password. • Use the **Test Wi-Fi Connection** feature in the Mobile Application to verify Wi-Fi communication.
Message that updates are required cannot be cleared.	• When a tour site already has credentials and is then converted to a no-tour site, credentials will warn that updates are required with an MT20W but will not be able to be cleared.
The batteries on my Control lock are completely dead.	• Jump Start the lock. See **Control Mobile Enabled Smart Lock Jump Start Process** on page **24** for more information.
CTE and credential reader stopped working.	• The Credential Reader and the Schlage CTE are "Paired" when initially Powered-ON. • If the Credential Reader is replaced or not connected when the Schlage CTE is powered up, the new Credential reader is not able to communicate with the Schlage CTE. • See **Credential Reader Connection to CTE** on page **173** for more information.
The device date and time are incorrect.	• After changing batteries or jump-starting a lock, the date and time can get out of sync. See **Setting Device Date and Time** on page **23** for more information.
Mobile credential user is unable to unlock assigned door.	• Verify the Mobile credential is enabled within the lock settings. • Verify that access has been given to the correct door. Mobile credentials are given access to doors the same method as physical credentials in ENGAGE. • Verify a Sync Device Update (update door file) has been performed at the door. Or wait until tomorrow after a Sync Overnight Wi-Fi Update has processed.
ENGAGE Web Application Badge search failed.	• The search for a badge (or credential) requires that the badge be initially enrolled using the MT20W or MT20 enrollment reader. • Credentials enrolled through a lock (at a door) do not have a Badge ID and cannot be found using the ENGAGE Web Application Badge Search utility.
Invalid Starting Badge ID	Setting the starting badge ID to a number lower than the existing badge ID is not permitted.
Badge ID Limit Reached	If the badge ID limit has been reached for a specific bit format, a message indicating that the maximum badge ID has been reached will be displayed. Use a different bit format.

Frequently Asked Questions

How can I determine the local Wi-Fi network settings?

- Consult with the local property IT responsible person.
- Use a Mobile Phone to connect and verify the local Wi Fi network.

Does ENGAGE work with 5.0GHz network routers?

- ENGAGE requires 2.4 GHz 802.11 b/g Wi-Fi
- ENGAGE is not compatible with 5.0 GHz routers.

What is the Wi-Fi network "Mandatory Data Rate"?

- The local Wi-Fi network router can be setup to connect with devices that communicate at a minimum data rate speed.
- Setting this minimum communication speed helps to ensure the local network traffic is as robust as possible by not responding to weak signals.
- The local IT professional can verify, review and adjust this setting if needed.
- Schlage MT20W and NDE devices require the local Wi-Fi network setting for maximum Mandatory Connection Speed to be 24Mbps or lower.
- Schlage LE and CTE devices support standard Wi-Fi data rates and always connect to the local Wi-Fi as necessary.

What is the ENGAGE Mobile device Bluetooth communication range?

- Bluetooth communication is low power by design, for longer battery life.
- Bluetooth communication is generally available up to 30 feet, for a Line-Of-Sight connection.
- Walls and obstacles will reduce communication range
- Bluetooth communication through walls and doors significantly reduces communication range.
- For all ENGAGE Mobile Application Bluetooth communications, the Administrator should be as close as possible to the device – < 10 feet of the device.
- When the ENGAGE Mobile Application successfully connects with the nearby device the device LED will be blinking.

What are the different ENGAGE Team Member Capabilities?

- See the table in Appendix A.

Do Property "Team Member" invitations Expire?

- When invitations are not confirmed by email, they expire in less than a week.
- Resend of invitations is possible for expired invitations at any time.
- Invitations and Team Members can be deleted at any time.

How do I know the Schlage MT20W is working?

- When ready and communicating, the Schlage MT20W LED is solid BLUE.
- If not Commissioned the LED is solid RED after booting up.
- The Schlage MT20W Boots Up upon power application.
- On Power up, the RED LED flashes and beeps.
- The BLUE LED begins flashing for a few seconds.
- The BLUE LED turns solid BLUE when the MT20W is ready for enrollments/programming.
- When using the USB direct mode of communication, the ENGAGE desktop must also be running

What are the Battery Life expectations of ENGAGE devices?

- Schlage Control: Battery life is 1.5 - 2 years depending on use.
- Schlage XE360: Battery life is 1 - 2 years depending on use.
- Schlage NDE: Battery life is 1 - 2 years depending on use.
- Schlage LE: Battery life is 1 - 2 years depending on use.

➔ **Note:** Advanced device reader sensitivity settings (High/Max) and Mobile Enabled device settings (Performance, Communication Range) will reduce battery life.

What happens when a device battery gets low?

- All battery enabled devices provide local feedback to the user at the door when the batteries are low. Nuisance Delay
- Low Battery status causes the lock to provide a “Nuisance Delay” LED display before allowing normal access.
- Nuisance Delay is about 3 seconds with flashing RED LED followed by the normal Access Granted Green LED.
- A Nuisance delay flashing RED LED followed by a GREEN LED, with access granted is NORMAL OPERATION. – Batteries need replaced
- A Nuisance Delay will be seen for up to 500 operations to allow time for the user to inform the Administrator that maintenance is needed.
- When the Nuisance delay is ignored, devices will enter “Critical Battery” mode and stop operating.
- Devices in critical battery mode do not operate normally or allow access
- A Pass-Through credential may be able to gain access to the device
- Mechanical key access may be required
- Control devices may use its Jump Start feature.
- Schlage NDE and LE devices display a RED LED ON solid (under the battery cover) when the lock has entered “Critical Battery” mode.
- Schlage XE360 devices display an AMBER LED flashing (on the front of the device) when the lock has entered “Critical Battery” mode
- The batteries must be replaced to begin normal operation.

What is a Nuisance Delay?

- Nuisance Delay operation is normal device operation when a device has entered its low battery mode. Normal access will be delay for a few seconds with the RED LED flashing, followed by unlocking and the GREEN LED while in Nuisance mode.
- A Nuisance delay occurs any time a valid credential is presented to a device with Low Batteries.
- Nuisance Delayed access is intended to allow the user time to tell the Administrator that the device needs attention.
- Access will be provided for up to 500 operations during Low Battery, Nuisance Delay operation.
- When a Nuisance Delay is ignored long enough that the device cannot reliability operate, the device transitions into “Critical” battery mode and stops normal operation.

What is Critical Battery Mode?

- Critical Battery mode is provided when the device batteries are nearly depleted.
- Devices in Critical Battery Mode display a RED LED.
- Control: Outside LED is solid RED.
- NDE80/NDEB: LED under the Battery Cover is solid RED.
- XE360: Outside LED is solid RED
- LE/LEB: Outside LED is solid RED.
- Normal lock operations are not possible in Critical Battery Mode:
- A “Pass-through” can be used to attempt to gain access.
- Provided the device still has enough power to run the motor.
- This is not guaranteed.
- If a valid Pass-Through credential does not allow access, a mechanical key or “JumpStart” with Control will be required

Can I use Lithium batteries?

- All ENGAGE battery operated devices require Alkaline Battery technology.
- DO NOT use Lithium batteries.
- DO NOT use “Heavy Duty” carbon batteries.

Why use a Physical Access Control Software (PACS) Managed Account?

- Physical Access Control Software (PACS) Partners may provide additional product and system functionality with features not available with ENGAGE.
- When considering a PACS to manage Access Control, please consult with Allegion Sales and the PACS provider before registering for a Partner Managed Account in the ENGAGE Web Application.

Can I change an ENGAGE managed account to a PACS account?

- YES - Switching devices from an ENGAGE Managed account to a Physical Access Control Software Managed account would require:
- All devices must be deleted from the original ENGAGE Managed account.
- All devices must be Factory Default Reset (FDR).
- All devices must be re-commissioned into the new PACS account.

What concerns are there with using No-Tour?

Devices:

- As BEST PRACTICE: Properties planning the use of No-Tour should enroll and commission the MT20W before any other devices are commissioned.
- Commissioning of an MT20W tells ENGAGE that the property is a No-Tour property and to enable the feature in all newly commissioned devices.

WARNING: Any device commissioned prior to the MT20W, is required to be synchronized (door file updated) again before the No Tour feature can be used. Devices enrolled before the MT20W are not No Tour capable until they are synchronized (Door File updated).

Physical Credentials:

- No Tour credentials have a limited number of sectors or folders to keep track of door assignments.
- There is a maximum of eleven (11) sectors or folders available for device assignment.
- For access programming that requires more than 11 devices, use Door Groups.
- For temporary access (Maintenance), Administrators should use User Activation and User Expiration settings to enable and disable access to days-of the-week and use User Schedules to limit access to a specific time-of-day.
- Do not use Door Assignments and Deletions for credentials intended for regular maintenance access.
- Deleted doors still occupy a slot on the credential as “Blocked”
- Door assignments include valid accesses and any door access that has been deleted.
- Deleted doors are still programmed onto the credential with a “Blocked” attribute to deny access when presented.
- The No-Tour credential blocks a replaced or deleted credential. The credential is not deleted from the lock memory.

Mobile Credentials:

- Mobile Credentials do not have a limit on door assignments.

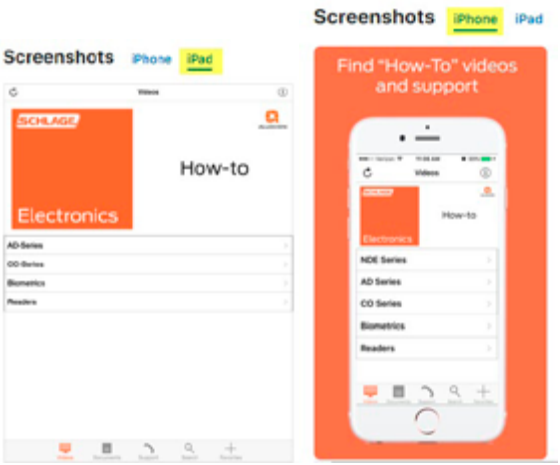
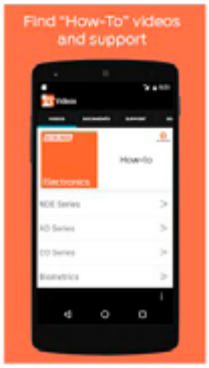
What concerns are there with Control devices and Schedules?

- When assigning User Schedules on Control devices, be advised:
- Users exiting a room (outside their programmed schedule) are not able to relock the deadbolt after exiting.
- The user that exits the door after their scheduled access. Will not be able to relock the door behind them, because the lock denies their credential as outside their scheduled access time(s).

Appendix A: Capabilities by Property Role

#	Capability	Administrator	Manager	Operator
	Roles & Application Access			
1	New ENGAGE Account Default Role	X		
2	Manage Property Information	X		
3	Multiple Roles per Property Account	X	X	X
4	Access Multiple Property Accounts	X	X	X
5	Web Application Access	X	X	X
6	Mobile Application Access	X	X	X
User Management				
7	Invite Users as Administrators	X		
8	Invite Users as Managers	X		
9	Invite Users as Operators	X	X	
10	Assign Users as Administrators	X		
11	Assign Users as Managers	X		
12	Assign Users as Operators	X	X	
13	Manage Users as Administrators	X		
14	Manage Users as Managers	X		
15	Manage Users as Operators	X	X	
16	Delete Users as Administrators	X		
17	Delete Users as Managers	X		
18	Delete Users as Operators	X	X	
19	Manage Users	X	X	
Device Management				
20	Commission Devices	X	X	
21	Connect to Devices	X	X	X
22	Delete Devices	X		
23	Manage Devices	X	X	
24	Run Diagnostics	X	X	X
25	Sync (Update Door Files)	X	X	X
26	Update Firmware	X	X	X
27	Update from Server	X	X	X
28	Get Audits	X	X	X
29	View Audits / Alerts	X	X	
30	Change Wi-Fi Settings	X	X	
31	View Wi-Fi Settings	X	X	X

Appendix B: ENGAGE Training

Training	Link
View 'how-to' videos via the Schlage YouTube channel. For best viewing results, use Chrome. 	Schlage YouTube Channel
 View 'how-to' videos, product datasheets, and install sheets on your iPhone or iPad.	iOS: Schlage Electronis How-To App
View 'how-to' videos, product datasheets, and install sheets on your Android.  	Android: Schlage Electronics How-To App

Appendix C: Credential Functions

Credential Function	Definition
Normal	Unlocks the lock momentarily. Relock delay period is 3 seconds, by default. Relock delay setting can be changed per device, as desired.
Toggle	Changes the state of the lock from locked to unlocked or unlocked to locked. Schlage Control **does not** support Toggle credentials. When a Toggle credential is programmed into a Control, the lock engages the thumb turn for the defined relock delay period.
Freeze	Freezes the lock in its current state (locked or unlocked). Lock remains frozen until a Freeze credential is presented again. The Freeze credential used to “unfreeze” a lock can be the same credential or a different Freeze credential.
One Time Use	Allows only one attempt with Normal Access granted. Schlage Control **does not** support One Time Use credentials and denies access anytime a One Time Use credential is presented.
Pass Through	Unlocks a lock momentarily. Gains access to a lock in Freeze and Lock Down states. Gains access during scheduled Holiday lockouts. Attempts to unlock a device that is in “Critical Battery Mode”.
Lock Down	Changes the state of the lock to locked and disables all normal user credentials. Pass Through credentials gain access when Lock Down is enabled. Freeze credentials must be used to return locks to normal state, from Lock Down
Block	Denies normal access to the lock and records the access attempt as an audit.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit **www.allegion.com**.

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

©2026 Allegion

ALLEGION™