



# ENGAGE

Managed Property  
User's Guide 7.5.2

DISTRIBUTED BY



ACCESS HARDWARE SUPPLY  
[accesshardware.com](http://accesshardware.com)

## About this document

- This User Guide is designed for the Administrators of ENGAGETM Managed Properties and product training teams.
- Administrators that 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
SES20171127F	16 DEC 2020	Reformatted doc. ENGAGE 7.5.2. Updates: Security updates and reader improvements
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

©2020 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

2	About this document	189	<b>Best Practices and Things to Remember</b>
2	Copyright	189	ENGAGE System Set-up
4	<b>Purpose</b>	189	ENGAGE Device Set-up
5	<b>System and Product Revisions</b>	190	Control Mobile Enabled Smart locks
6	<b>Terms and Definitions</b>	191	Factory Default Reset
6	Terms	191	Moving Devices Between ENGAGE Accounts
6	Notes, Cautions and Warnings	191	Dual Technology Credentials
7	<b>Introduction to ENGAGE Technology</b>	192	<b>Troubleshooting</b>
8	<b>ENGAGE or PACS Managed Properties</b>	192	Activity and Diagnostics Audits
8	ENGAGE Managed Properties	192	Inviting Team Members
8	PACS Managed Properties	192	Device Commissioning
9	<b>Overview of ENGAGE Enabled Products</b>	192	Construction Mode
9	LE and LEB Mobile Enabled Wireless Mortise Locks	193	MT20W
10	NDE80 and NDEB Mobile Enabled Wireless Cylindrical Locks	193	MT20W does not connect to the local Wi-Fi Network
11	Control Mobile Enabled Smart Lock	193	Control Mobile Enabled Smart Lock - “Jump Start” Process
12	CTE Single Door Controller	194	Setting Device Date and Time
13	MT20 Credential Enrollment Readers	194	Device Firmware Updates Overnight Not Performed
13	MT20W Credential Enrollment Readers	194	CTE and Credential Reader Stopped Working
14	<b>Wi-Fi Network Requirements</b>	195	<b>Frequently Asked Questions</b>
15	<b>Account and Site Setup</b>	200	<b>Appendix A: Capabilities by Property Role</b>
15	ENGAGE Web Application	201	<b>Appendix B: ENGAGE Training</b>
16	Account Setup	202	<b>Appendix C: ENGAGE Credential Functions</b>
19	Account Team Members		
22	Schedules		
25	Default Device Settings		
39	No-Tour Overview		
40	ENGAGE Mobile Application		
41	<b>Installation and Commissioning</b>		
42	Control Mobile Enabled Smart Lock		
50	LE and LEB ENGAGE Devices		
58	NDE80 and NDEB ENGAGE Devices		
68	CTE Controller with Multi-Technology Readers		
80	MT20		
82	MT20W ENGAGE Device		
98	<b>Daily System and Other Operations</b>		
98	Users Overview		
99	Credentials Overview		
111	Add a Credential to a User		
113	Assign Door Access to User		
119	Mobile Credential Overview		
123	Device Groups Overview		
126	Credential Reuse: Best Practices		
138	Using Master Credentials		
143	Deleting Devices		
145	Updating Device Firmware		
157	Scheduled “Overnight” Firmware Updates		
159	Retrieving Audit Data from Devices		
162	Viewing Audit Information		
180	Device Firmware Updates		
185	Viewing Audit Information		

# 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.

This document is broken down into the following major sections:

- Introduction – Describes the purpose of the document, outlines the ENGAGE managed systems and devices applicable to this user guide, and defines terms and acronyms referenced in this document. (Sections: 1-3)
- Overviews – Briefly describes managed properties, ENGAGE enabled products, and No-Tour. (Sections: 4-6)
- ENGAGE Network / Applications / Account Setup – Provides Wi-Fi requirements, describes the ENGAGE applications, step-by-step instructions for setting up an initial account, and other account features. (Section 7)
- ENGAGE Devices – The most common installation issues, the commissioning process (enroll a device into ENGAGE) by device type, construction credentials, factory default reset, and other features. (Section 8)
- System Operations –These are daily system operations performed by Administrators using either the web or Mobile applications. (Section 9)
- Best Practices & Troubleshooting – These sections provide useful information on things to remember, troubleshooting, frequently asked questions, and appendixes. (Sections 10-13)



# System and Product Revisions

**Table 4.1: ENGAGE Enabled Devices and Revisions** shows the revision levels for systems and products described in this document.

<b>Table 4.1: ENGAGE Enabled Devices and Revisions</b>	
<b>System</b>	<b>Revision Level</b>
ENGAGE Software	7.5
<b>ENGAGE Mobile Software and Operating System</b>	
Android	04.05.15 OS 6.0 or above
iPhone	03.03.39 OS 11.1 or above
<b>Locking Devices</b>	
Control Mobile Enabled Smart Locks	04.06.03
LE Wireless Mortise Locks	01.08.05
LEB Wireless Mortise Locks	03.06.10
NDE80 Wireless Cylindrical Locks	02.13.02
NDEB Wireless Cylindrical Locks	03.06.10
CTE Single Door Controllers	01.4.19
<b>Credential Readers and Controllers</b>	
RU/RM	01.02.42
MTB11-RS485	60.47.07
MTB15-RS485	60.47.07
MT20	39.00.00
MT20W	39.04.00

The latest firmware and software versions are available on the [ENGAGE Support Resources](#) web site. 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.

# 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.

# Introduction to ENGAGE Technology

The Allegion ENGAGE technology makes it easy to connect people, openings and access together, delivering cost-effective intelligence and efficiency to any property.

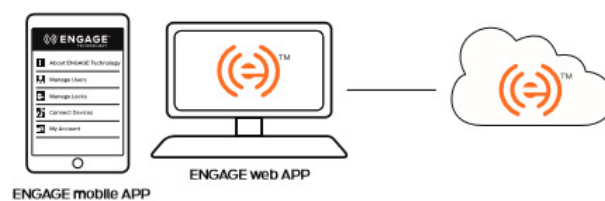
Robust Access Control solutions featuring ENGAGE Technology can be customized to fit any size business or budget and easily adapt to growing or changing business needs.

With the ENGAGE cloud-based web and Mobile applications, it's easy to configure settings, manage users, assign access privileges, and view audits and alerts from anywhere.

Updates to configuration and access privileges can be sent while physically near the device with an ENGAGE Mobile application, or, to wirelessly send updates without visiting the device, the administrator may leverage the existing Wi-Fi network and/or built-in No-Tour capability.

The ENGAGE web and mobile applications will allow enhanced capabilities including audit filtering, lock schedules, user schedules, and holidays.

## Flexible ENGAGE Solutions



### Manage access

Manage your site from anywhere with ENGAGE cloud-based web and mobile applications.

- Configure lock/device settings
- Add new users and enroll credentials
- Manage users and assign access privileges
- New! Set lock schedules, holidays, user schedules
- View and export audits and alerts
- Invite others to assist with administration

**For more information, download the ENGAGE™ web and mobile app data sheet from [allegionengage.com](http://allegionengage.com)**

→ **Note:** Administrators will save time and effort when setting up an account by:

- Reviewing this document and planning for the hardware implementations
- Understanding how the ENGAGE family of products will be implemented and support the Access Control requirements.
- Defining all property default settings and schedules

# 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.

There are two basic options:

- Use the free ENGAGE Cloud-based software and mobile applications offered by Allegion for robust property-wide access control and monitoring.
- Use software managed by Allegion's Physical Access Control Software (PACS) providers for additional features and access control and management by others.

## ENGAGE Managed Properties

The ENGAGE Managed Properties are managed using the free ENGAGE Web and Mobile applications.

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

## PACS Managed Properties

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

 **WARNING:** When planning to use a PACS system, please consult your Allegion sales associate and PACS provider

# 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.



Fig. 8.1: 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 and NDEB 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.

### 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
- 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



Fig. 8.2: NDE80 and NDEB Wireless Cylindrical Locks

## 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. Field upgrade kits are available to retrofit an older Control to the newer Mobile Enabled version.

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. 8.3: Schlage Control Deadbolt identifying mark**.

### 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



Fig. 8.3: Schlage Control Deadbolt identifying mark



BE467



FE410

Fig. 8.4: Control Mobile Enabled Smart Locks

Allegion offers a MTK15-RS485 and MTKB15-RS485 wall mounted reader with keypad interface. However, when using ENGAGE, the CTE is not compatible with keypad data entry.

Keypad versions, MTK15-RS485 and MTKB15-RS485 wall mounted reader with keypad are not supported by ENGAGE at the time of this writing.

## CTE Single Door Controller

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. 8.5: CTE Controller and Wall Mounted MT15-RS485 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 MT11-485 or MT15-485 and MTB11-485 and MTB15 credential readers
- Construction mode is based on MASTER and USER access construction credential enrollments

### 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.



Fig. 8.6: Mobile Credential Enabled identifying symbol



Fig. 8.7: MTB11-RS485 and MTB15-RS485 Readers



- 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.

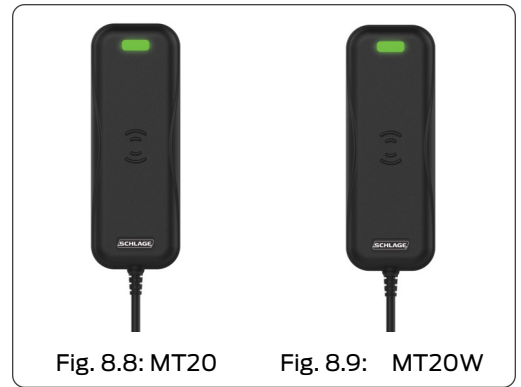


Fig. 8.8: MT20

Fig. 8.9: 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

# 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 **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 9.1: Wi-Fi Network Requirements**

Required Wireless Frequency	2.4 GHz (802.11 b/g) (NDE80, MT20W, CTE/MT reader)		
Alternate Wireless Frequency	2.4 GHz (802.11 b/g/n) (LE/LEB, NDEB and CTE/MTB reader)		
Mandatory Connect Data Rate	24 Mbps when working with NDE and MT20W → <b>Note:</b> 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		

# Account and Site Setup

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

## ENGAGE Web Application

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.

### Supported Web Browsers

The ENGAGE Web Application is supported by the following web browsers:

- Google Chrome 48.0 or newer
- Internet Explorer 11.0 or newer
- Microsoft Edge 12 or newer
- Mozilla Firefox 49 or newer
- Safari for Mac OS 10 or newer

## Account Setup

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

When setting up a new account, perform the following tasks described below:

### Create an Account

1. Navigate to <https://portal.allegionengage.com/signin>.
2. Select **Create Account**.
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**.
6. Select **OK** when account has been successfully created;
7. Go to the email used to create the account and open the verification.
  - Look for an email from [tickets@allegionengage.uservoice.com](mailto:tickets@allegionengage.uservoice.com).
8. Select **Confirm my account** to activate.

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.

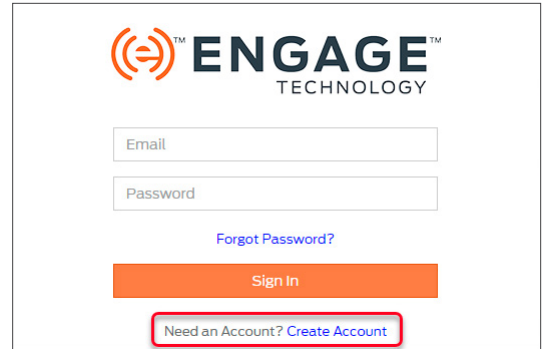

 The image shows the ENGAGE Logon Screen. At the top is the ENGAGE TECHNOLOGY logo. Below it are two input fields: 'Email' and 'Password'. A link 'Forgot Password?' is positioned between the two fields. Below the password field is an orange 'Sign In' button. At the bottom, there is a red-bordered box containing the text 'Need an Account? Create Account'.

Fig. 10.1: ENGAGE Logon Screen

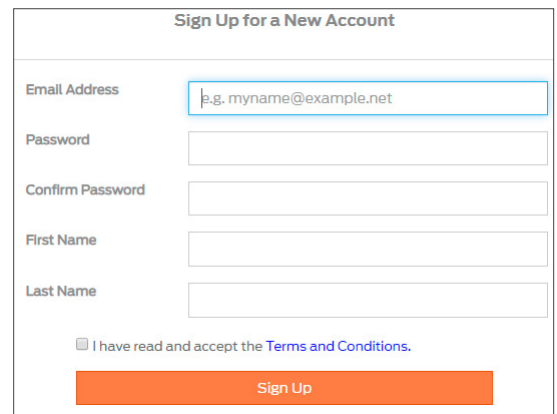

 The image shows the 'Sign Up for a New Account' screen. It has a title bar 'Sign Up for a New Account'. Below it are several input fields: 'Email Address' (with a placeholder 'e.g. myname@example.net'), 'Password', 'Confirm Password', 'First Name', and 'Last Name'. At the bottom, there is a checkbox labeled 'I have read and accept the Terms and Conditions.' and an orange 'Sign Up' button.

Fig. 10.2: ENGAGE Create Account Screen

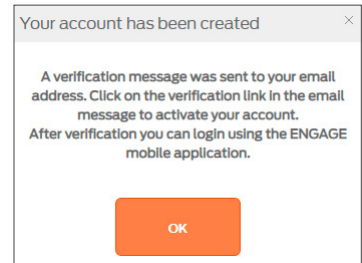

 The image shows a confirmation dialog box titled 'Your account has been created'. The text inside says: 'A verification message was sent to your email address. Click on the verification link in the email message to activate your account. After verification you can login using the ENGAGE mobile application.' There is an orange 'OK' button at the bottom.

Fig. 10.3: ENGAGE Account Created

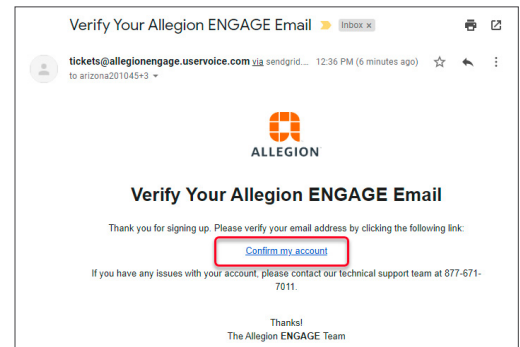
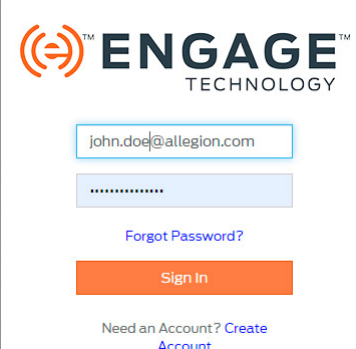

 The image shows an email from 'tickets@allegionengage.uservoice.com' with the subject 'Verify Your Allegion ENGAGE Email'. The email body contains the Allegion logo, the title 'Verify Your Allegion ENGAGE Email', and a message: 'Thank you for signing up. Please verify your email address by clicking the following link:'. Below this is a red-bordered box with the link 'Confirm my account'. At the bottom, it says 'Thanks! The Allegion ENGAGE Team'.

Fig. 10.4: Verification Email

### Log In

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



ENGAGE<sup>TM</sup>  
TECHNOLOGY

john.doe@allegion.com

\*\*\*\*\*

[Forgot Password?](#)

**Sign In**

Need an Account? [Create Account](#)

Fig. 10.5: Login screen

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

Create a new Site

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

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

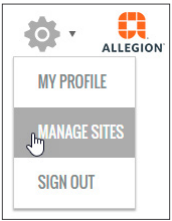


Fig. 10.6: MANAGE SITES

- 3. Select **Create New Site** button.

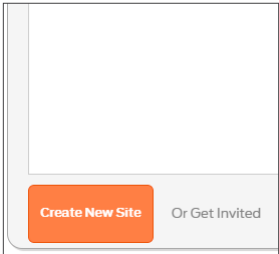


Fig. 10.7: Create New Site Button

- 4. In the **Create New Site** screen, enter the following information:
  - Select **ENGAGE** from the **Site Software** drop-down.
  - Enter a descriptive **Site Name** (Oak Tree Property in this example).
  - Select the **Site Type**.
  - Select the appropriate **Time Zone**.
  - Adjust the **Daylight Saving Time** option adjust as needed.
- 5. Select the **Save** button.

A screenshot of the 'Create New Site' form. It contains several fields: 'Site Software' (a dropdown menu with 'ENGAGE' selected), 'Site Name' (a text input field with 'Oak Tree Property'), 'Site Type' (a dropdown menu with 'Commercial Office' selected), 'Time Zone' (a dropdown menu with '(UTC-05:00) Eastern Time (US & Canada)' selected), and 'Daylight Saving Time' (a toggle switch currently set to 'ON'). At the bottom are 'Save' and 'Cancel' buttons.

Fig. 10.8: Create New Site Screen

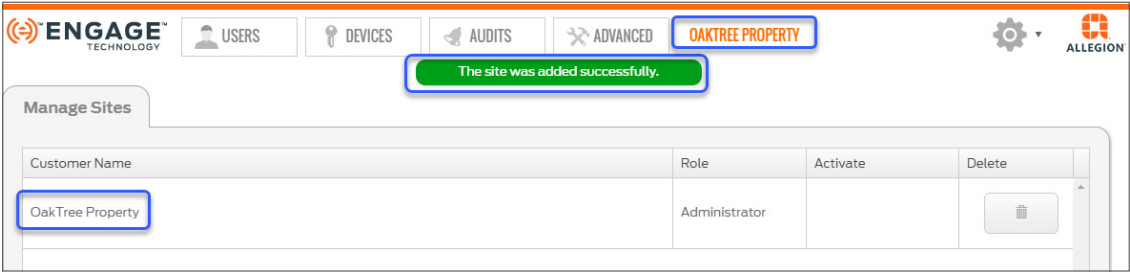


Fig. 10.9: Site added successfully

- 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.

## Account Team Members

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 204.

**Table 10.1: Team member roles**

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

### Add Team Member

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

Assign team members as Administrators, Managers, or Operations to help manage the property.

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

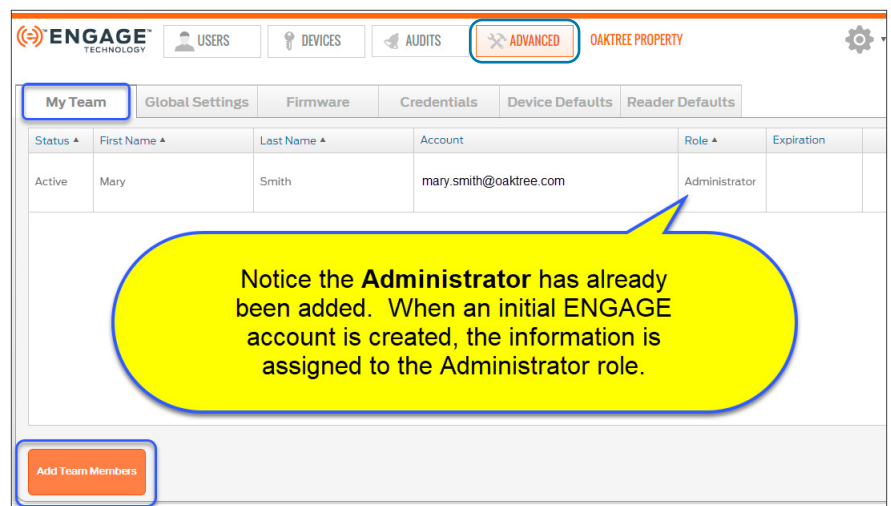


Fig. 10.10: Add Team Members

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 10.1: Team member roles**.

Fig. 10.11: Invite new team members

5. Select the **Send Invitation** button.
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 or Delete Invitation** on page 21.

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 21.

### Verify new team member

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.
2. Click the **Accept This Invite** link.

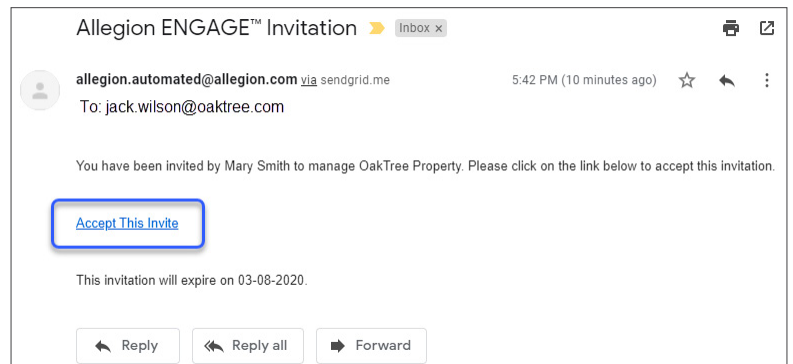


Fig. 10.12: Allegion ENGAGE Invitation Email

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

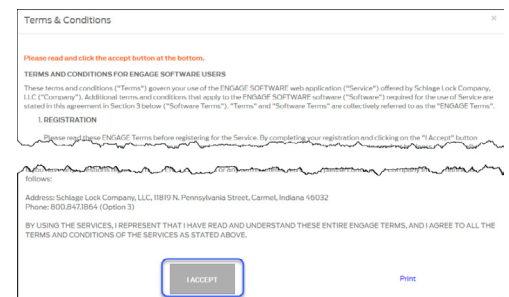


Fig. 10.13: Accept Terms & Conditions

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

Fig. 10.14: 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.
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.

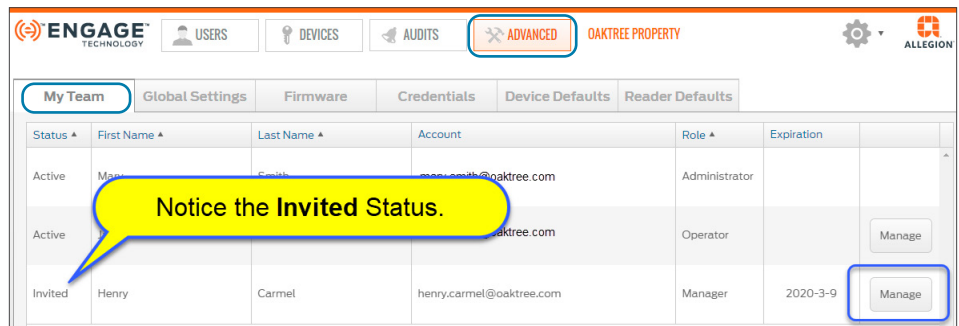


Fig. 10.15: Manage Team Member

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

User Schedules may be created before any actual users are entered into the ENGAGE system.

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

Any User Schedule changes will not be active until devices are updated.

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

## Schedules

There are three types of Schedules:

- User Schedules: pg 22
- Device Schedules: pg 23
- Holidays: pg 24

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

### User Schedules

User Schedules are used to control individual door access that is limited to a day or days, time of day, or a specific maintenance schedule. Think of User Schedules as First Shift, Second Shift, etc.

Defined User Schedules are assigned to individual Users when their door access permissions are selected. A maximum of 16 User Schedules can be defined per property.

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

#### Add/Edit/Delete User Schedule

1. **Log In.**
2. Select the **Users** menu and the **Schedules** pull-down.

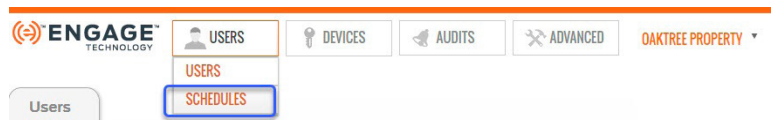


Fig. 10.16: Users > Schedules

3. Select the **Add New User Schedule** button.

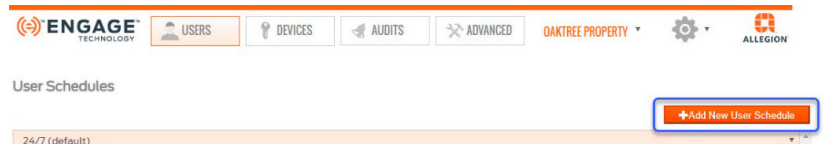


Fig. 10.17: Add New User Schedule button

4. Complete required fields:
  - a. **Name:** enter a descriptive name
  - b. **Access Begins:** select the time access will begin
  - c. **Access Ends:** select the time access will end
  - d. **Scheduled Days:** check applicable day(s)
5. When finished, select **Save**.
6. To modify a User Schedule, do one of the following:
  - Select **Edit** to open the schedule and update any setting.
  - Select **Deactivate** to remove the schedule from the devices.
  - Select **Delete** to remove the schedule from the site.

Add New Schedule

Name:

Scheduled Time:

Access Begins:

Access Ends:

Scheduled Days:

☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Fig. 10.18: Add New User Schedule

User Schedules

24/7 (default)

Pool #1

Access	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Begins	6:00 AM	6:00 AM	6:00 AM	6:00 AM	6:00 AM	6:00 AM	6:00 AM
Ends	11:00 PM	11:00 PM	11:00 PM	11:00 PM	11:00 PM	11:00 PM	11:00 PM

Deactivate - Update Locks Only  
Delete - Must update all the Credentials and Locks

Click to expand and close schedules.

Fig. 10.19: User Schedules

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

**Dog on Next Exit** and **Undog** are not applicable.

RU/RM exit devices are products that can Remotely Monitor an opening and/or Remotely “Dog” (Unlock) and “Undog” (Lock) via Device Schedules

RU/RM devices are normally managed in PACS accounts and provided here ONLY for Allegion product demonstrations in an ENGAGE account.

## Device Schedules

Device Schedules are defined to schedule automatic lock/unlock operations at a door. Device Schedules are actions to be automatically performed at the door. A maximum of eight (8) Device Schedules can be defined per property. Think of Device Schedules as Open Hours, Lock up Time, etc.

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

### Create/Add/Edit Device Schedules

1. **Log In.**
2. Select **Devices** > **Schedules**.
3. Click **Add New Event Schedule**.



Figure 10.20: Devices > Schedule

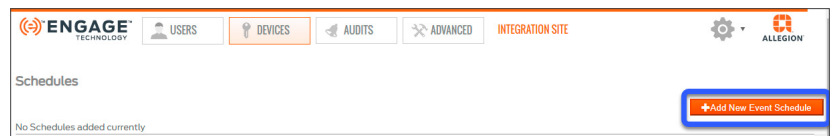


Fig. 10.21: Add New Event Schedule Button

4. From the **Add New Schedule** screen, complete required fields:
  - a. **Name:** enter a descriptive name of the device schedule
  - b. **Action – Start:** select the desired start action
  - c. **Action – End:** select the desired end action
    - **Unlock:** users can pass through door without a credential
    - **Lock:** credential required to access door
    - **Do Nothing:** lock state does not change
  - d. **Start:** select when the action will start
  - e. **End:** select when the action will end
  - f. **Scheduled Days:** check applicable

Fig. 10.22: Add New Schedule

5. Select **Save**, when completed

6. The new schedule has been added to the list of **Device Schedules**.

Action	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Device Type: Lock
Unlock	6:00 AM	6:00 AM	6:00 AM	6:00 AM	6:00 AM	6:00 AM	6:00 AM	Assign Devices
Lock	10:00 PM	10:00 PM	10:00 PM	10:00 PM	10:00 PM	10:00 PM	10:00 PM	

Fig. 10.23: Confirm the schedule settings

7. Select the new **Laundry #1** schedule to expand the schedule.
8. Select **Assign Devices**.
9. Select any device listed in the **Un-Assigned Devices** column and move it to the **Assigned Devices** Column.
10. Select **Save** to complete the Device Schedule assignments.

Fig. 10.24: Assign devices

Select the **Edit** Button to open the schedule and update any setting.

Select the **Delete** to remove the schedule from ENGAGE.

Requires Device and Credential Updates before changes are active.

**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

**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.

**Create/Add/Edit Holidays**

1. **Log In.**
2. Select **Holidays > Devices**.
3. Click **Add New Holiday**.
4. From the **Add New Holiday** screen, complete the required fields:
  - a. **Name:** enter a descriptive name of the holiday schedule
  - b. **Holiday Start:** select the desired start date and time
  - c. **Holiday End:** select the desired end date and time.
  - d. **State:** select the desired state of the door during this holiday
    - **Locked:** credential required to access door
    - **Unlocked:** users can pass through door without a credential
    - **Restricted Access:** passthrough credential required to access door
5. Click the **Save** button.
6. Select the new **New Year's Day** schedule to expand the schedule.
7. Select **Assign Devices**.
8. Select any device listed in the **Un-Assigned Devices** column and move it to the **Assigned Devices** Column.
9. Click **Save** to complete the Device Schedule assignments.

Select the **Edit** Button to open the schedule and update any setting.

Select **Delete** to remove the schedule from ENGAGE.

Requires Device and Credential Updates before changes are active.

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



Fig. 10.25: Devices &gt; Holidays

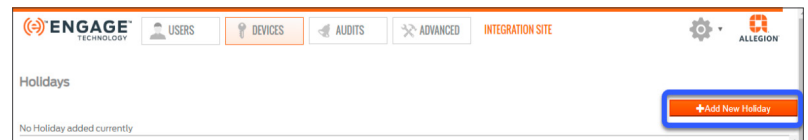


Fig. 10.26: Add New Holiday Button

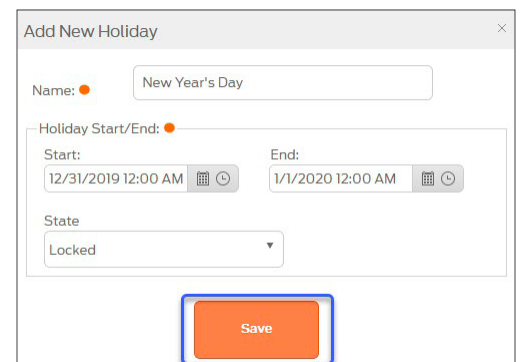


Fig. 10.27: Add New Holiday

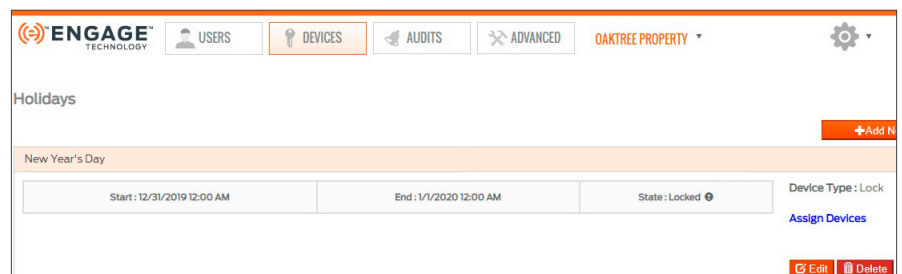


Fig. 10.28: New Holiday Added

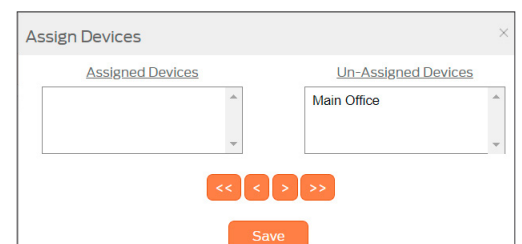


Fig. 10.29: Assign devices

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 default device settings.

## Default Device Settings

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. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
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 26
- **CTE** on page 27
- **LE and LEB** on page 28
- **NDE80 and NDEB** on page 29
- **RU/RM** on page 30

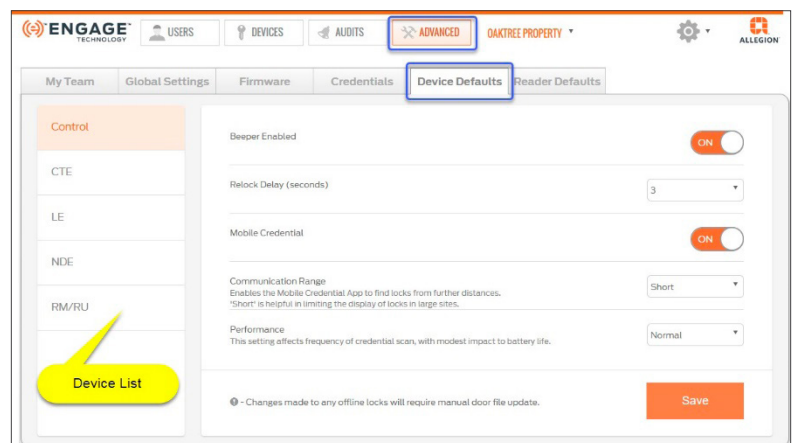


Fig. 10.30: Advanced > Device Defaults

## Control Mobile Enabled Smart Lock

The screenshot shows the 'Control' tab selected in the left sidebar. The main settings area includes:

- Beeper Enabled:** A toggle switch set to 'ON'.
- Relock Delay (seconds):** A dropdown menu set to '3'.
- Mobile Credential:** A toggle switch set to 'ON'.
- Communication Range:** A dropdown menu set to 'Short'. Below it, a note states: 'Enables the Mobile Credential App to find locks from further distances. "Short" is helpful in limiting the display of locks in large sites.'
- Performance:** A dropdown menu set to 'Normal'. Below it, a note states: 'This setting affects frequency of credential scan, with modest impact to battery life.'

At the bottom, there is a note: 'Changes made to any offline locks will require manual door file update.' and a 'Save' button.

Fig. 10.31: Control Default Settings

**Table 10.2: 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	<ul style="list-style-type: none"> <li>ON: Lock will accept Mobile Credential access and the following options are available.</li> <li>OFF: Mobile Credential use is disabled</li> </ul>
Communication Range	<p>Enables the Schlage Mobile Credential application to find locks from short or longer distances.</p> <p>➔ <b>Note:</b> This is a PACS only feature. This setting has no effect on ENGAGE accounts.</p>
Performance	<p>This setting effects how often the device scans for a Mobile Credential.</p> <ul style="list-style-type: none"> <li>Normal: Default</li> <li>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.</li> </ul>

## CTE

Fig. 10.32: CTE Default Settings

Table 10.3: CTE Device Property Wide Settings

Setting	Description
Beeper Enabled	<ul style="list-style-type: none"> <li>ON: the lock beeper will sound to provide device status.</li> <li>OFF: the lock beeper will remain silent.</li> </ul>
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	<ul style="list-style-type: none"> <li>ON (enabled): the Propped Door Delay selection is required.</li> <li>OFF: the following option is not available</li> </ul> <p>→ <b>Note:</b> The setting applies ONLY to devices that support Door Position Sensor (DPS) for Propped Door Audits.</p>
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	<ul style="list-style-type: none"> <li>ON: lock will accept Mobile Credential access and the following options are available.</li> <li>OFF: Mobile Credential use is disabled</li> </ul>
Communication Range	<p>Enables the Schlage Mobile Credential application to find locks from short or longer distances.</p> <p>→ <b>Note:</b> This is a PACS only feature. This setting has no effect on ENGAGE accounts</p>
Anti-Tailgate	<ul style="list-style-type: none"> <li>OFF: no special action is taken, the device relocks on the normal relock schedule.</li> <li>ON: the CTE will use the DPS sensor to immediately relock when the door closes and terminate the relocking period upon closure.</li> </ul>
DPS Enabled	<ul style="list-style-type: none"> <li>OFF: use when no DPS is installed.</li> <li>ON: the CTE will know that a DPS is installed and can enable the Door Propped and Anti-tailgate features.</li> </ul>



## LE and LEB

The screenshot shows the 'LE' settings page. The left sidebar has a menu with 'LE' selected. The main content area lists the following settings:

- Beeper Enabled:** Toggle switch set to ON.
- Relock Delay (seconds):** Dropdown menu set to 3.
- ADA Relock Delay (seconds):** Dropdown menu set to 30.
- Propped Door Delay (seconds):** Dropdown menu set to 20.
- Power Fail Mode:** Dropdown menu set to Secure.
- Blink Interior LED:** Toggle switch set to OFF.
- Blink Interior LED Rapidly:** Toggle switch set to OFF.
- Mobile Credential:** Toggle switch set to ON.
- Communication Range:** Dropdown menu set to Short. Subtext: 'Enables the Mobile Credential App to find locks from further distances. "Short" is helpful in limiting the display of locks in large sites.'
- Performance:** Dropdown menu set to Normal. Subtext: 'This setting affects frequency of credential scan, with modest impact to battery life.'

At the bottom, there is a note: 'Changes made to any offline locks will require manual door file update.' and a 'Save' button.

Fig. 10.33: LE Default Settings

Table 10.4: LE and LEB Device Property Wide Settings

Setting	Description
Beeper Enabled	<ul style="list-style-type: none"> <li>ON: the lock beeper will sound to provide device status.</li> <li>OFF: the lock beeper will remain silent.</li> </ul>
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. <ul style="list-style-type: none"> <li>Secure : Locked</li> <li>Passage: Unlocked</li> <li>AS IS: no change</li> </ul>
Blink Interior LED	<ul style="list-style-type: none"> <li>ON: the Interior LED will blink while in Privacy Mode to inform the occupant of the secured status.</li> <li>OFF: default</li> </ul>
Blink Interior LED rapidly	<ul style="list-style-type: none"> <li>ON: increases how often the Inside LED is flashing for better visibility.</li> <li>OFF: default</li> </ul>
Mobile Credential	<ul style="list-style-type: none"> <li>OFF: Mobile Credential use is disabled.</li> <li>ON: lock will accept Mobile Credential access and the following options are available.</li> </ul>
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. <p>➔ <b>Note:</b> This is a PACS only feature. This setting has no effect on ENGAGE accounts.</p>
Performance	Affects how often the device scans for a Mobile Credential. <ul style="list-style-type: none"> <li>Normal: Default</li> <li>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.</li> </ul>



## NDE80 and NDEB

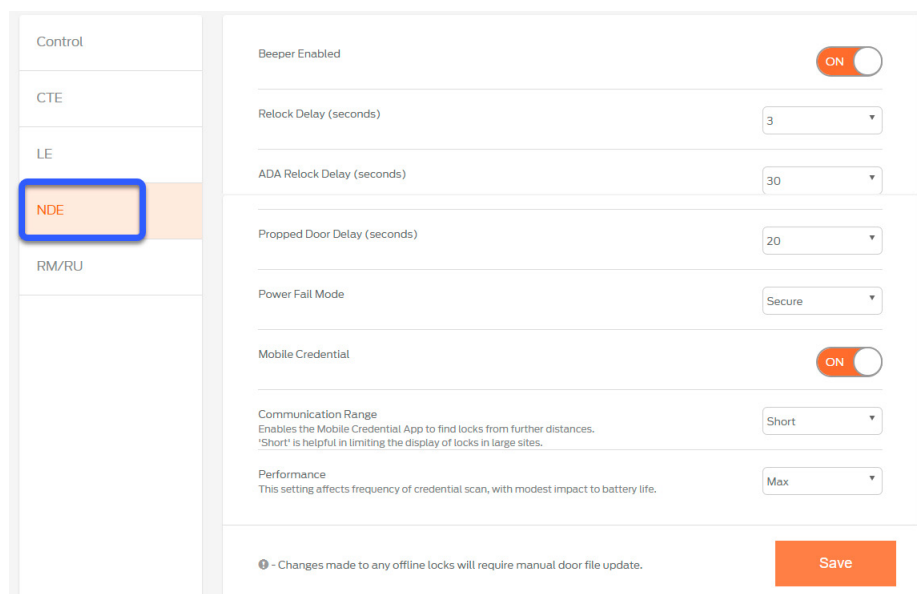


Fig. 10.34: NDE Default Settings

Table 10.5: NDE80 and NEDB Device Property Default Settings	
Setting	Description
Beeper Enabled	<ul style="list-style-type: none"> <li>ON: the lock beeper will sound to provide device status.</li> <li>OFF: the lock beeper will remain silent.</li> </ul>
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. <ul style="list-style-type: none"> <li>Secure : Locked</li> <li>Passage: Unlocked</li> <li>AS IS: no change</li> </ul>
Mobile Credential	<ul style="list-style-type: none"> <li>OFF: Mobile Credential use is disabled.</li> <li>ON: lock will accept Mobile Credential access and the following options are available.</li> </ul>
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. <b>→ Note:</b> 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. <ul style="list-style-type: none"> <li>Normal: Default</li> <li>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.</li> </ul>

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

Control

CTE

LE

NDE

RM/RU

Beeper Enabled

ON

Propped Door Delay (seconds)

20

- Changes made to any offline locks will require manual door file update.

Save

Fig. 10.35: RU/RM Default Settings

Table 10.6: RU/RM Device Property Default Settings	
Setting	Description
Beeper Enabled	<ul style="list-style-type: none"><li>• ON: the lock beeper will sound to provide device status.</li><li>• OFF: the lock beeper will remain silent.</li></ul>
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.

→ **Note:** Reader Default settings apply to LE, NDE, and Multi-Technology Reader product families. The MT20 and MT20W credential enrollment readers will read any compatible credential and therefore, do not have Reader Default settings.

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

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Select **Advanced** menu then **Reader Defaults** tab.
3. Adjust as needed and click **Save**.

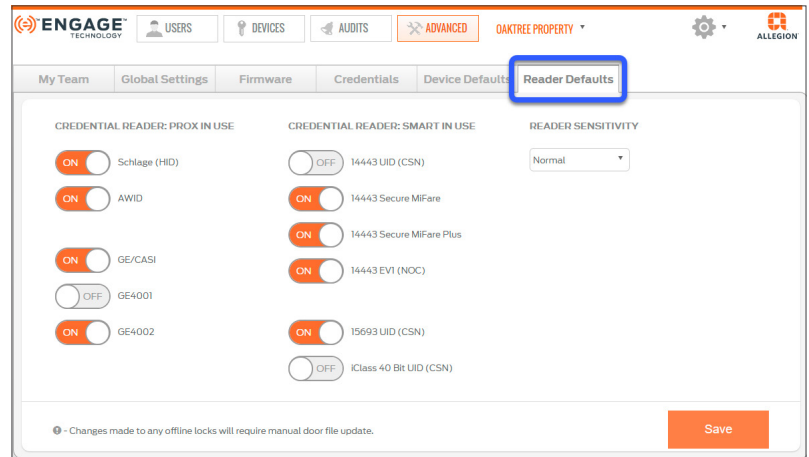


Fig. 10.36: Advanced > Reader Defaults

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.

## Individual 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.

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Select the **Devices** menu and the **Devices** pull down.
3. Select a previously commissioned device from the device list.
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.

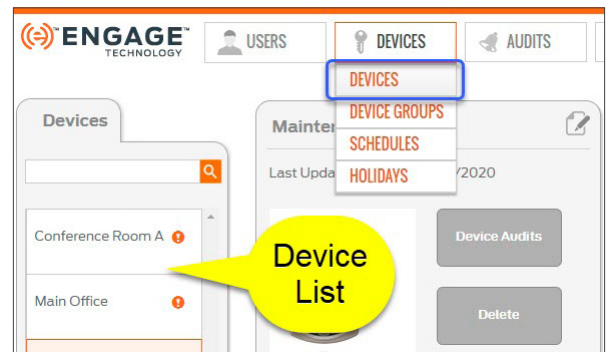


Fig. 10.37: Devices > Devices

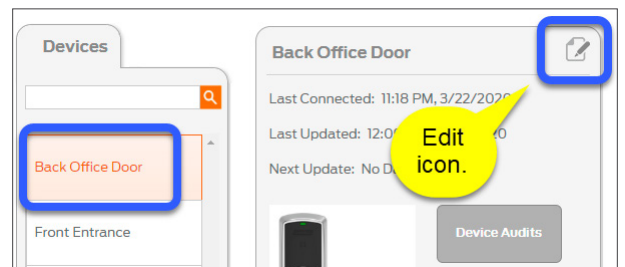


Fig. 10.38: Edit Individual Device

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.

The screenshot shows the 'Settings' tab of the Control Mobile Enabled Smart Lock interface. The 'Settings' tab is selected and highlighted with a blue box. The interface is divided into three sections: Properties, Relock Delay, and Additional Settings. The Properties section contains fields for Model (BE467B), Serial Number (E20000000055485), and Name (Maintenance Office). The Relock Delay section contains a dropdown menu set to 3 seconds. The Additional Settings section contains a toggle switch for Beeper Enabled, which is currently turned on. At the bottom of the interface, there are two buttons: Save (orange) and Cancel (blue).

Fig. 10.39: Control Individual Settings

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

The screenshot shows the 'Mobile Credential' tab of the Control Mobile Enabled Smart Lock interface. The 'Mobile Credential' tab is selected and highlighted with a blue box. The interface shows a toggle switch for Mobile Credential, which is currently turned on. Below this, there are two sections: Communication Range and Performance. The Communication Range section has a dropdown menu set to Short. The Performance section has a dropdown menu set to Normal. At the bottom of the interface, there are two buttons: Save (orange) and Cancel (blue).

Fig. 10.40: Control Mobile Credential Settings

Table 10.7: Control Mobile Enabled Smart Lock Individual Settings	
Setting	Description
<b>Settings Tab</b>	
Name	Device Name
Relock Delay	Immediately after unlocking, set the lock to automatically relock itself between 1 – 30 seconds
Beeper Enabled	<ul style="list-style-type: none"><li>• ON: the lock beeper will sound to provide device status.</li><li>• OFF: the lock beeper will remain silent</li></ul>
<b>Mobile Credential Tab</b>	
Mobile Credential	<ul style="list-style-type: none"><li>• OFF: Mobile Credential use is disabled</li><li>• ON: lock will accept Mobile Credential access</li></ul>
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances  → <b>Note:</b> 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. <ul style="list-style-type: none"><li>• Normal: Default</li><li>• 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.</li></ul>

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.

SettingsReaderMobile Credential

Properties:  
Model: LEBMS  
Serial Number: F2000000F143F8C  
Name: Main Office  
Function: Storeroom  
  
LE Series Storeroom Lock:  
The lock is normally secure. A valid credential will change the state of the lock depending on the credential function (Normal, Toggle, etc.). The inside lever will always unlock the door. A mechanical key will momentarily unlock the door.

Relock Delay:  
Immediately after unlocking, the lock should automatically relock itself in:  
3 Seconds  
Except for an ADA enabled credential which will automatically relock in:  
30 Seconds  
Record Propped Door Audit After:  
20 Seconds  
Power Fail Mode:  
If the batteries fail:  
Lock the door

Schedules:  
None Assigned  
"First-Person-in" Unlocks Door  
Holidays:  
None Assigned  
Additional Settings:  
Beeper Enabled  
Blink Interior LED when Locked  
Blink Interior LED rapidly

SaveCancel

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.

SettingsReaderMobile Credential

CREDENTIAL READER: PROX IN USE  
Schlage (HID)  
AWID  
GE/CASI  
GE4001  
GE4002

CREDENTIAL READER: SMART IN USE  
14443 UID (CSN)  
14443 Secure MiFare  
14443 Secure MiFare Plus  
14443 EV1 (NOC)  
15693 UID (CSN)  
iClass 40 Bit UID (CSN)

READER SENSITIVITY  
High

SaveCancel

SettingsReaderMobile Credential

Mobile Credential  
Communication Range:  
Enables the Mobile Credential App to find locks from further distances. 'Short' is helpful in limiting the display of locks in large sites.  
Short  
Performance:  
This setting affects frequency of credential scan, with modest impact to battery life.  
Max

SaveCancel

Fig. 10.41: LE Individual Settings

**Table 10.8: LE and LEB Device Settings**

Setting	Description
Name	The name of the device
<b>Settings Tab</b>	
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. <ul style="list-style-type: none"> <li>Secure : Locked</li> <li>AS IS: no change</li> <li>Passage: Unlocked</li> </ul>
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	<ul style="list-style-type: none"> <li>ON: the lock beeper will sound to provide device status.</li> <li>OFF: the lock beeper will remain silent</li> </ul>
Blink Interior LED	Requires a DPS sensor and Privacy or Apartment lock functions. <ul style="list-style-type: none"> <li>ON: LED on the inside of the device to blink while the door is locked and closed</li> <li>OFF: default</li> </ul>
Blink Interior LED rapidly	Requires a DPS sensor and Privacy or Apartment lock functions <ul style="list-style-type: none"> <li>ON: increases how often the Inside LED is flashing for better visibility.</li> <li>OFF: default</li> </ul>
<b>Reader Tab</b>	
Credential Reader: Prox in Use	Choose the technology used by readers in your site: <ul style="list-style-type: none"> <li>Schlage (HID)</li> <li>GE4001</li> <li>AWID</li> <li>GE4002</li> <li>GE/CASI</li> </ul>
Credential Reader: Smart in Use	Choose the technology used by readers in your site: <ul style="list-style-type: none"> <li>14443 UID (CSN)</li> <li>14443 EV1 (NOC)</li> <li>14443 Secure MiFare</li> <li>15693 UID (CSN)</li> <li>14443 Secure MiFare Plus</li> <li>iClass 40 Bit UID (CSN)</li> </ul>
Reader Sensitivity	<ul style="list-style-type: none"> <li>Set to Normal by default and is recommended for most properties.</li> <li>Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.</li> </ul>
<b>Mobile Credential Tab</b>	
Mobile Credential	<ul style="list-style-type: none"> <li>OFF: Mobile Credential use is disabled.</li> <li>ON: lock will accept Mobile Credential access</li> </ul>
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. <p>➔ <b>Note:</b> This is a PACS only feature. This setting has no effect on ENGAGE accounts.</p>
Performance	Affects how often the device scans for a Mobile Credential. <ul style="list-style-type: none"> <li>Normal: Default</li> <li>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.</li> </ul>

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.

Settings

Reader

Mobile Credential

Properties:

Model: NDEB

Serial Number: A20000000F14863F

Name: Mail Room

Function: Storeroom

NDE Series Storeroom Lock:

The lock is normally secure. A valid credential will change the state of the lock depending on the credential function (Normal, Toggle, etc.). The inside lever will always unlock the door. A mechanical key will momentarily unlock the door.

Relock Delay:

Immediately after unlocking, the lock should automatically relock itself in:

3 Seconds

Except for an ADA enabled credential which will automatically relock in:

30 Seconds

Record Propped Door Audit After:

20 Seconds

Power Fail Mode:

If the batteries fail:

Lock the door

Schedules:

None Assigned

☐ "First-Person-in" Unlocks Door

Holidays:

None Assigned

Additional Settings:

ON

Beeper Enabled

Save

Cancel

Settings

Reader

Mobile Credential

CREDENTIAL READER: PROX IN USE

ON

Schlage (HID)

ON

AWID

ON

GE/CASI

OFF

GE4001

ON

GE4002

CREDENTIAL READER: SMART IN USE

OFF

14443 UID (CSN)

ON

14443 Secure MiFare

ON

14443 Secure MiFare Plus

ON

14443 EV1 (NOC)

ON

15693 UID (CSN)

ON

iClass 40 Bit UID (CSN)

READER SENSITIVITY

High

Save

Cancel

Settings

Reader

Mobile Credential

ON

Mobile Credential

Communication Range:

Enables the Mobile Credential App to find locks from further distances. 'Short' is helpful in limiting the display of locks in large sites.

Short

Performance:

This setting affects frequency of credential scan, with modest impact to battery life.

Max

Save

Cancel

Fig. 10.42: NDEB Individual Settings



**Table 10.9: NDE80 and NDEB Device Settings**

Setting	Description
<b>Settings Tab</b>	
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. <ul style="list-style-type: none"> <li>Secure : Locked</li> <li>AS IS: no change</li> <li>Passage: Unlocked</li> </ul>
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	<ul style="list-style-type: none"> <li>ON: the lock beeper will sound to provide device status.</li> <li>OFF: the lock beeper will remain silent</li> </ul>
<b>Reader Tab</b>	
Credential Reader: Prox in Use	Choose the technology used by readers in your site: <ul style="list-style-type: none"> <li>Schlage (HID)</li> <li>GE4001</li> <li>AWID</li> <li>GE4002</li> <li>GE/CASI</li> </ul>
Credential Reader: Smart in Use	Choose the technology used by readers in your site: <ul style="list-style-type: none"> <li>14443 UID (CSN)</li> <li>14443 EV1 (NOC)</li> <li>14443 Secure MiFare</li> <li>15693 UID (CSN)</li> <li>14443 Secure MiFare Plus</li> <li>iClass 40 Bit UID (CSN)</li> </ul>
Reader Sensitivity	<ul style="list-style-type: none"> <li>Set to Normal by default and is recommended for most properties.</li> <li>Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.</li> </ul>
<b>Mobile Credential Tab</b>	
Mobile Credential	<ul style="list-style-type: none"> <li>OFF: Mobile Credential use is disabled.</li> <li>ON: lock will accept Mobile Credential access</li> </ul>
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. <p>➔ <b>Note:</b> This is a PACS only feature. This setting has no effect on ENGAGE accounts.</p>
Performance	Affects how often the device scans for a Mobile Credential. <ul style="list-style-type: none"> <li>Normal: Default</li> <li>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.</li> </ul>

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 product family.

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

CTE

Adjust as needed and Save to apply changes.

SettingsReaderMobile Credential

Properties:

Model: CTE

Serial Number: 2100000000001EBD

Name: Front Entrance

Function: Storeroom

CTE Series Storeroom Device:  
The device is normally secure. A valid credential will change the state of the device depending on the credential function (Normal, Toggle, etc.).

Relock Delay:

Immediately after unlocking, the lock should automatically relock itself in:

3 Seconds

Except for an ADA enabled credential which will automatically relock in:

30 Seconds

Propped Door Trigger:

OFF

Propped Door Trigger Enabled

When enabled, record an audit when this door has been open for the following duration:

20 Seconds

Schedules:

None Assigned

☐ "First-Person-in" Unlocks Door

Holidays:

None Assigned

Additional Settings:

ON

Beeper Enabled

OFF

Anti-Tailgate (immediate relock on door close)

OFF

DPS Enabled

Save

Cancel

SettingsReaderMobile Credential

CREDENTIAL READER: PROX IN USE

ON

Schlage (HID)

ON

AWID

ON

GE/CASI

OFF

GE4001

ON

GE4002

CREDENTIAL READER: SMART IN USE

OFF

14443 UID (CSN)

ON

14443 Secure MiFare

ON

14443 Secure MiFare Plus

ON

14443 EV1 (NOC)

ON

15693 UID (CSN)

ON

iClass 40 Bit UID (CSN)

READER SENSITIVITY

High

Save

Cancel

SettingsReaderMobile Credential

ON

Mobile Credential

Communication Range:

Enables the Mobile Credential App to find locks from further distances. 'Short' is helpful in limiting the display of locks in large sites.

Short

Save

Cancel

Fig. 10.43: CTE Individual Settings

**Table 10.10: CTE Device Settings**

Setting	Description
<b>Settings Tab</b>	
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	<ul style="list-style-type: none"> <li>ON (enabled): the Propped Door Delay selection is required.</li> <li>OFF: the following option is not available</li> </ul> <b>→ Note:</b> 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	<ul style="list-style-type: none"> <li>ON: the lock beeper will sound to provide device status.</li> <li>OFF: the lock beeper will remain silent</li> </ul>
Anti-Tailgate	<ul style="list-style-type: none"> <li>OFF: no special action is taken, the device relocks on the normal relock schedule.</li> <li>ON: the CTE will use the DPS sensor to immediately relock when the door closes and terminate the relocking period upon closure.</li> </ul>
DPS Enabled	<ul style="list-style-type: none"> <li>OFF: use when no DPS is installed.</li> <li>ON: the CTE will know that a DPS is installed and can enable the Door Propped and Anti-tailgate features.</li> </ul>
<b>Reader Tab</b>	
Credential Reader: Prox in Use	Choose the technology used by readers in your site: <ul style="list-style-type: none"> <li>Schlage (HID)</li> <li>GE4001</li> <li>AWID</li> <li>GE4002</li> <li>GE/CASI</li> </ul>
Credential Reader: Smart in Use	Choose the technology used by readers in your site: <ul style="list-style-type: none"> <li>14443 UID (CSN)</li> <li>14443 EV1 (NOC)</li> <li>14443 Secure MiFare</li> <li>15693 UID (CSN)</li> <li>14443 Secure MiFare Plus</li> <li>iClass 40 Bit UID (CSN)</li> </ul>
Reader Sensitivity	<ul style="list-style-type: none"> <li>Set to Normal by default and is recommended for most properties.</li> <li>Use a Reader Sensitivity of High or Max to enable a more reliable reading of physically smaller key fobs due to smaller antenna.</li> </ul>
<b>Mobile Credential Tab</b>	
Mobile Credential	<ul style="list-style-type: none"> <li>OFF: Mobile Credential use is disabled.</li> <li>ON: lock will accept Mobile Credential access</li> </ul>
Communication Range	Enables the Schlage Mobile Credential application to find locks from short or longer distances. <b>→ Note:</b> This is a PACS only feature. This setting has no effect on ENGAGE accounts.

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.

When commissioning the Schlage MT20W or Control Mobile Enabled Smart Lock, the No-Tour feature is automatically enabled within the ENGAGE web application

## No-Tour 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.

To take advantage of the No-Tour feature, the administrator will program a physical credential in their office with new or changed access rights and have the programmed credential make the changes at the affected door(s) when the credential is presented by the user for normal access.

Access right updates can always be accomplished through the normal Sync process when No-Tour is not used or when device configuration is also being adjusted.

When access updates are needed, Administrators should take advantage of the No-Tour feature.

**WARNING:** The No-Tour feature **will not** update device settings like relock delays, schedule updates, or beeper ON/OFF. Only access updates may be accomplished using the No-Tour feature.

### No-Tour Limitations

Although the No-Tour feature saves time and effort during daily operations, it does have some limitations.

No-Tour items to keep in mind include:

- Only access right updates (additions/deletions) can be accomplished using the No-Tour.
- Lost credentials: Access updates to DELETE the credential should be accomplished by the Administrator using the Sync process to guarantee the credential is removed from all affected devices.
- Any Device settings like relock delay or schedule changes are **never** transferred to the devices when using No-Tour
- No-Tour credentials are limited to 11 door access programming at any time.
- When more than 11 door assignments are needed, the Administrator should use "Door Groups" for common area doors, that group the doors together and use only one door assignment.

## ENGAGE Mobile Application

### Overview

The ENGAGE Mobile Application is used to commission, program and update a property with ENGAGE enabled devices. Use the ENGAGE 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.

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.

The Mobile application is available as a free download from either the iTunes App Store (iOS) or the Google Play Store (Android).

- iOS devices: [ENGAGE Mobile app - iTunes App Store](#)
- Android devices: [ENGAGE Mobile app - Google Play Store](#)

**⚠ CAUTION:** Mobile devices including Tablets 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)

**Table 10.11** describes how the functions within the ENGAGE web and ENGAGE Mobile applications can be shared.

<b>Table 10.11: Web and Mobile Application Functions</b>		
<b>Function</b>	<b>ENGAGE Web</b>	<b>ENGAGE Mobile</b>
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

### Mobile Devices

Use of the ENGAGE System requires the use of a Mobile device to communicate with the ENGAGE devices. Mobile phones and tablets with Bluetooth and cell access work well for this application.

While it is impossible to keep up with all the different Mobile devices and the latest operating software versions, Allegion endeavors to make our systems compatible with the widest variety of Mobile devices possible.

Using the newest “Flagship” Mobile devices is recommended for optimum functionality and robust performance when using any ENGAGE products.

The ENGAGE Mobile Application software is available free on the standard “Application Store” sites. ENGAGE requires the following Mobile device software operating systems:

- iPhone – 11.1 and above
- Android – 6.0 and above

# Installation and Commissioning

This section emphasizes some common ENGAGE device installation issues the Administrator and installation personnel will want to pay close attention to during the initial product installation. Additionally, the Commissioning process for each ENGAGE enable device is provided.

The Administrator will use the standard Door Preparation Templates and Product Installation Instructions provided with the product (In the box) for installation details and to perform the actual installation.

Some specific notes and places where installers have had concerns to be aware of are presented here for clarity.

The links below are provided for quick reference to the individual ENGAGE product offerings. Select a link to go to the Allegion web site for more product details.

**Table 11.1: Device Installation Guides**

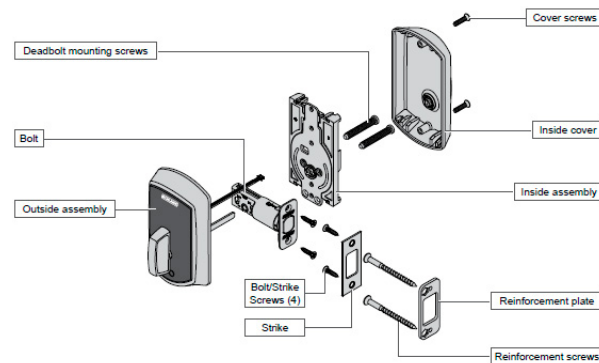
Device	Links to Allegion Product Information
Schlage Control Mobile Enabled Smart Lock	Deadbolt and Interconnect <a href="https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-control-wireless.html">https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-control-wireless.html</a>
Schlage LE and LEB Wireless Mortise Lock	LE Standalone Wireless Mortise: <a href="https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-le-wireless-lock-standalone.html">https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-le-wireless-lock-standalone.html</a> LE Networked Wireless Mortise: <a href="https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-LE-wireless-lock-networked.html">https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-LE-wireless-lock-networked.html</a>
Schlage NDE and NDEB Wireless Cylindrical Lock	NDE Standalone Wireless: <a href="https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-nde-wireless-lock-standalone.html">https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-nde-wireless-lock-standalone.html</a> NDE Networked Wireless: <a href="https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-NDE-wireless-lock-networked.html">https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-NDE-wireless-lock-networked.html</a>
Schlage CTE with Multi-Tech Rdr MT11 MTB11-RS485, MT15 MTB15-RS485	CTE: <a href="https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-cte.html">https://us.allegion.com/en/home/products/categories/electronic-locks/schlage-cte.html</a> Multi-Technology Readers <a href="https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html">https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html</a>
Schlage MT20W Enrollment Rdr	MT20W: <a href="https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html">https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html</a>
Schlage MT20 Enrollment Reader	MT20: <a href="https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html">https://us.allegion.com/en/home/products/categories/readers/schlage-multi-technology-readers.html</a>

## Control Mobile Enabled Smart Lock

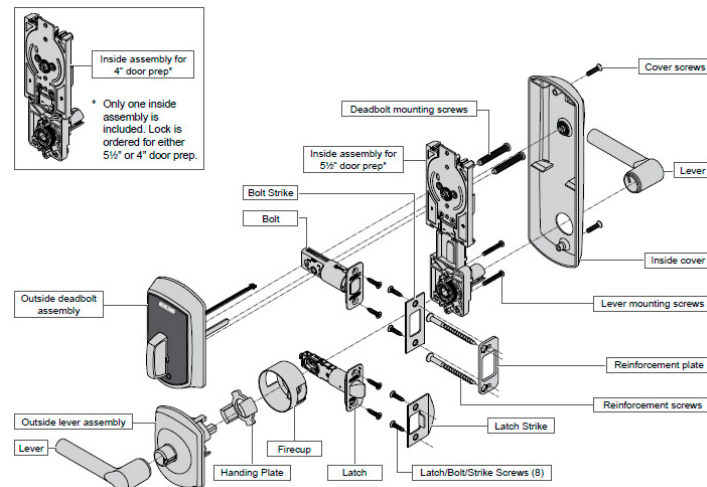
### Device Introduction

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

**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.



**Fig. 11.1: Control Mobile Enabled Smart Lock – exploded view**



**Fig. 11.2: Control Mobile Enabled Smart Interconnected Lock - exploded view**

**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.

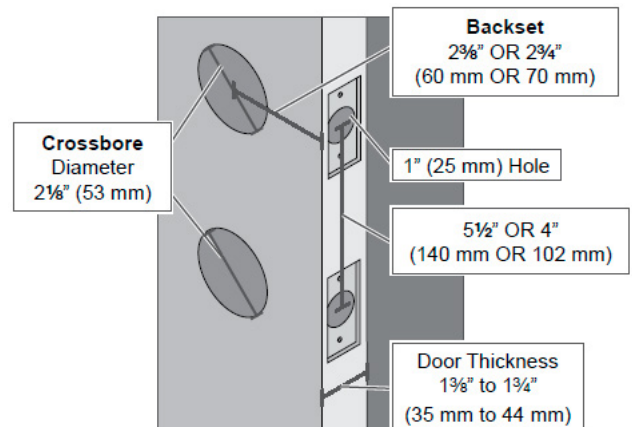


Fig. 11.3: Interconnect Door Prep requirements

**Install the Device**

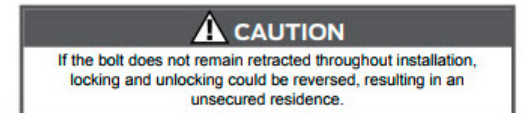
Install the Schlage Control Mobile Enabled Smart Lock as directed in the installation instructions provided in the box.

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.

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



2a Install the outside assembly on the outside of the door.

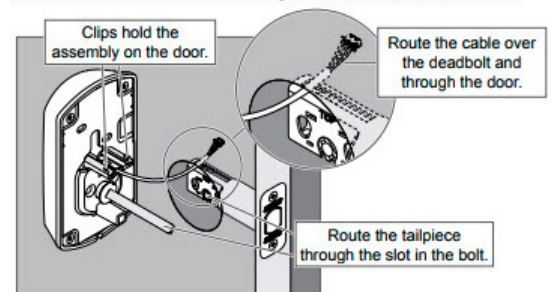
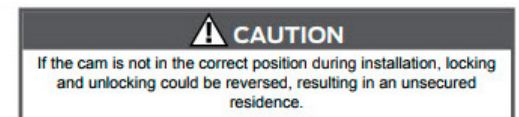


Fig. 11.4: Outside Assembly

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.



3a Make sure the cam on the inside assembly is in the correct position.

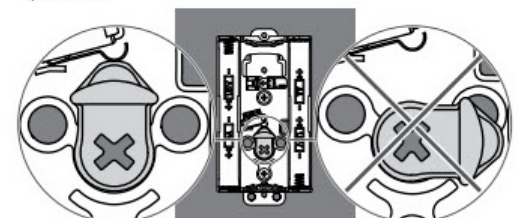


Fig. 11.5: Cam Position



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

3d Connect the cable to the inside assembly.

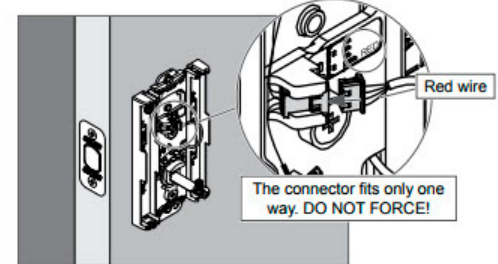


Fig. 11.6: Electrical Connection

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.

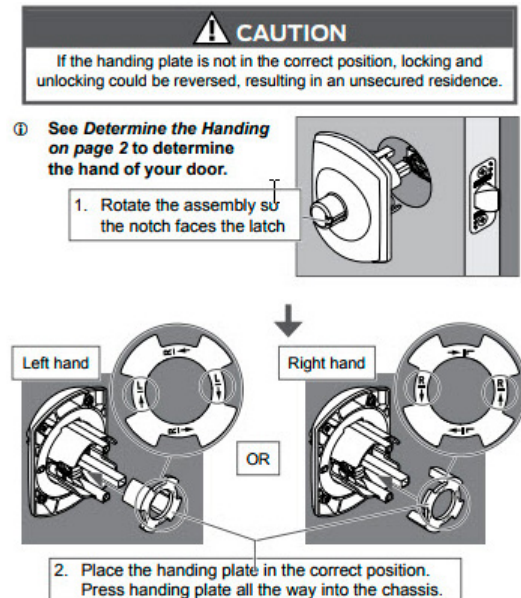


Fig. 11.7: Handing Plate

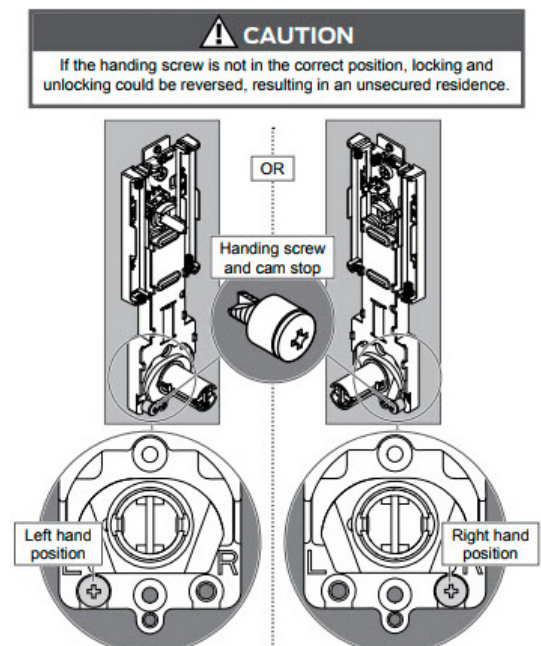


Fig. 11.8: Handing Screw



## Factory Default Reset (FDR) Overview

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.

## Perform a Factory Default Reset (FDR)

1. Remove inside cover.
2. Disconnect at least 1 battery for 10 seconds.
3. Reconnect batterie(s).
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. 11.9: Interconnect

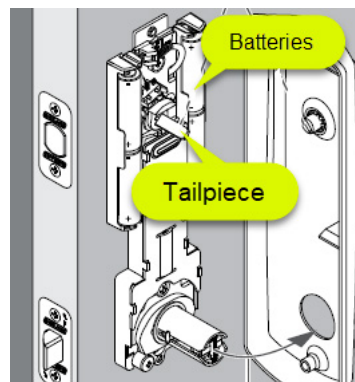
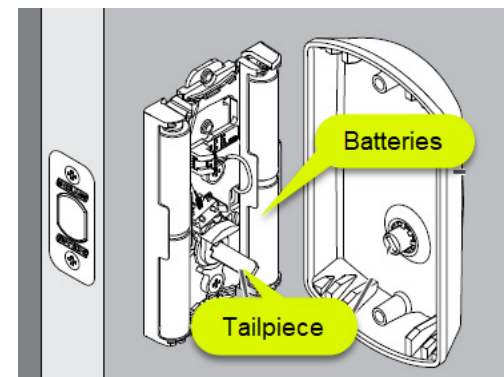


Fig. 11.10: Deadbolt



## 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 Overview

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 the 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.

## Commissioning the Control Mobile Enabled Smart Lock

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
  - **Note:** Depending on the model of your Mobile device (Android or iOS), one of the following screens is presented
  - **Note:** An iPhone device is used in this example for commissioning the Control Mobile Enabled Smart Lock
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.

**WARNING:** Before commissioning a device, Administrators should create any needed schedules and review Property Wide default device settings.

**CAUTION:** When commissioning a Control Mobile Enabled Smart Lock, the ENGAGE No-Tour feature is automatically enabled within the ENGAGE web application

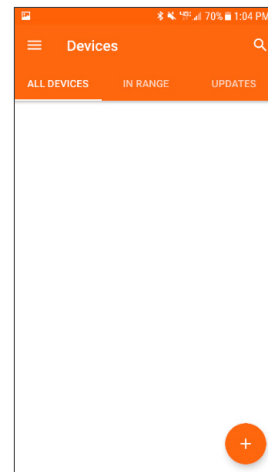


Fig. 11.11: Android Device Menu

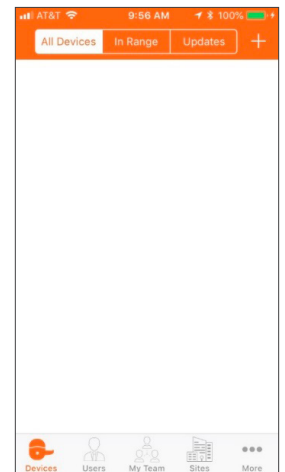


Fig. 11.12: iOS Device Menu

6. **Select** the Control Lock in the "Select a device type" screen.

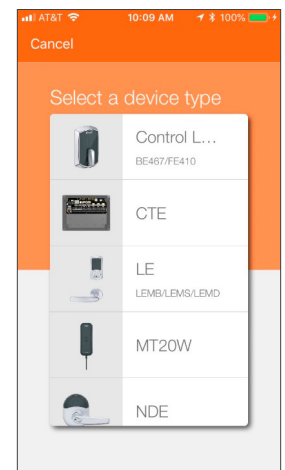


Fig. 11.13: Control Lock Screen

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** (pg. 25) 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
  - We will use the previously defined Schlage Control Mobile Enabled Smart lock default settings.

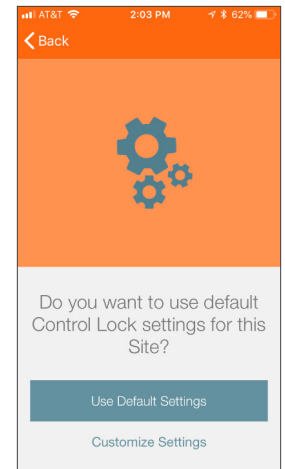


Fig. 11.14: Default or Customize

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.
  - In this case we selected the **Schlage Lock** with serial number **E10000000001B846**.

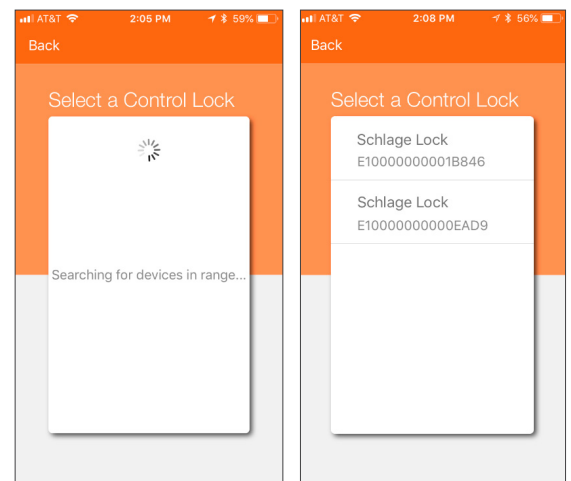


Fig. 11.15: Select a Lock Screens

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**.

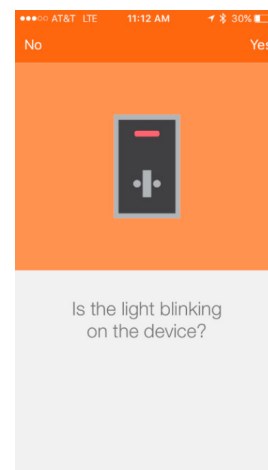


Fig. 11.16: Light blinking screen

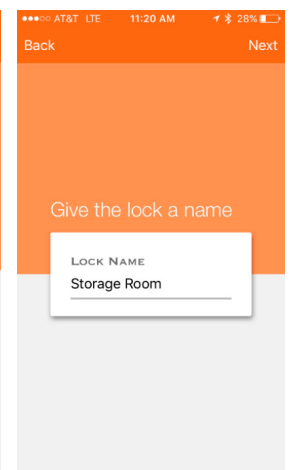


Fig. 11.17: Name Lock screen

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.

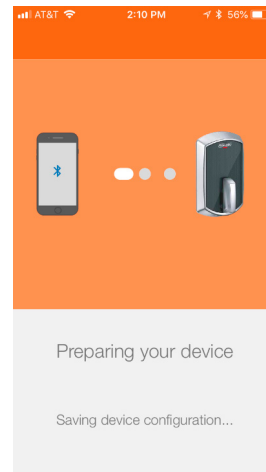


Fig. 11.18: Preparing your device

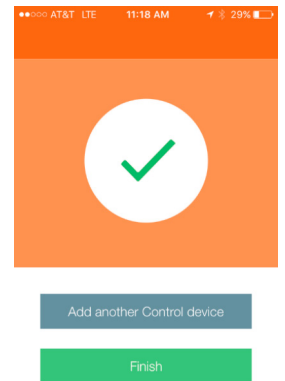


Fig. 11.19: Commission successful

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.

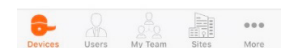
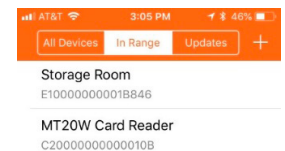


Fig. 11.20: In Range screen

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

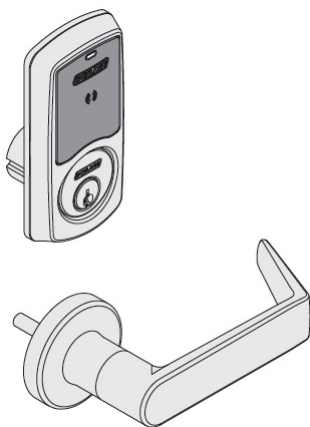
An LE may be updated to an LEB with replacement components, however, no additional door preparation is required.

## LE and LEB ENGAGE Devices

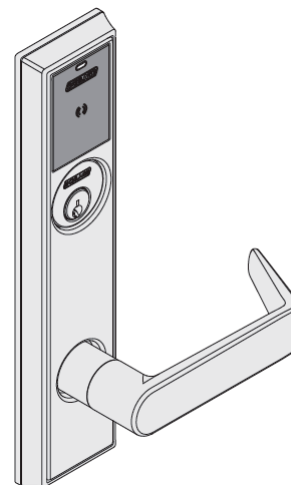
The installation instructions outlined here are excerpts from the Installation Instructions found in the box and highlight the most common issues encountered when installing the device.

Before installing the device, review the Installation Instructions for the Schlage LE or LEB lock contained in the box.

**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. 11.21: LE Wireless Mortise Lock

### Tools Needed:

Phillips screwdriver (#1, #2)

pin wrench

needle-nose pliers

tape measure

### Prepare to Install the Device

1. Verify the door is properly prepared before installation
  2. 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
  3. 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
- **Note:** 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.
- **Note:** It is **RECOMMENDED** you dry fit the chassis into the mortise pocket to verify final fit and adequate wire clearance

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

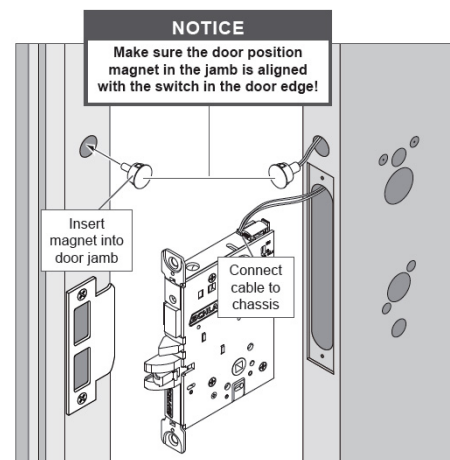


Fig. 11.22: LE/LEB external DPS with Deadbolt

**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.

Rotate the latch 180° (if necessary).

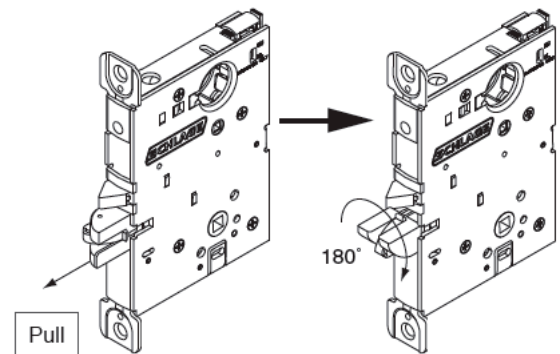


Fig. 11.23: Latch Direction

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

Use pliers carefully to install mounting posts to avoid damage.

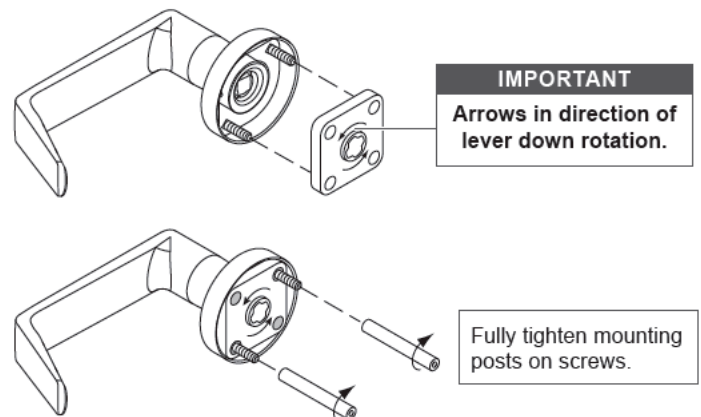


Fig. 11.24: Spring Cage Arrow Direction

- 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.

**NOTICE**  
Handing screw and microswitch must be on the INSIDE of the door.

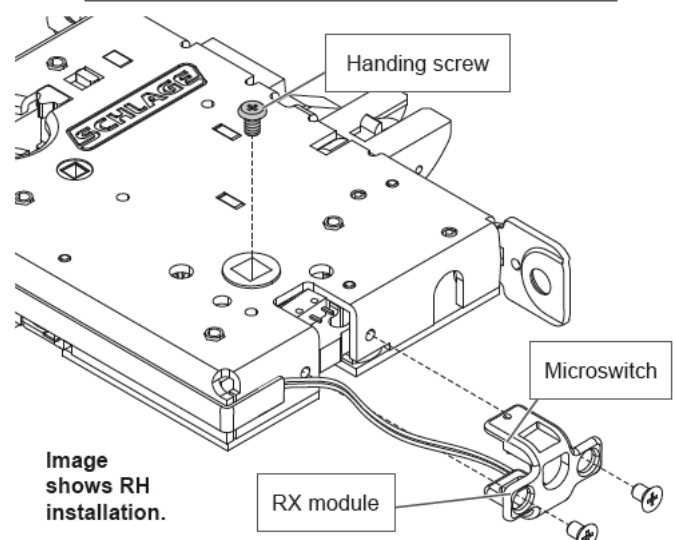


Fig. 11.25: Handing Screw & Microswitch



## 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 Overview

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 Default Device Settings on page 25 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.

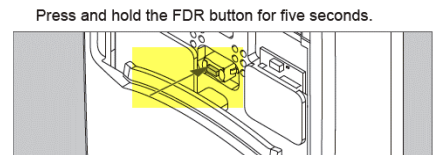


Fig. 11.26: FDR Button

### 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 ENGAGE 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 Overview

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 Default Device Settings on page 25 for more information.



**Construction Access Mode:**

- 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 Default Device Settings on page 25 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.

## Commissioning the LE and LEB Locks

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

- All default Device Settings 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:** The iOS and Android devices have slightly different screen displays however the functions are the same. When devices have been commissioned, this screen will display the name of the commissioned devices.

4. Select the + sign to select the nearby LE or LEB lock being commissioned,
  - a. iOS Mobile device: + sign in the upper right-hand corner.
  - b. Android Mobile device: + sign in the lower right-hand corner.

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** (pg. 25) 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.

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



Fig. 11.27: Android Device Menu

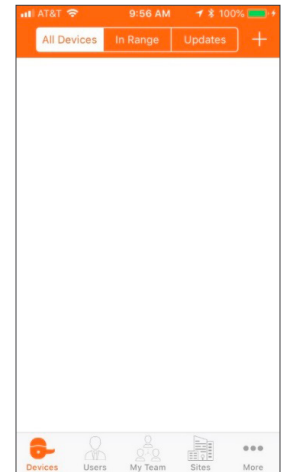


Fig. 11.28: iOS Device Menu

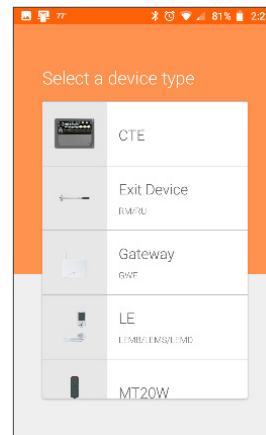


Fig. 11.29: Device Type

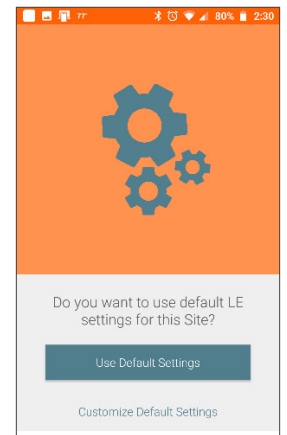


Fig. 11.30: Site Settings

7. Turn and release the inside LE lever to cause the lock to "advertise" its presence with its Bluetooth (BLE) radio.
8. **Select Next.**

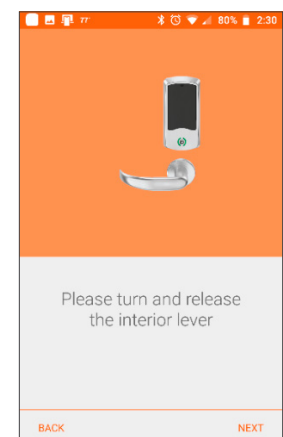


Fig. 11.31: Advertise Presence

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.

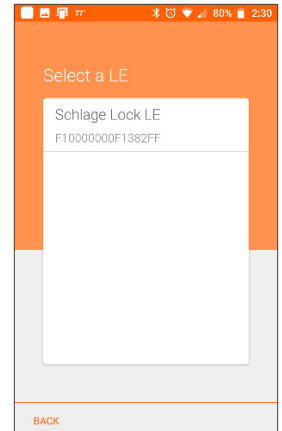


Fig. 11.32: Select LE Device

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 its LED RED.

11. **Select Yes** After verifying the LED is blinking.

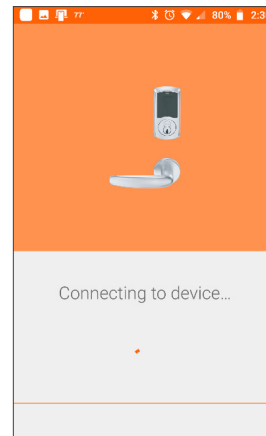


Fig. 11.33: Connecting

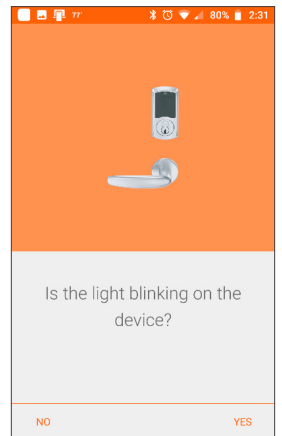


Fig. 11.34: Light Blinking

12. **Enter a descriptive name** for your device under **Device Name**.

- **Storage** is used here

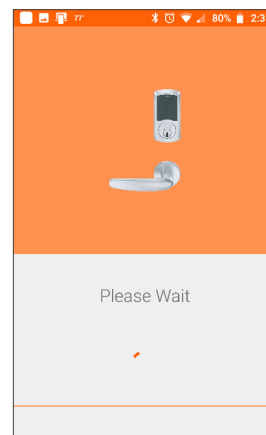


Fig. 11.35: Please Wait

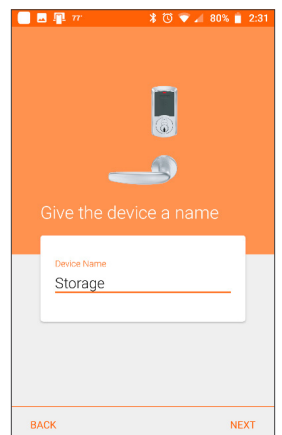


Fig. 11.36: Name Device

## 13. Select the lock function.

- **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 pushbutton 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.

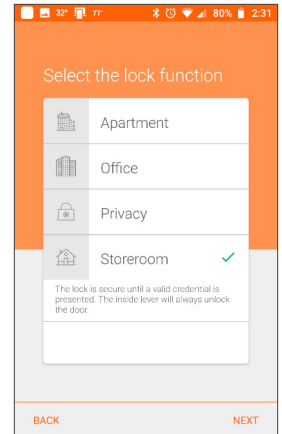


Fig. 11.37: Lock Function

**WARNING:** The Apartment, Office, and Privacy lock functions require the Inside Push Button (IPB) or deadbolt thumbturn to be available for proper operation.

14. Select **Next**.

## 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.
- Only select a **SAVED** network if the network is available at the physical door location.

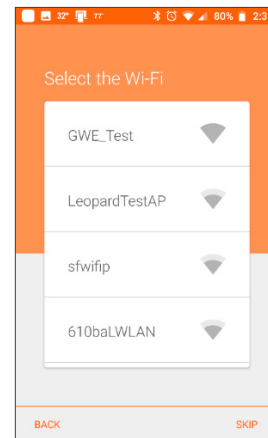


Fig. 11.38: Android Wi-Fi Screen



Fig. 11.39: 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. Refer to Enabling Wi-Fi Network Requirements section 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.

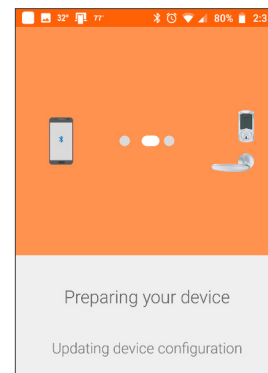


Fig. 11.40: Device Configuration

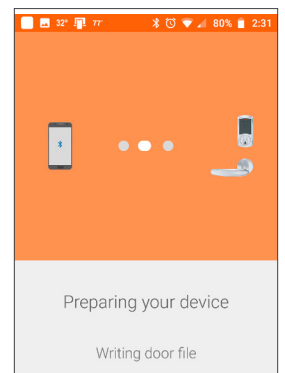


Fig. 11.41: Writing Door File

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.

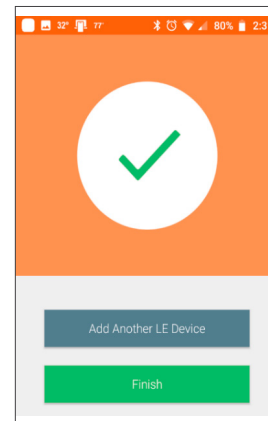


Fig. 11.42: Finish or Add Another

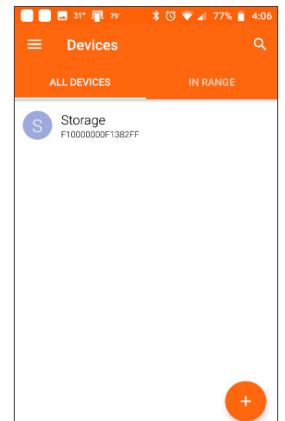


Fig. 11.43: Newly commissioned device

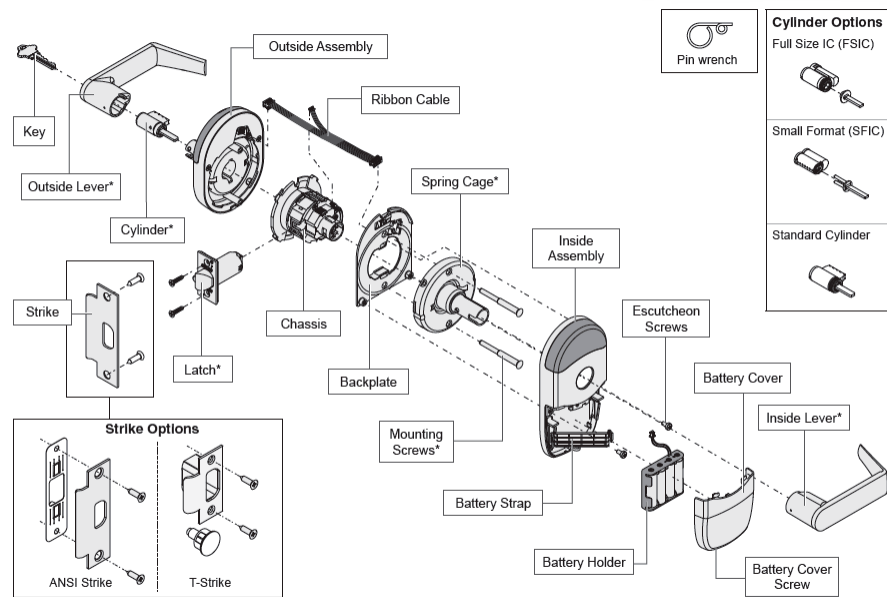
## NDE80 and NDEB ENGAGE Devices

### Device Introduction

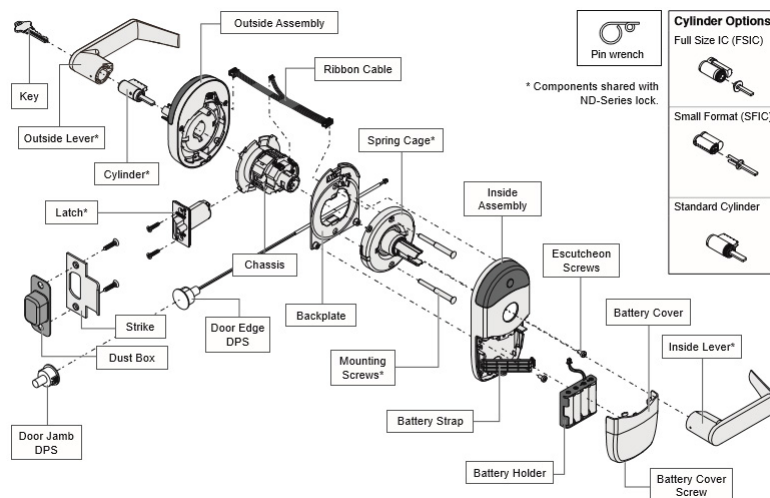
The installation instructions outlined here are excerpts from the devices' Installation Instructions in-the-box and cover the most common issues encountered when installing the device.

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



**Fig. 11.44: NDE80 Wireless Cylindrical Lock exploded view**



**Fig. 11.45: NDEB Wireless Cylindrical Lock exploded view**

**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.**

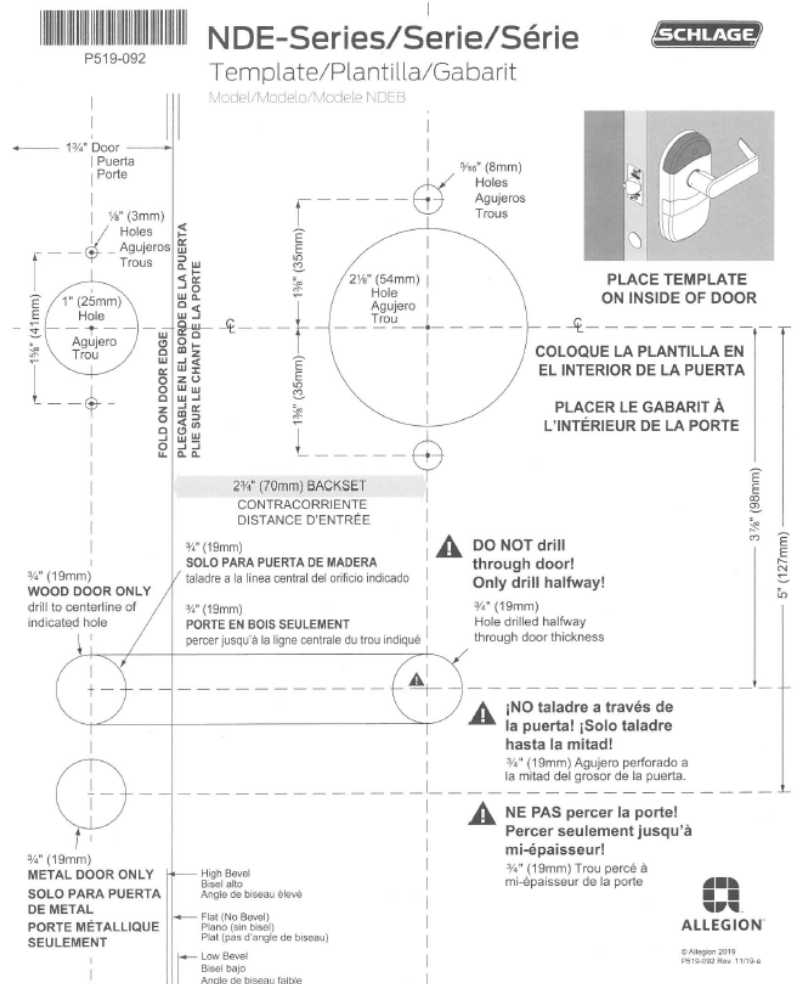
1. Verify the door is properly prepared for the Schlage NDE80 or NDEB installation before attempting to install.

- The Schlage NDE80/NDEB and the mechanical ND locks use the SAME basic door preparation template
- 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



**Fig. 11.46: ND Series Lever Lock door drilling template (NDE80 and NDEB)**

**WARNING: The Centerline of the Latch Bore Hole and the Centerline of the through Door Bore MUST be accurate for proper latch retraction.**



## Install the Device

1. Install the NDE or NDEB as indicated in the Installation Instructions.

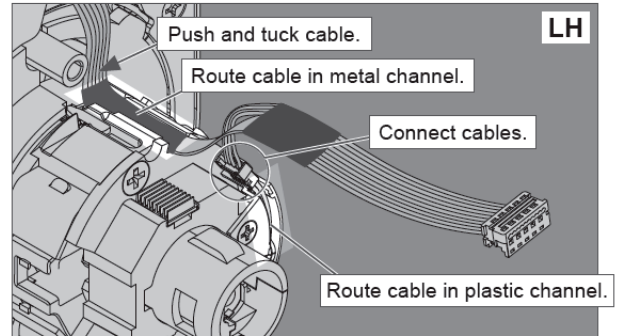
**WARNING:** Ensure cable is routed with no pinching and with both cable connections properly seated in the proper channels.

**CAUTION:** Ensure the installed latch and chassis are properly aligned and fully engaged.

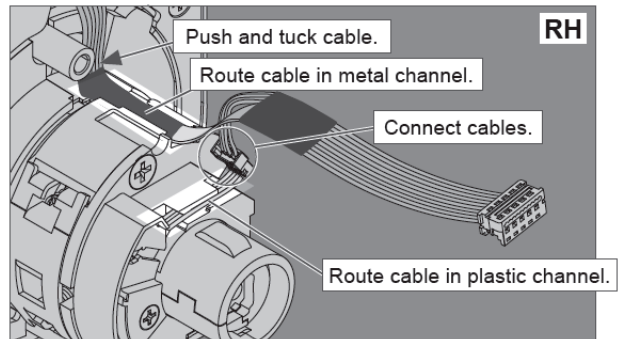
**WARNING:** For non-standard door thickness, carefully follow the door thickness adjustment steps outlined in the Door Thickness Adjustment section.

- 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.



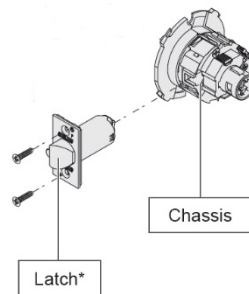
OR



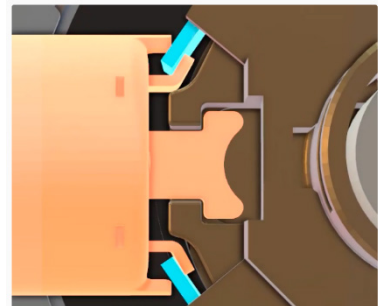
Tuck connected chassis cable into appropriate channel.

Fig. 11.47: Connect Chassis Cables

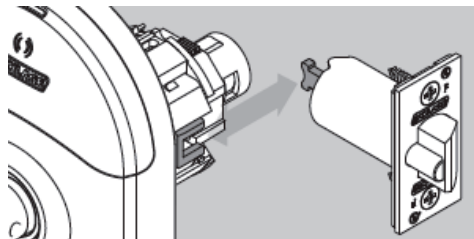
2. Insert the chassis into the installed latch.



4. Align Latch prongs and Chassis slide



3. Check the Latch prongs and the Retractor Slide engagements are properly connected.



**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.

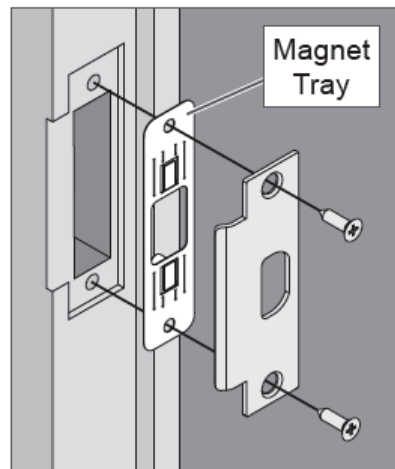
Install the provided standard DPS magnet or install the magnet tray along with the appropriate strike.

→ **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.

**WARNING:** The Door Position Sensor magnet tray or T-Strike magnet **MUST** be installed for proper Door Position sensing and proper calibration during commissioning

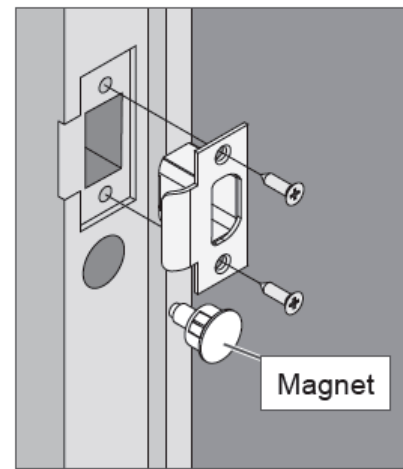
**CAUTION**

Magnet or magnet tray and included strike must be installed! **DO NOT DISCARD!**



ANSI Strike

OR

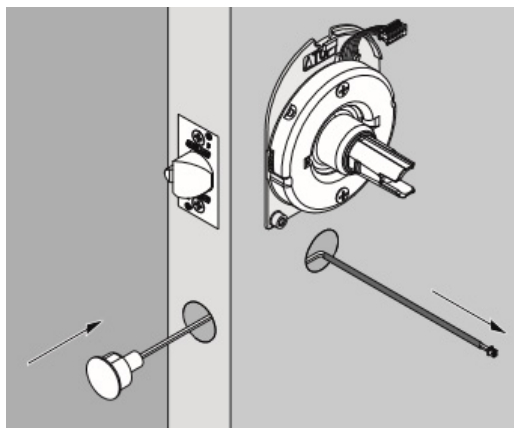


T-Strike

Fig. 11.48: NDE80 Magnet and Strike options

**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.

Connect DPS wire (1), route wire behind tabs (2), and tuck excess wire back into the hole in door (3).

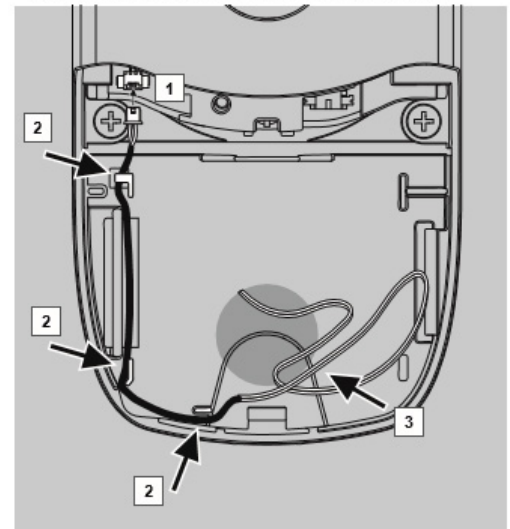


Fig. 11.49: NDEB DPS wire routing

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.

Press and hold the FDR button for five seconds.

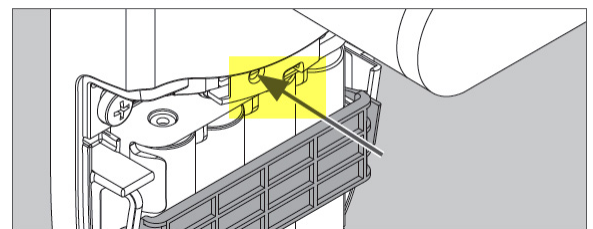


Fig. 11.50: NDE80 or NDEB FDR Button

### 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 **Disable** 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.

## Commissioning the Device

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

- Administrators should define all Schedules and all Default Device Settings 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 Sync 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 ENGAGE Mobile Application.
  3. The blank Devices Menu will appear.
- **Note:** The figures above show that no devices are commissioned into the property as both are blank. When devices have been commissioned, this screen will display the name of the commissioned devices.
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.

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

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

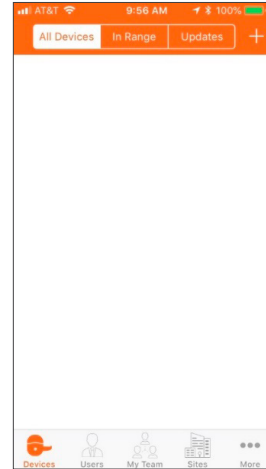


Fig. 11.51: iOS Device Menu

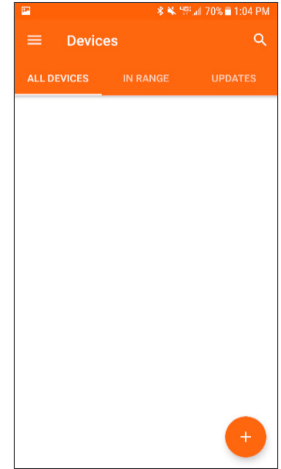


Fig. 11.52: Android Device Menu

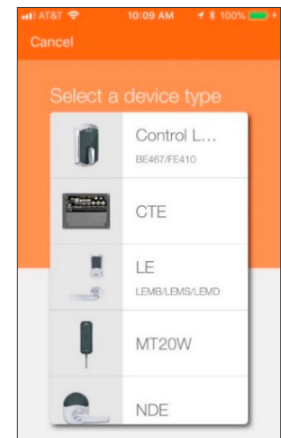


Fig. 11.53: Device Type

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** (pg. 25) 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.
7. Select **Use Default Settings**.

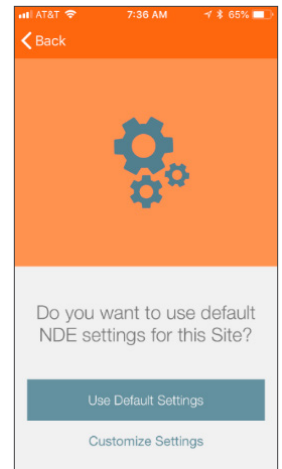


Fig. 11.54: Use Default Settings

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.

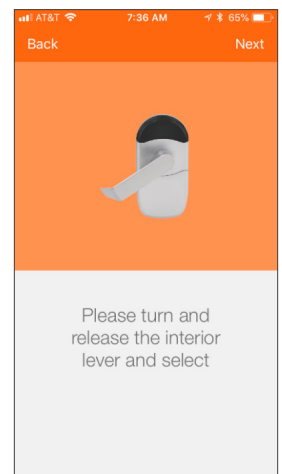


Fig. 11.55: Advertise Presence

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 **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.

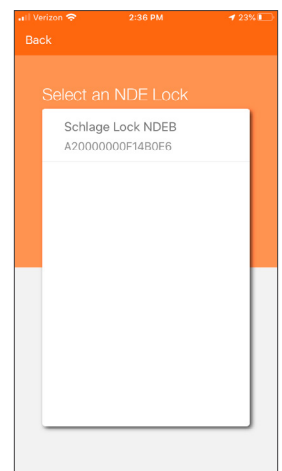


Fig. 11.56: Select the NDEB Device

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

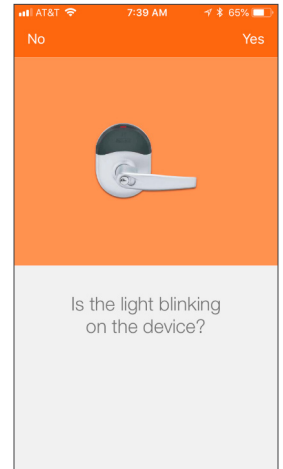


Fig. 11.57: Light Blinking

12. Provide a descriptive name (Main Office) under **Device Name**.  
 13. Select Next.

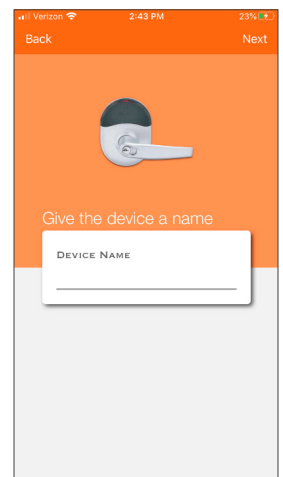


Fig. 11.58: Name Device

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.**  
     → **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.

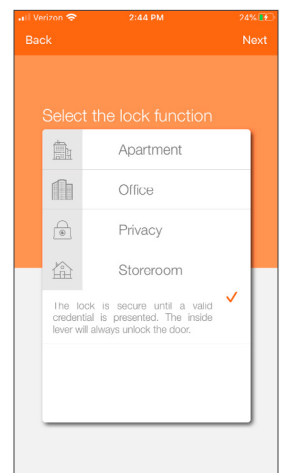
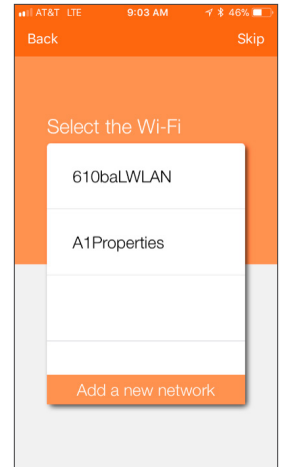


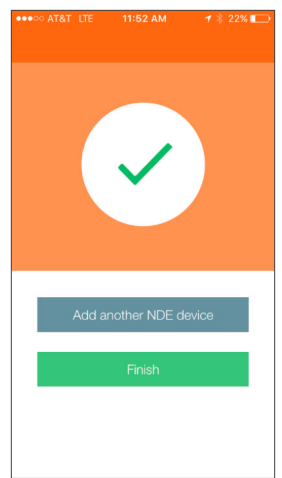
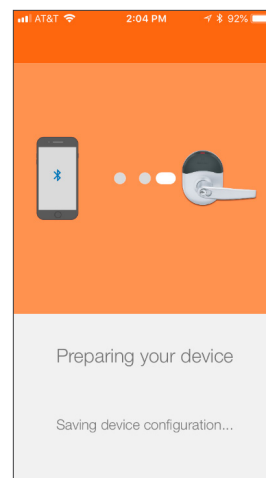
Fig. 11.59: Select the lock function

16. **Select Skip** Let's assume that the property's local Wi-Fi network has not been set up yet and there are no local Wi-Fi network connections available.

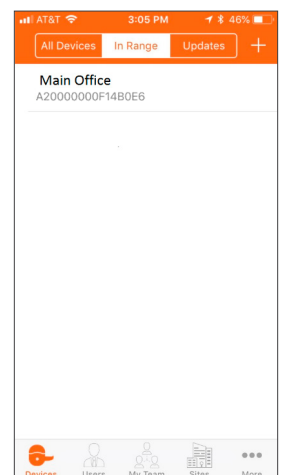
→ **Note:** See **Enabling Wi-Fi Network Connection Settings** for setup requirements when a Wi-Fi network is available, and the Administrator would like to take advantage of the Schlage NDE "Nightly Call in" feature.



17. **Select Finish** or, **Select Add another NDE device.**



18. The Schlage NDE lock is shown in the ENGAGE Mobile Application Devices screen with its new descriptive name.





## CTE Controller with Multi-Technology Readers

### Device Introduction

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

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.

**WARNING: DO NOT USE A POWER DRILL!** ONLY use a hand tool to install the devices to prevent product damage.

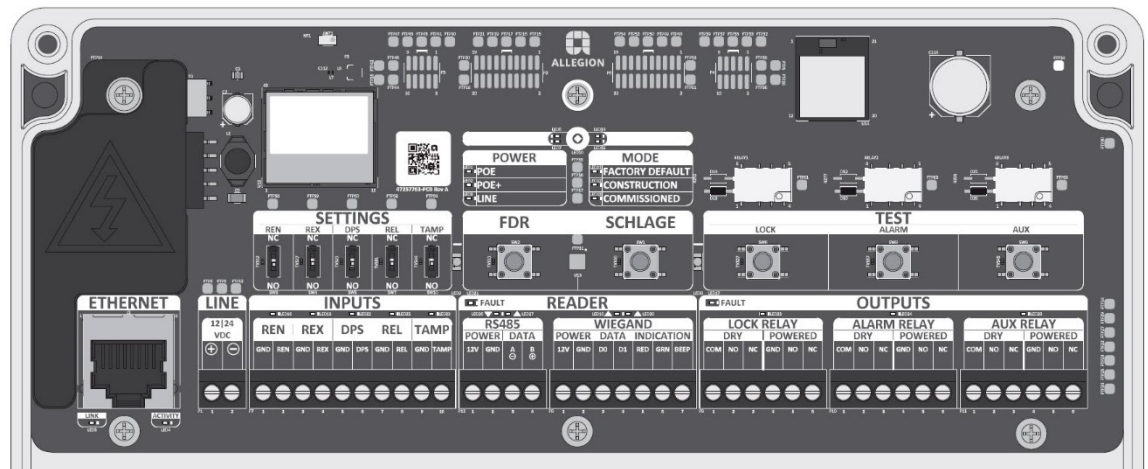


Fig. 11.60: CTE Printed Circuit Board (PCB) Diagram

### 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  $-35^{\circ}\text{C}$  to  $+66^{\circ}\text{C}$  ( $-31^{\circ}\text{F}$  to  $+151^{\circ}\text{F}$ ).
- 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.

CTE does not support wall mounted readers with a keypad (MTK15).

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.

⚠

**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.

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.

Credential Reader Installation

The CTE supports one door opening and one wall mounted Credential Reader at a time.

The original MT11-485 mullion reader and MT15-485 single gang readers initially available have been updated to provide Mobile Credential compatibility MTB11-RS485 and MTB15-RS485.



Fig. 11.61: Original Readers



Fig. 11.62: 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 11.2: 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.

- 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.

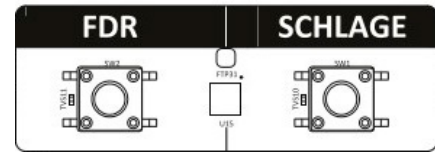


Fig. 11.63: CTE / Reader Connection Switches

Fig. 11.64: 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.

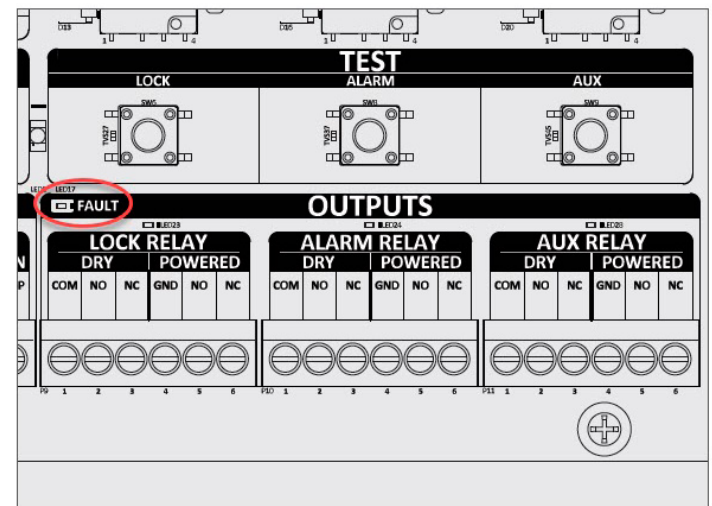
Each of the three output relays (lock, alarm, and auxiliary) has three DRY outputs and three POWERED outputs that can be manually activated using a push-button on the CTE PCB.

- 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.

### Credential Reader Test

Use this button push sequence to test the reader connection in any CTE MODE.

- Press and release the SCHLAGE button.
- Quickly press the FDR button 2 times.
- A correctly wired MT or MTB Wall Mounted Reader:
  - Will beep and blink **AMBER** 3 times.
  - The RS485 LEDs will repeatedly flash indicating good communication is happening.



CTE Outputs: LOCK, ALARM, and AUX.  
Located below TEST buttons.

Fig. 11.65: CTE TEST Switches

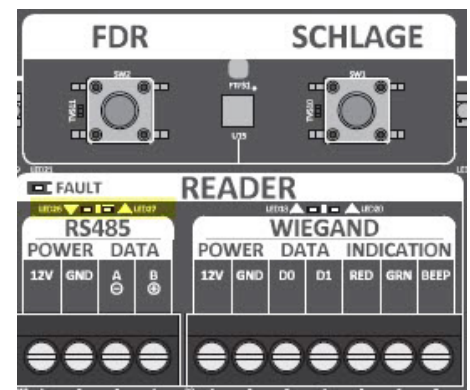


Fig. 11.66: Reader Test Switches

## 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**.

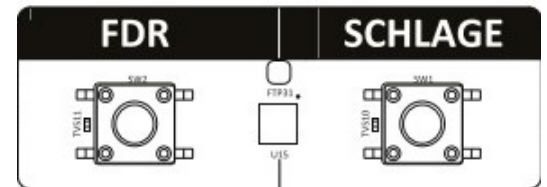


Fig. 11.67: CTE FDR and SCHLAGE Switches

## Verify Success of the FDR

The CTE STATUS LED will be solid **RED** and the MODE LED for Factory Default will be solid **GREEN**.

## 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.

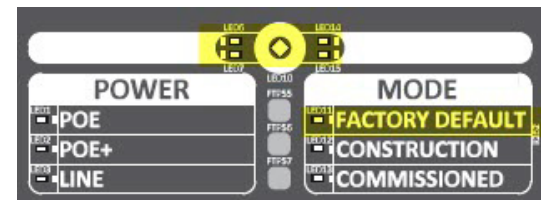


Fig. 11.68: FDR Mode

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.

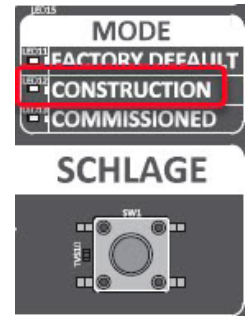


Fig. 11.69: Construction Mode

### 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.

## 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 following screens is presented.
  - An Android device is used in this example.

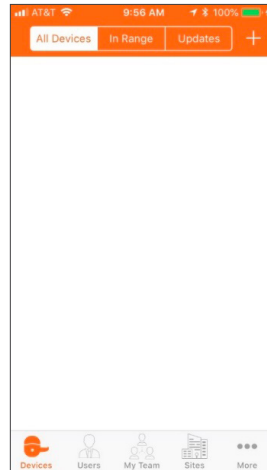


Fig. 11.70: iOS Device Menu

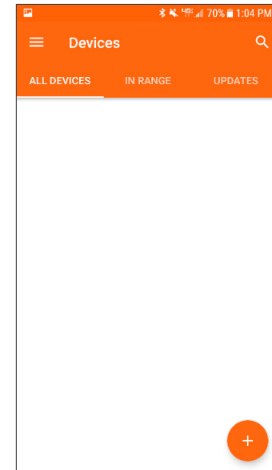


Fig. 11.71: Android Device Menu

→ **Note:** The iOS and Android devices have slightly different screens however the functions are the same. The figures above show that no devices are commissioned into the property. When devices have been commissioned, this screen will display the name of the commissioned devices.

3. To select the nearby CTE 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.
4. Select the **CTE** device type for commissioning.

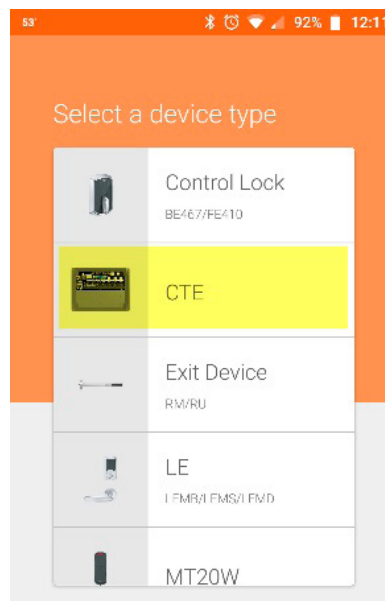
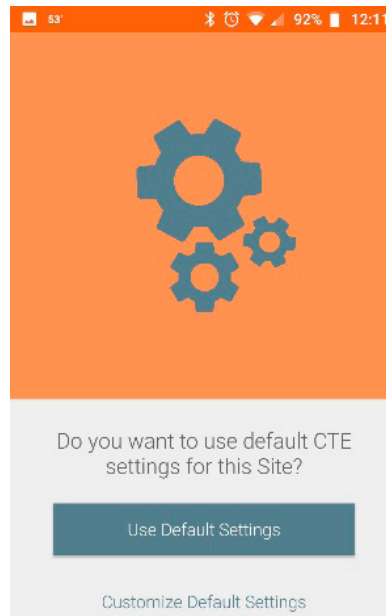


Fig. 11.72: Device Type

5. 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** (pg. 25) 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. 11.73: Site Settings



#### 6. Select Use Default Settings

- 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.

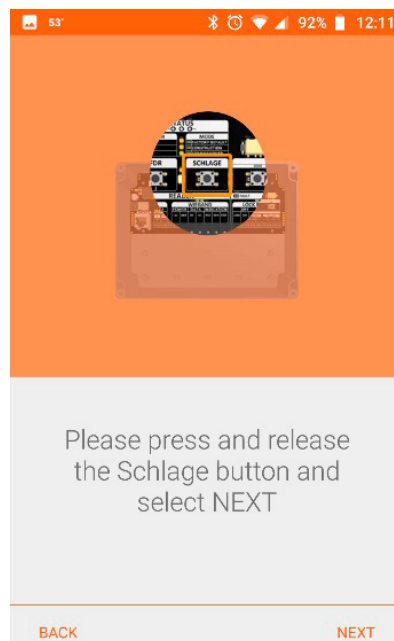


Fig. 11.74: Advertise Presence

- From the list of displayed devices, select the **CTE device** to be commissioned.

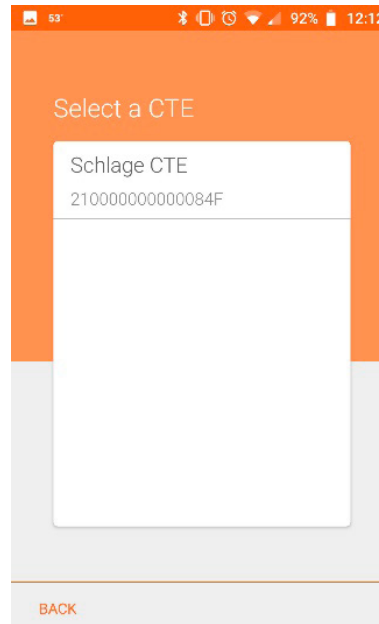


Fig. 11.75: Select CTE Device

→ **Note:** The CTE “advertises” for 2 minutes to allow selection. When the device appears in this screen, the number is the device serial number.

**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

9. After the CTE has been selected, it will connect to the device and then ask you to verify the LED is blinking **RED**.

Fig. 11.76: Connecting

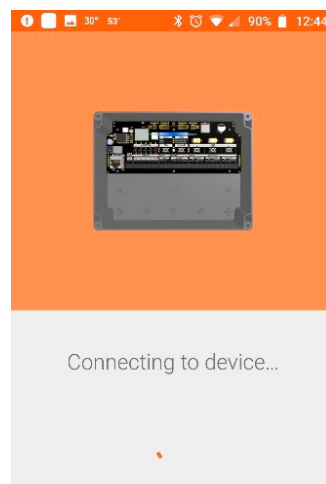
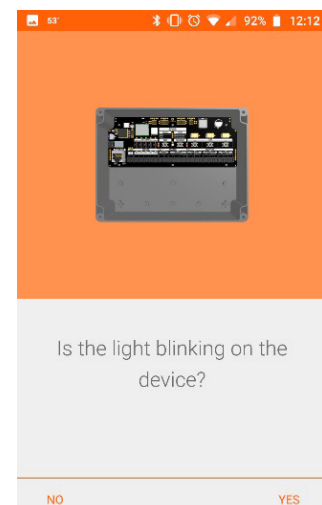


Fig. 11.77: Light Blinking



10. After verifying the LED is blinking, select **Yes**. It will ask you to **Please Wait** while it processes.



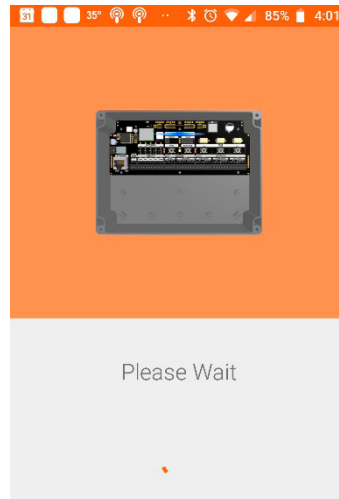


Fig. 11.78: Please Wait

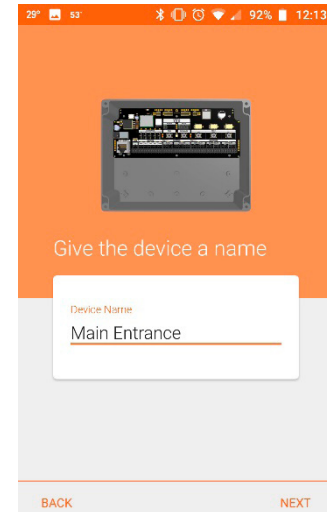


Fig. 11.79: Name Device

1. Provide a descriptive name under **Device Name**
2. Select Next.

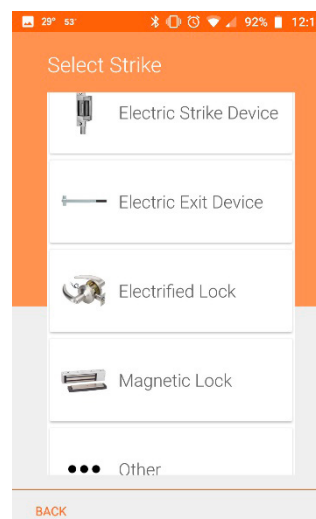


Fig. 11.80: Strike Type

3. Select the **strike type** installed on the door.
  - If your strike type is not listed, select **Other**.
4. Select the **AUX Relay** type.
  - If your AUX relay is not listed, select **Other**.
  - If there are no auxiliary relays, select **Nothing Connected**.



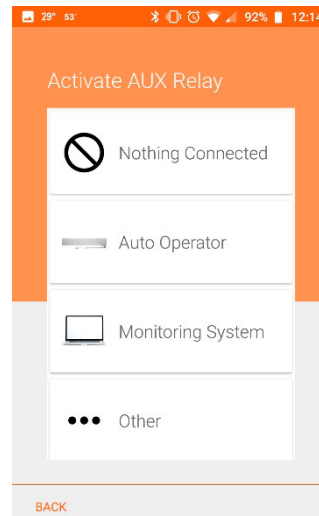


Fig. 11.81: AUX Relay

5. Select if the door has a **horn**.
  - If there is no horn, select **Nothing Connected**.

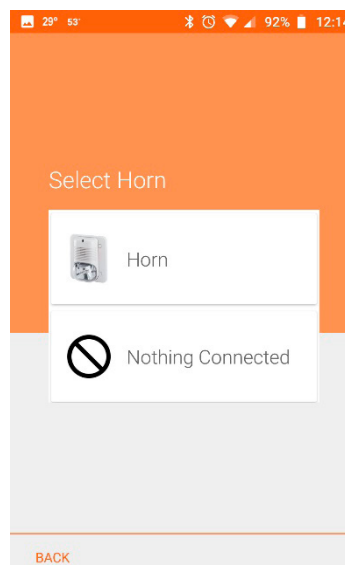


Fig. 11.82: Horn

**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

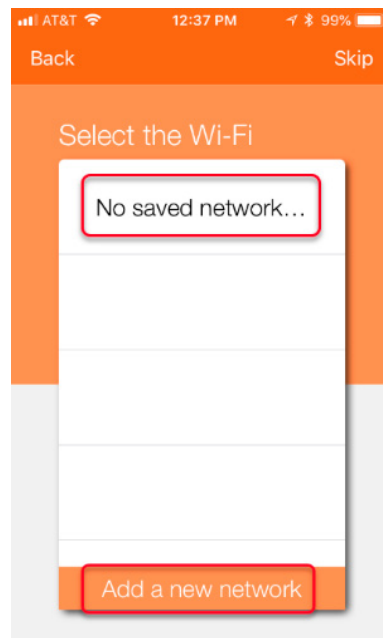


Fig. 11.83: iPhone Wi-Fi Screen

- **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 Enabling Wi-Fi Network Connection Settings 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.

6. Your device is being prepared.

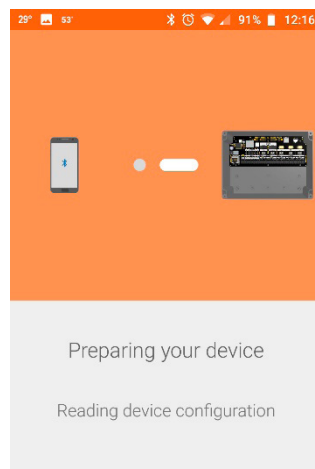


Fig. 11.84: Device Configuration

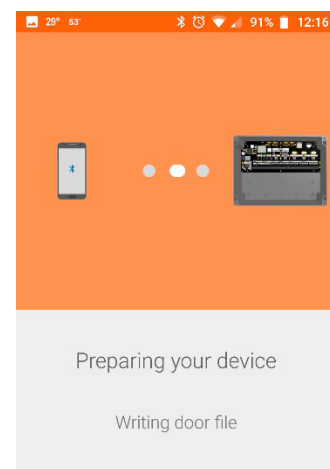


Fig. 11.85: Writing Door File

7. 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.

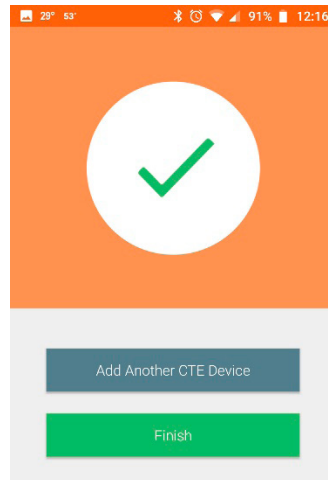


Fig. 11.86: Device Added

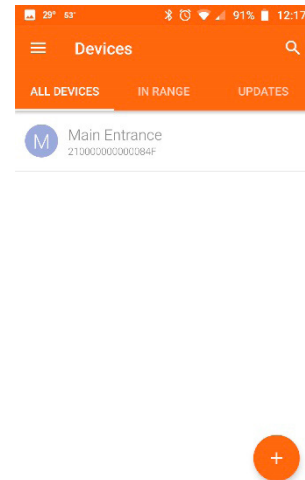


Fig. 11.87: Commissioning Successful

## 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.
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.

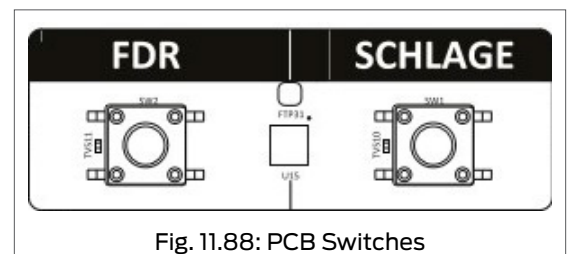


Fig. 11.88: PCB Switches

## MT20

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.

**WARNING:** The MT20 is not compatible with the ENGAGE No-Tour features. Administrators that want to use No-Tour must use the MT20W

### 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.

### 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.



Fig. 11.89: MT20

### 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.

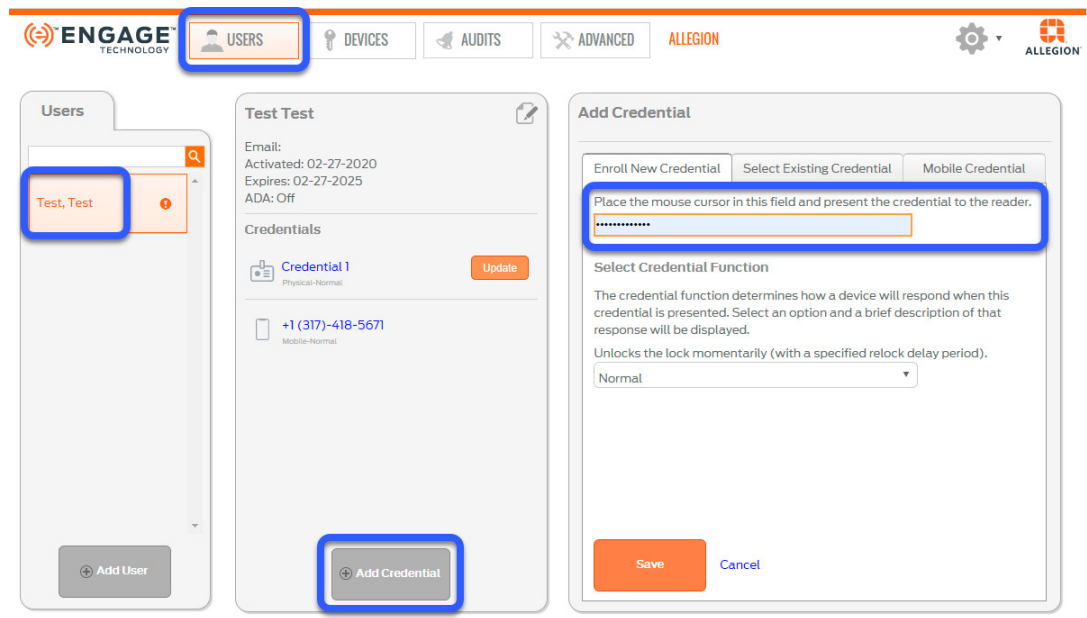


Fig. 11.90: Enroll New Credential

- 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.

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.

**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.

## MT20W ENGAGE Device

Before you begin, review the product information for the Schlage MT20W contained in the box. Also, in the box will be the MT20W Enrollment Reader User Guide and the Factory Reset Default Configuration card.

The ENGAGE administrator will want to determine how the ENGAGE Web Application system is to communicate with the MT20W. There are two options available:

- Setup using the local Wi-Fi network for wireless communication
- Setup using the computer USB port for wired communication

### Device Introduction

The MT20W multi-technology enrollment reader is designed to simplify the enrollment of smart and multi-technology credentials in “No-Tour” multifamily applications.

Site administrators use the MT20W to program smart credentials, when presented at a lock will automatically update the lock user access database.

This automated No-Tour process eliminates the need for the property staff to have to visit each lock to deliver updates (Sync) and allows the User to carry the new information to the lock for immediate updates, when needed.

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.



Fig. 11.91: MT20W

### MT20W initial power up

No special hardware installation is required, just plug the MT20W into the computers' USB connector. The MT20W will use the USB port for its power.

Wait a moment while the MT20W boots-up. There will be a series of **RED** LED flashes and beeps.

When ready, the LED will be solid **RED** waiting for the next step in the setup process, commissioning into an ENGAGE account.

### 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.

### MT20W Configuration Card

The MT20W Credential Enrollment Reader 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.

### 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.
  - a. Wait a few seconds for the boot-up process to complete.
  - b. Within the first 60 seconds after power up, **present** and **hold** the Configuration Card to the Reader.
    - i. 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.

## Commissioning the MT20W

Commissioning a MT20W enrolls the enrollment reader into ENGAGE, defines the MT20W “Friendly Name” name, and prepares the MT20W for later setup steps.

→ **Note:** When commissioning a MT20W Credential Enrollment reader, the No-Tour ENGAGE feature is automatically enabled within the ENGAGE web application.

To commission the MT20W, perform the following:

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.
  - An iOS Mobile device is used in this example

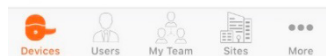
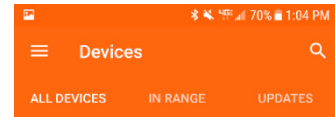
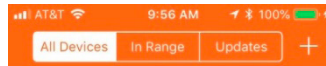


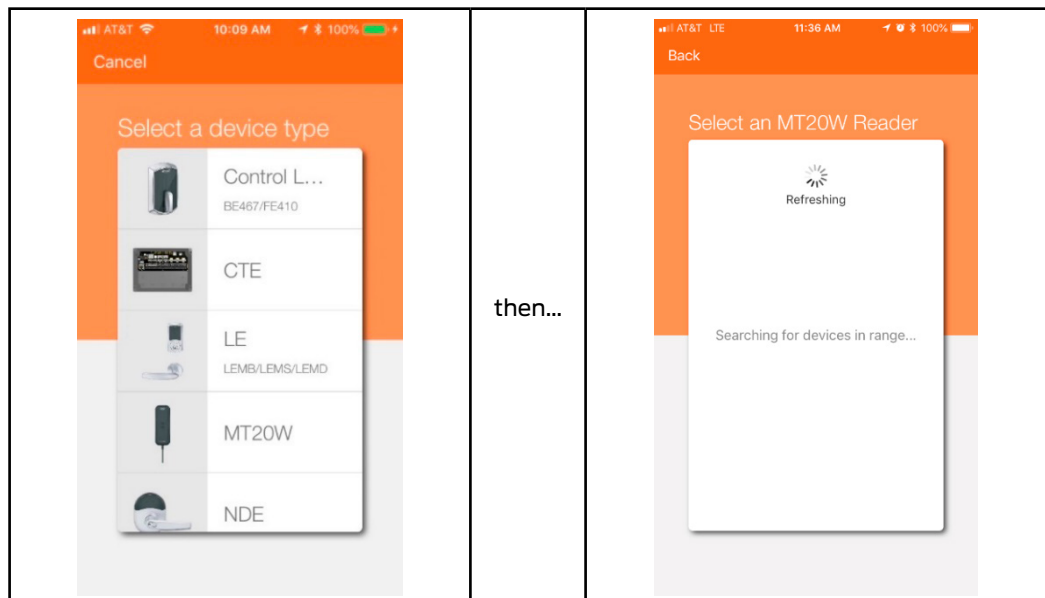
Fig. 11.92: iOS device menu



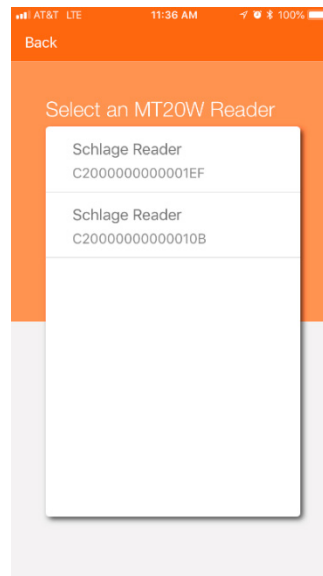
Fig. 11.93: Android device menu

→ **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(s).

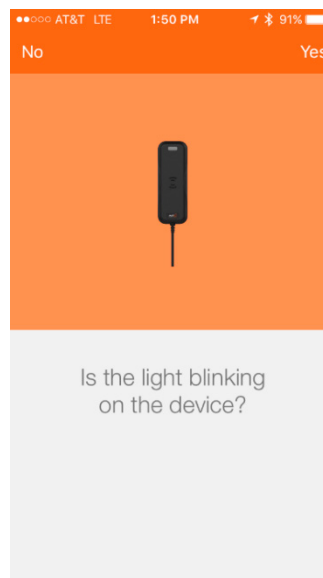
4. **Select the Plus** to begin searching for available “advertising” devices



5. **Select the MT20W** device type in the “Select a device type”

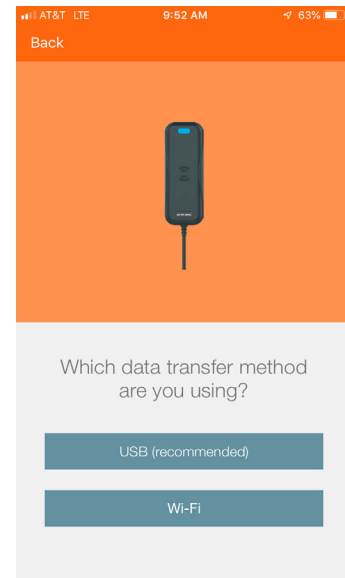
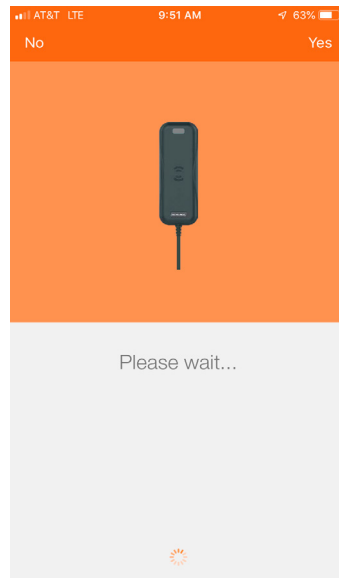


6. **Select** the specific Schlage Reader (MT20W) device to be commissioned from the list of nearby devices provided.
  - More than one device may be available for commissioning.
  - We chose **Schlage Reader** serial number **C20000000000010B** by tapping on that specific Schlage Reader in the screen as shown below.
7. Confirm the Schlage MT20W Credential Reader selected for Commissioning.
  - The Blue LED is flashing slowly to indicate it has been selected.



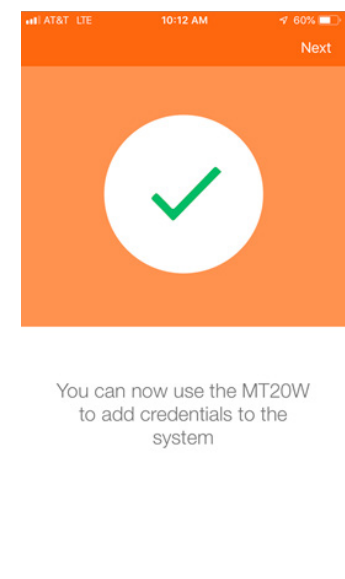
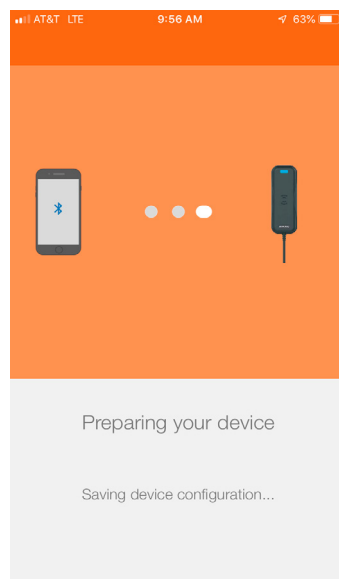
8. **Select Yes.**





- 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?

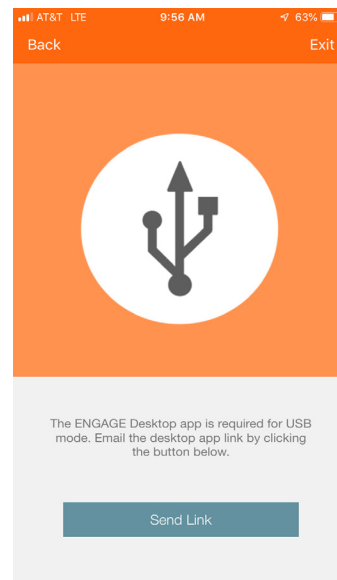
9. **Select USB** (recommended).



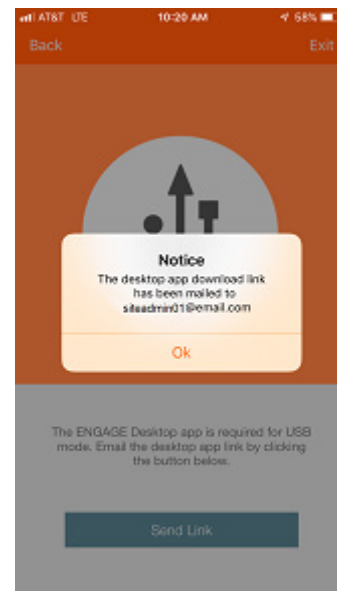
10. **Preparing your device** and **SUCCESS checkmark** screen displays

**WARNING:** When using USB communication, you must also **INSTALL** and **RUN** the **ENGAGE PC Desktop Application**. The MT20W LED will be **BLUE** when ready for communication. The MT20W will take a few seconds to boot up after power is applied. For USB communication, the MT20W firmware must be at version 39.02.00 or higher.

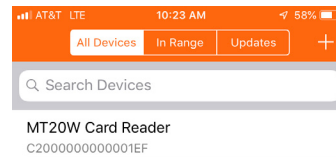
11. Click **Next** in the top right-hand corner to continue.
12. The USB symbol with the **Send Link** button displays.
  - Selecting the **Send link** button will send an email and ENGAGE™ PC Desktop Application link to the Administrator's email.



13. **Select Send Link.**



14. Acknowledge the **Notice** and **Select Ok**.
15. Then **Select Exit** in the top right-hand corner to continue. The **All Devices** screen displays showing the recently commissioned MT20W.

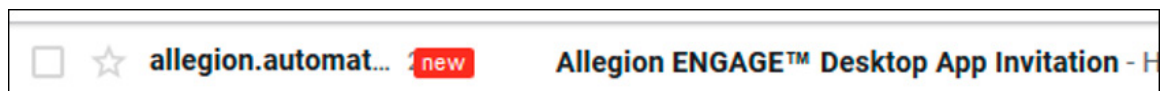


**WARNING:** Before using the MT20W with USB communication, you **MUST** complete the MT20W setup by installing and **RUNNING** the ENGAGE USB PC Desktop Application

### Installing the ENGAGE PC Desktop Application

After the Desktop Application Send Link button is selected, the ENGAGE system sends a link to the Administrators email with instructions. Go to the email and follow the link instructions.

1. **Check Email** – look for this item in the Administrator’s email.



2. **Open** the email and then **Select** the appropriate Operating System version for your computer.



Hi (Site Admin Name),

Download our desktop app to allow the card reader to communicate over USB. Feel free to contact us with any questions at 877-671-7011




Windows

macOS

3. **Select Windows** or **macOS** operating system button.
4. **Navigate** to the PC “Download” folder.

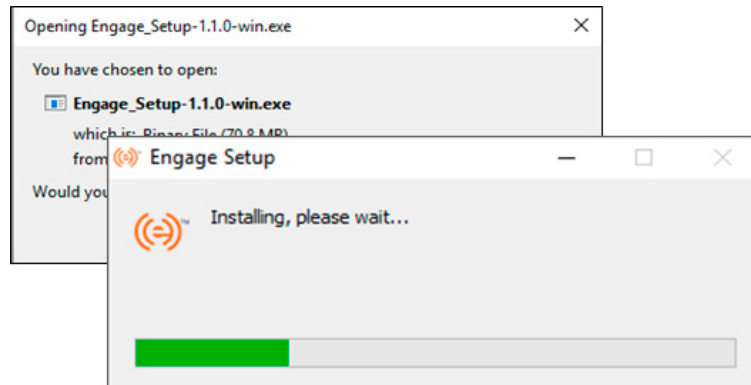
5. **Locate** the Engage Setup installation application.

 Engage_Setup-1.0.0-win.exe	11/15/2018 4:01 PM	Application	72,597 KB
--	--------------------	-------------	-----------

6. Run (Double-Click) the Engage\_Setup-X.x.x-win.exe installation application to install it.

**WARNING:** PC Administration authority (permissions) are required in order to install the ENGAGE Desktop Application on the computer. The “Xs” in the installation application name is the software version

7. **Observe** the installation process where the next screens are shown.



8. When the installation is successful, and a MT20W is connected to the USB computer port. The following screens display on the desktop.

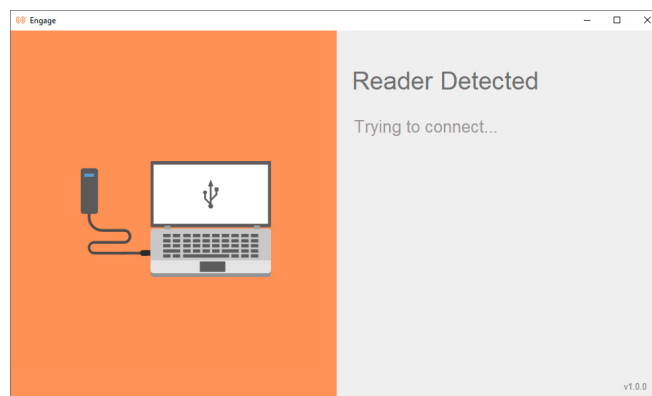


Fig. 11.94: Reader Detected

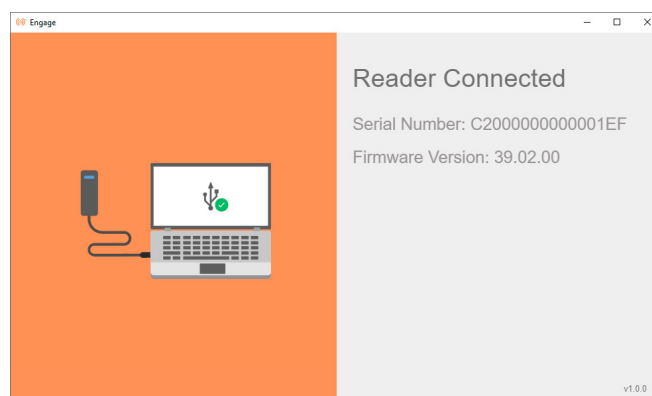


Fig. 11.95: Reader Connected

**WARNING:** Do NOT use the “X” in the top right corner to close the ENGAGE Desktop Application. The ENGAGE Desktop Application is required to 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.

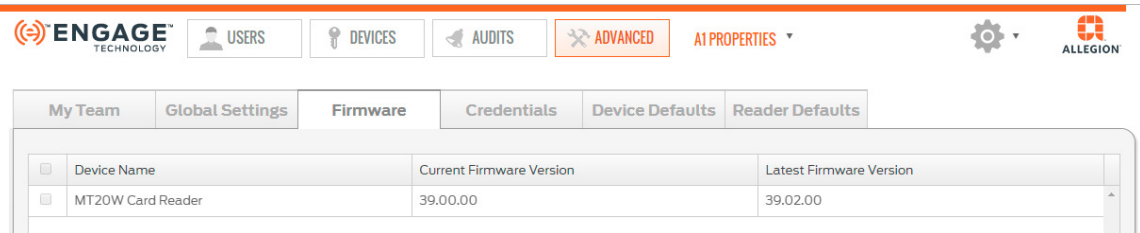
→ **Note:** After the MT20W reader and Computer connection is established, the serial number and firmware version of the MT20W are shown.

### Verifying and Updating MT20W Firmware

If the MT20W is already Commissioned at your site, there are two ways to confirm the MT20W firmware version. You can either use your ENGAGE Web application or ENGAGE Mobile application.

→ **Note:** Using the ENGAGE Web Application to verify the current MT20W firmware revision:

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**.

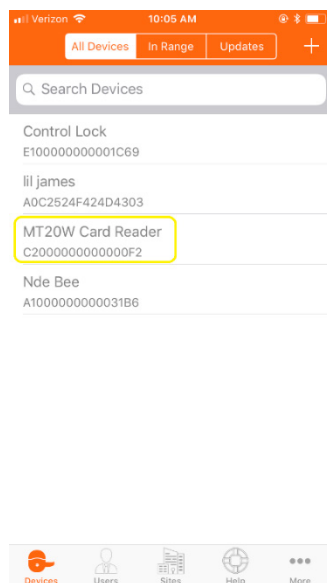


Device Name	Current Firmware Version	Latest Firmware Version
MT20W Card Reader	39.00.00	39.02.00

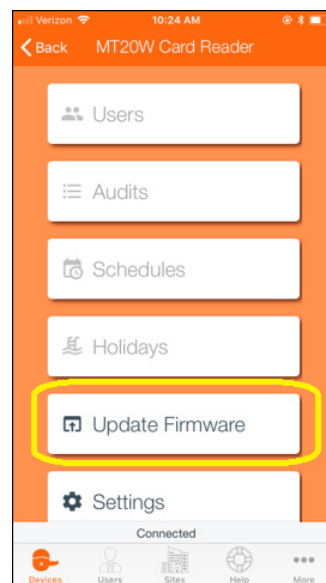
→ **Note:** In this case the MT20W firmware is not at the latest revision. If the current MT20W firmware version is earlier than version 39.02.00, you must update the firmware before using the Mobile application to enable USB communication. USB communication is only available when the MT20W firmware is 39.02.00 or higher.

→ **Note:** Using the ENGAGE Mobile Application to verify the current MT20W firmware revision:

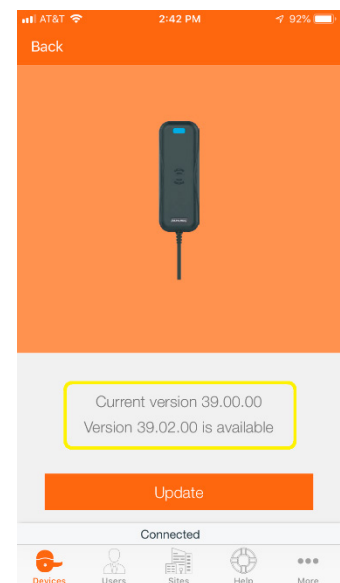
#### 6. Connect to the MT20W



#### 7. Select Update Firmware

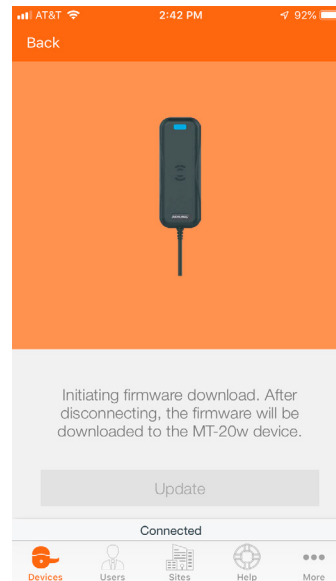


#### 8. Is Firmware Current?



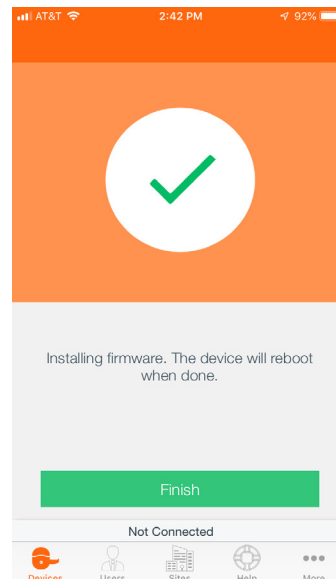
**WARNING:** The MT20W firmware update is ONLY possible when the MT20W is communicating over the local Wi-Fi network. When firmware updates are needed, temporarily enable Wi-Fi network communication to proceed.

9. The **Initiating firmware download** screen displays.



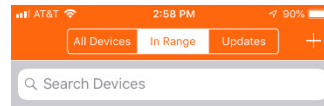
10. The firmware is downloaded to the MT20W.

11. The **Installing firmware** screen displays.



12. **Select Finish.**

13. The **In Range** Mobile device display is shown. (currently blank)



14. 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.
15. **Swipe** 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.

### MT20W USB communication mode

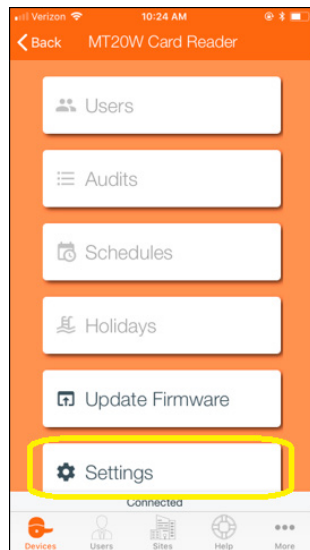
The MT20W may be configured to communicate with ENGAGE via USB connection or via a local Wi-Fi network connection.

USB connectivity is recommended for the most robust data connection.

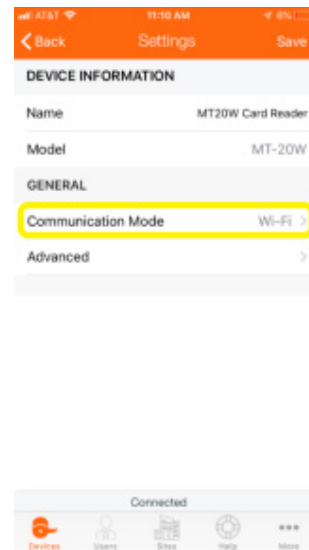
When connected and communicating with the MT20W, follow these steps to change from a local Wi-Fi network to USB communication mode.

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.

**WARNING:** The ENGAGE Desktop Application is required to be running in the background anytime the MT20W is using USB connectivity 📶




### 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.

8. **OPEN** the ENGAGE Desktop Application, the information on the screen instructs you to connect the MT20W to your PC to get started.

**WARNING:** The ENGAGE Desktop Application is required to be running in the background anytime the MT20W is using USB connectivity.  The MT20W LED will be RED when the ENGAGE Desktop Application is NOT running. The ENGAGE Icon symbol shows in your PC system tray anytime the ENGAGE Application is running

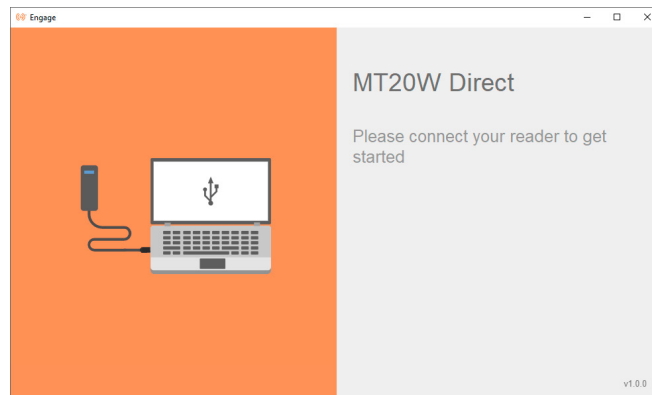


Fig. 11.96: MT20W Direct

9. **Plug** the MT20W into the USB port on the PC, the ENGAGE Desktop Application detects the reader and begins communication.
  - After power up, the MT20W must go through a boot up process BEFORE a connection is accomplished.
  - Be patient, this may take a few seconds.

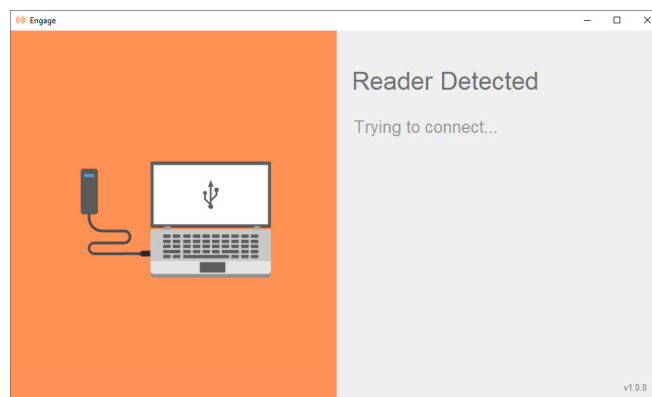


Fig. 11.97: Reader Detected

- After the connection is established, the serial number and firmware version of the MT20W displays on the screen.

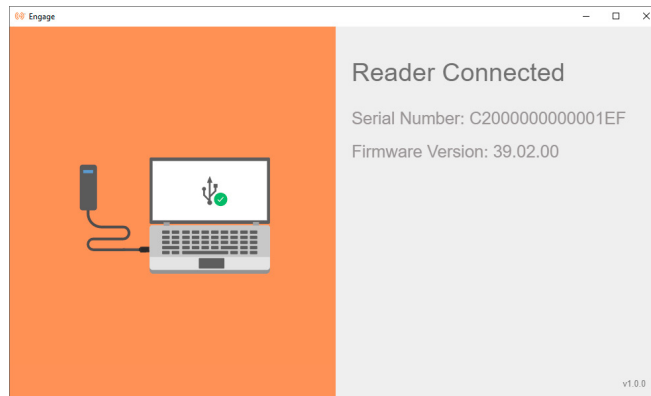


Fig. 11.98: Reader Connected

- When a credential programming error occurs, an error message along with the error code displays on the screen along with a notification.

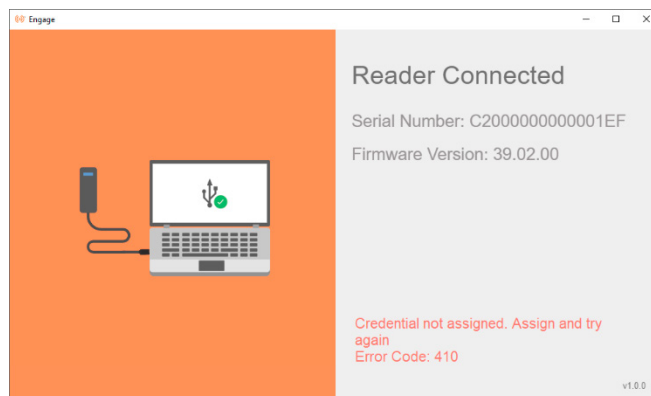


Fig. 11.99: Error Detected

- When the USB enabled MT20W reader is un-plugged from the computer, the Application screen shows that the reader is disconnected.

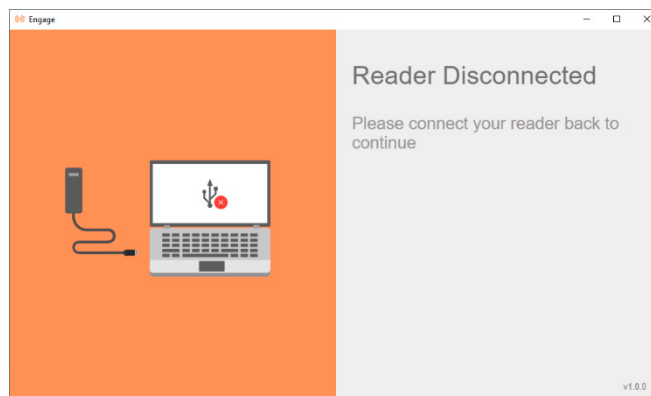
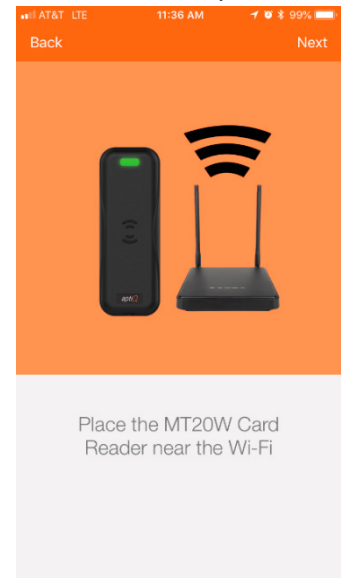


Fig. 11.100: Reader Disconnected

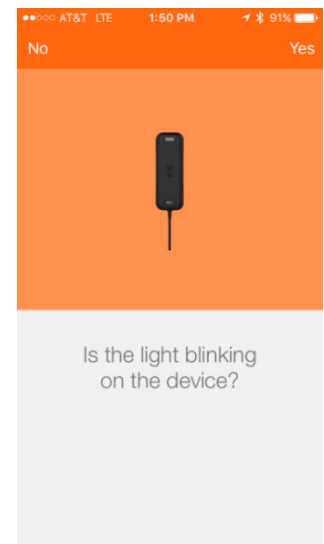
**MT20W Wi-Fi communication mode (Optional)**

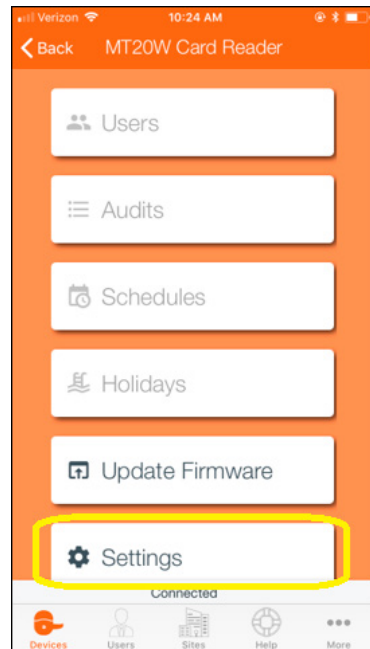
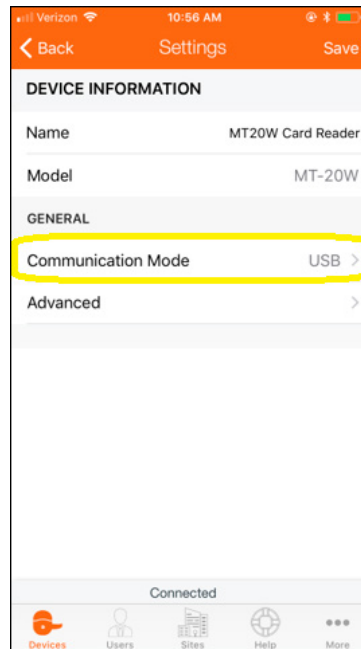
When connected and communicating with the MT20W, follow these steps to change from USB to Wi-Fi communication mode.

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. Select Wi-Fi under Communication Mode.****8. Enter the Wi-Fi network details:**

- Depending on the Wi-Fi network security chosen, you will need to enter different information.
- In this case we chose Wi-Fi SSID **610baLWLAN** and the **WPA2 (PEAP)** network security protocol.
- Both a Username and Password are required.

**9. Select Next**

➔ **Note:** The MT20W will connect with the local Wi-Fi network using the entered network settings. Wait a few moments until the MT20W provides a solid Blue LED indicating it has successfully connected with the local wireless area network.

**WARNING:** 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. You can also verify the local network security settings by using your Mobile Phone to enter the network settings and temporarily connect to verify local Wi-Fi network connection requirements.

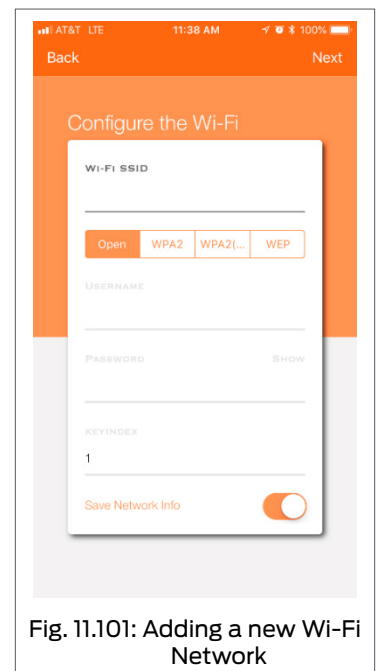
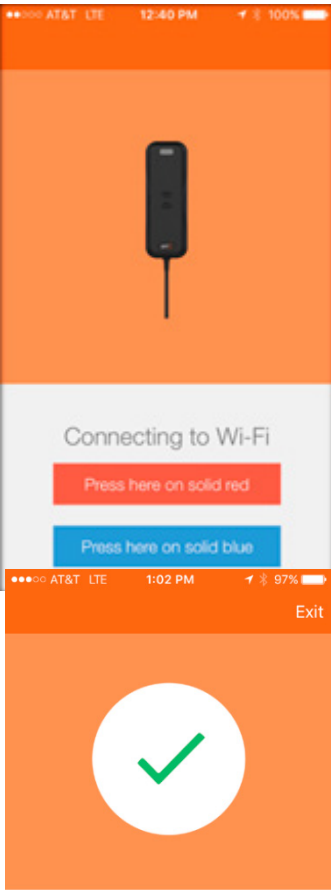


Fig. 11.101: Adding a new Wi-Fi Network

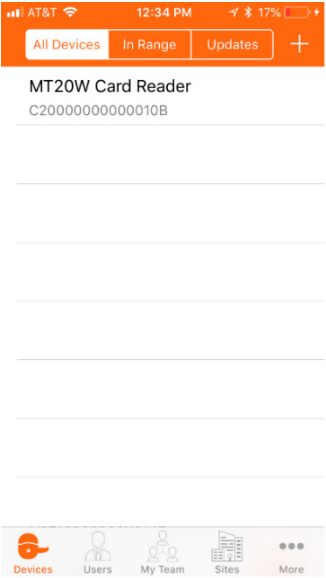
10. Select the Blue **Press here on solid blue** bar to continue.



11. Acknowledge the “Setup Complete” message. Select **Exit**.

You can now use the  
MT20W to add  
credentials to the  
system

12. 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.



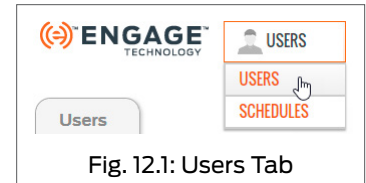
# Daily System and Other Operations

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

## Users Overview

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

- Add the user and details into the ENGAGE Web account
- Assign a Physical or Mobile Credential to the User to be used for access
- Assign the appropriate access privileges to the individual user
- Finally, the assigned doors will need **Sync** (programmed) before the new user and access assignments will be valid.

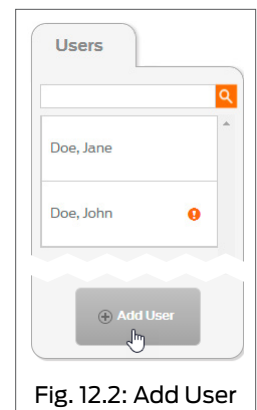


### Add User

Adding a new user may be accomplished by using either of the ENGAGE web or ENGAGE Mobile applications.

→ **Note:** The ENGAGE web application is the preferred method for data entry due to ease of entry and larger keyboard.

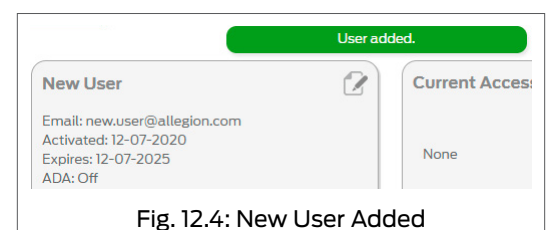
1. **Log In.**
2. Hover over the **Users** menu and select **Users** from the pull-down menu.
3. Select Add User.
4. From the **Add New User** screen, complete required fields:
  - a. **First Name:** enter the first name of the user.
  - b. **Last Name:** enter the last name of the user.
  - c. **Email Address, optional:** enter user email address.
  - d. **ADA:** Select this setting when the resident requires additional time to access doors. This enables ADA (American Disabilities Act)
  - e. **Activation & Expiration:** (required)
5. Select **Save**.



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.

The screenshot shows the 'Add New User' form. It has fields for 'First Name' (with a red dot), 'Last Name' (with a red dot), and 'Email Address'. Below these is an 'ADA' section with a toggle switch set to 'OFF'. Underneath are 'Activation' and 'Expiration' fields, both with red dots and calendar icons. At the bottom are 'Save' and 'Cancel' buttons. The caption below the image is 'Fig. 12.3: Add New User'.

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



## Credentials Overview

There are three types of User Access credentials supported by ENGAGE. Two physical credentials (Smart and Proximity) and a Mobile Credential type.

- **Smart Credentials:** Smart credentials are read/write capable, providing encrypted and secure and based on open, global standards
  - **Proximity Credentials:** Proximity credentials from Schlage provide a convenient access control solution for facilities with less demanding security needs.
    - Schlage proximity credentials are compatible with most industry-leading proximity readers.
  - **Mobile Credentials:** Mobile Credentials provide a convenient User Access using their smart phone replacing the more standard physical credentials. Mobile Credentials require the User to download and use the Schlage Mobile Access Application with their Mobile phone instead of using a physical card or fob credential.
    - Mobile Credentials do not support No-Tour functionality (yet). Support for No-Tour is planned soon.
- **Note:** When ordering physical credentials, the Serial Number range and Facility Code should be assigned through Res CardTrax™ account CT8X4248 that is maintained internally by Allegion. Consult Allegion Sales Support for details. The CardTrax account **MUST** be referenced on Construction Credential orders for Schlage Control Mobile Enabled Smart Locks
- **Note:** New User Access credentials out of the box must first be enrolled into ENGAGE to be listed for selection and assignment to an individual User
- **Note:** Proximity and Mobile Credential types **DO NOT** support No-Tour functionality
- Enrollment of these credentials types is accomplished using one of the following methods:
1. **Physical credentials** may be enrolled into ENGAGE individually as needed.
  2. **Physical credentials** may be enrolled into ENGAGE In bulk, allowing many credentials to be enrolled quickly and stored in ENGAGE ready for quick user assignments later. (a stock list)
  3. **Mobile Credentials** are always added individually into ENGAGE, and the user will use the Schlage Mobile Access smart phone application for access.
  4. **Physical and Mobile credentials** may be enrolled “At a door”. However, credential naming, tracking and audit ENGAGE features are not available for credentials enrolled at a door.
    - Enrollments at the door, is **NOT recommended**.

Each of these credential enrollment processes are described in the following sections.

**⚠ CAUTION: Construction Mode:** 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.

**★ BEST PRACTICE:** Each user be assigned **ONLY** one credential

## Enroll New Smart and Proximity Credentials Individually

Administrators will need to enroll a new credential whenever a new user is added or a credential needs replacement.

1. Plug the MT20W credential enrollment reader into the computer USB port.

**WARNING:** 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. Wait a few seconds until the reader boots up and begins communication. The LED will light solid **BLUE** when ready.
3. **Log In.**



Fig. 12.5: Ready MT20W

4. Hover over the **Users** menu and then select the **Users** from the pull-down.
5. Select the appropriate user.

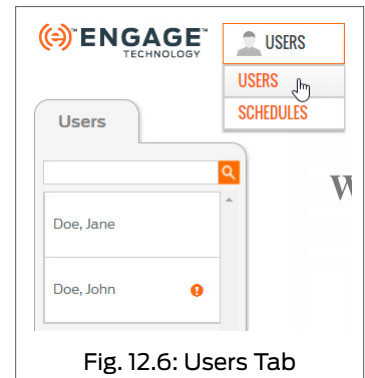


Fig. 12.6: Users Tab

6. From the Users card, select **Add Credential**.

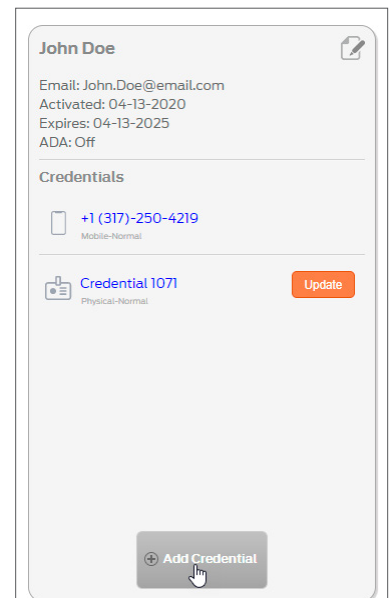


Fig. 12.7: Add Credential



- 7. Select Existing Credential tab.

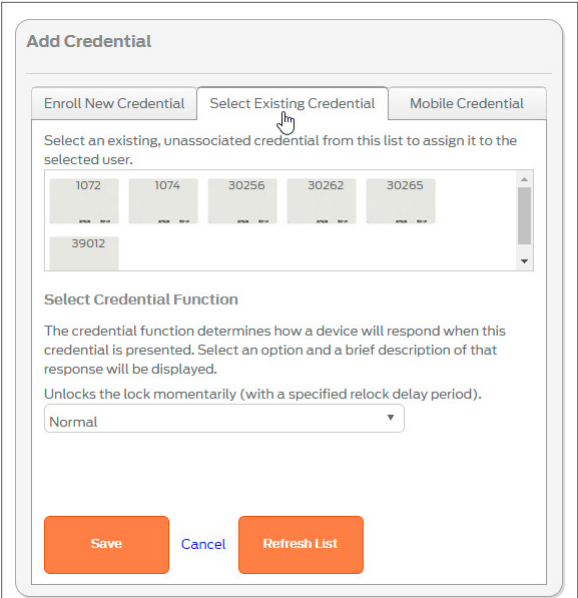


Fig. 12.8: Select Existing Credential

- 8. Take a new physical credential to be enrolled out of the box.
- 9. Present the new credential to the MT20W. The MT20W turns GREEN and beeps 1 time when the credential is accepted.



Fig. 12.9: Physical credential

- 10. Wait a few seconds and then click Refresh List.  
→ **Note:** If the credential number does not appear in the list, wait a few seconds and select the Refresh List button again.

The “Ink Stamped” number on your credential will appear in the “Select Existing Credential” list.

Fig. 12.9 shows an ISO Glossy Card credential #1070.

- **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.

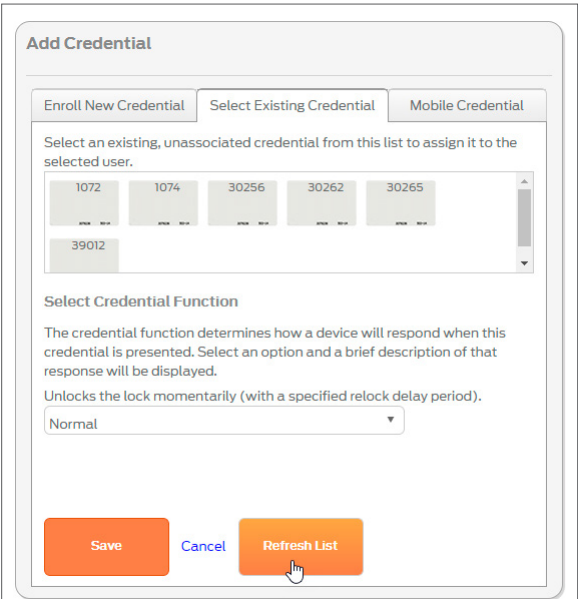


Fig. 12.10: Individual Credential 1070 Enrolled

## Enrolling New Smart and Proximity Credentials in Bulk

Bulk physical credential enrollment is the recommended credential enrollment process for ENGAGE. Using bulk credential enrollments will allow faster initial property setup and streamline the credential assignment processes, later.

When a new credential is presented to the MT20W, the MT20W will automatically enter the credential into the “Select Existing Credential” tab on the Add Credential ENGAGE menu.

Bulk credential enrollments can save time and is the recommended method for credential enrollments. However, the Administrator is required to manage the stored and enrolled credentials and match each individual credential “Ink Stamp” number when actual User assignments are made.

Follow these simple steps to enroll credentials in bulk for assignment later.

### When the MT20W is using Wi-Fi connectivity:

1. Plug the MT20W into a computer or wall USB power plug for power.
2. Wait a few seconds for the MT20W boot up process to complete
  - A properly commissioned MT20W will be ready for credential enrollments when displaying a solid BLUE LED
3. Present a new credential to the MT20W
  - The MT20W turns **GREEN** and beeps 1 time when the credential is accepted.
4. Wait a few seconds for the MT20W to return to “Ready” with the BLUE LED illuminated.
5. Repeat steps 3 and 4 presenting new credentials, **One-At-A-Time** until all credentials have been enrolled. To verify and view recently enrolled credentials, the Administrator will want to:
  - **Log In.**
  - **Select** a new or existing **User**, **Select** the **Add Credential** button, on the **Add Credential** card, **Select** the **Select Existing Credential** tab.
  - **View** each of the recently enrolled and available credentials

### When the MT20W is using USB connectivity:

1. Plug the MT20W into a computer for power and communication with the computer.
2. Go to the ENGAGE Web application <https://portal.allegionengage.com/signin> and log into your account.
3. Ensure the **ENGAGE Desktop Application** is running on the computer.
  - If not, Start the ENGAGE Desktop Application
4. Wait a few seconds for the MT20W boot up process to complete and for the ENGAGE Desktop Application to connect with the MT20W.
  - A properly commissioned MT20W will be ready for credential enrollments when displaying a solid BLUE LED
5. Present a new credential to the MT20W
  - The MT20W turns **GREEN** and beeps 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:

- Wait a few seconds then, **Select** a new or existing **User**, **Select** the **Add Credential** button, on the **Add Credential** card, **Select** the **Select Existing Credential** tab.
- **View** each of the recently enrolled and available credentials
  - ➔ **Note:** If the credentials do not appear in the list, wait a few seconds and select the Refresh List button to try again.

The recently added and unassociated bulk credentials will appear in the **Select Existing Credential** tab on the **Add Credential Card**.

The screenshot shows the 'Add Credential' interface with three tabs: 'Enroll New Credential', 'Select Existing Credential' (which is selected), and 'Mobile Credential'. Under the 'Select Existing Credential' tab, there is a prompt: 'Select an existing, unassociated credential from this list to assign it to the selected user.' Below this prompt is a table of credentials:

1066	1070	11722	4580
------	------	-------	------

Below the table is a 'Select Credential Function' section. It includes a description: 'The credential function determines how a device will respond when this credential is presented. Select an option and a brief description of that response will be displayed.' and a specific instruction: 'Unlocks the lock momentarily (with a specified relock delay period)'. A dropdown menu is set to 'Normal'. At the bottom of the form are three buttons: 'Save' (orange), 'Cancel' (blue), and 'Refresh List' (orange).

Fig. 12.11: Select Existing Credential

When using multi-technology credentials and ENGAGE locks with multi-technology credential readers as your credential enrollment reader, Administrators should 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 New Credentials at a Door (NOT Recommended)

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; however, this method is NOT recommended because some functionality normally available in ENGAGE is not available.

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

**WARNING:** Credentials assigned using the ENGAGE Mobile Application and commissioned ENGAGE device method as shown here are not searchable in the ENGAGE database.

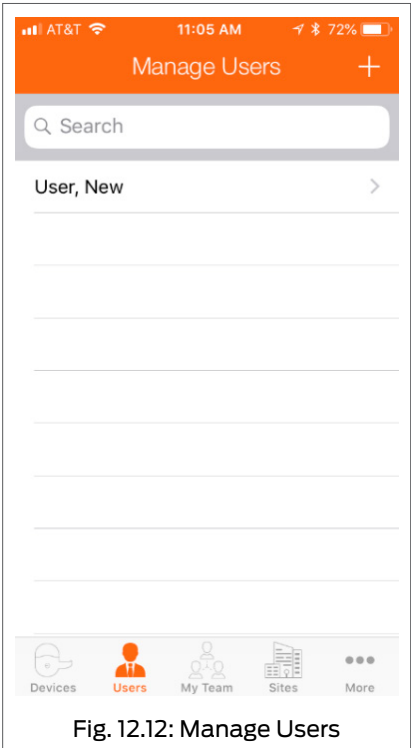


Fig. 12.12: Manage Users

- 4. Select the **Credentials** Menu.

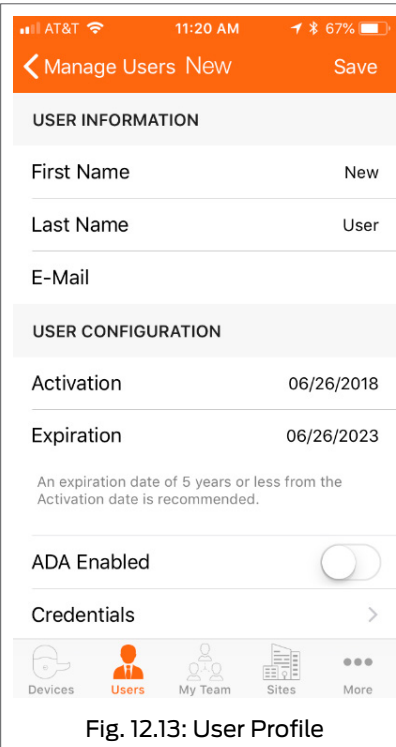


Fig. 12.13: User Profile

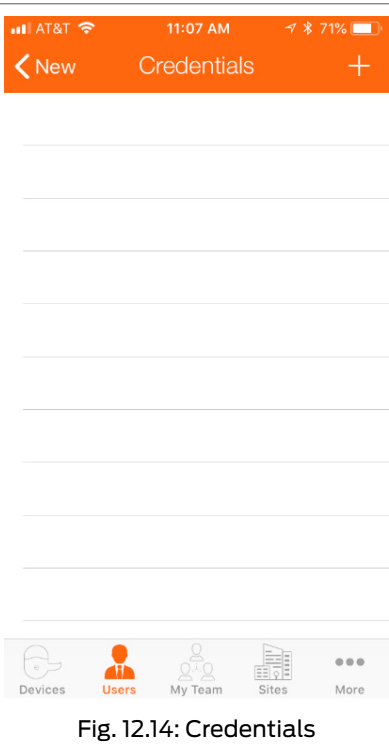
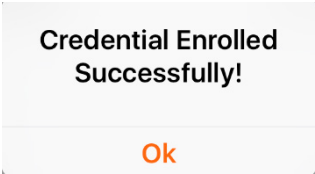


Fig. 12.14: Credentials

- 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.
- 6. Select a specific device from the **Available Enrollment Readers** list.
  - In this case we chose **Storage**.

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

- 7. **Present** the new credential to the nearby **Storage** device.
  - If no credential is presented, the process “Times Out” after 20 seconds so the device can return to its normal use - securing an opening.
  - When the device reads the credential, the credential “**Value**” recorded and is displayed with asterisks **\*\*\*\*\***. The credential NAME is “Credential 1”.
- 8. Select **Save**.
- 9. **VERIFY SUCCESS:** See the **Credential Enrolled Successfully!** Message.



- 10. Select **Ok**.

**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.

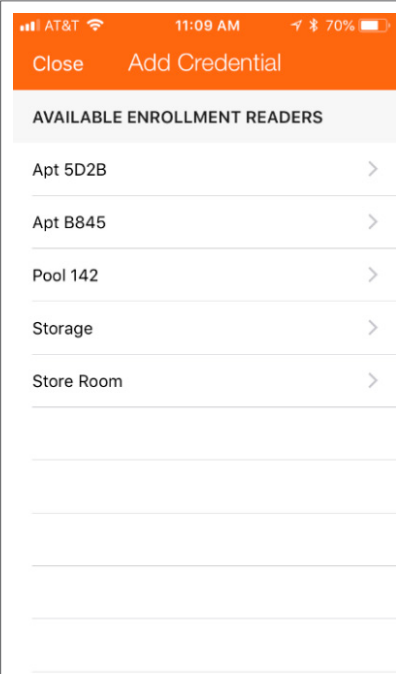


Fig. 12.15: Add Credential

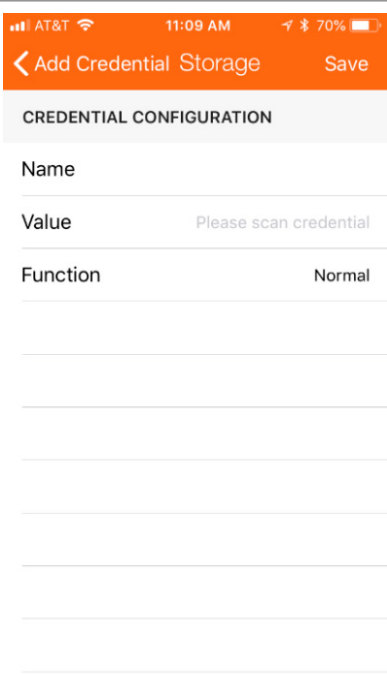


Fig. 12.16: Credential Configuration

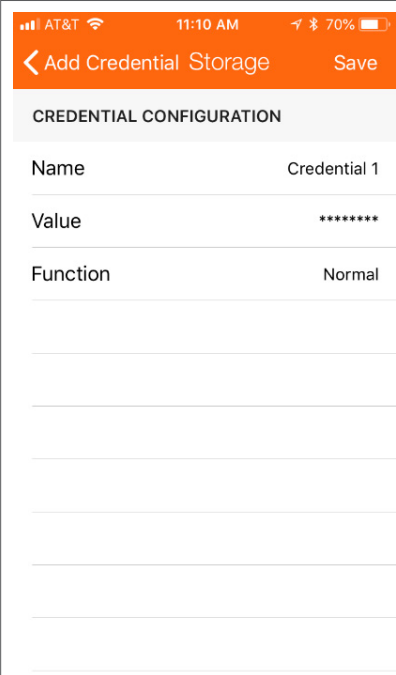


Fig. 12.17: Credential Enrolled

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.

## Enrolling Mobile Credentials

The process of enrolling Mobile Credentials into ENGAGE is three step process:

1. Enter the User and Credential details in ENGAGE,
  2. Download and set up of the Schlage Mobile Access application.  
 → **Note:** See Download and Install the Schlage Mobile Access Application on page 121 for more information.
  3. Use the Schlage Mobile Access Application to gain access to a door.  
 → **Note:** To allow ENGAGE Mobile Credential features and to create and assign Mobile Credentials, the Administrator must have at least one Mobile Enabled device commissioned into the ENGAGE account.
1. **Log In.**
  2. Hover over the **Users** menu and select **Users** from the pull-down menu.
  3. Select the appropriate user.

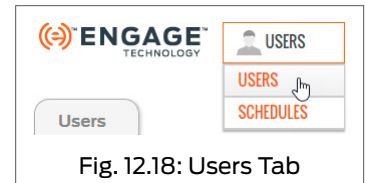


Fig. 12.18: Users Tab

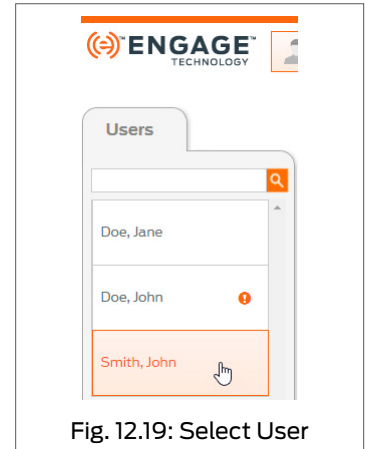


Fig. 12.19: Select User

4. Select the **Add Credential** button.

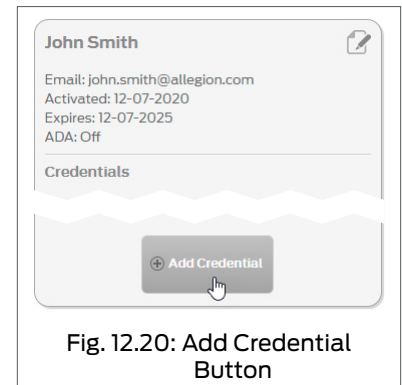


Fig. 12.20: Add Credential Button

If your screen displays **Your devices do not currently support mobile credentials**, then click [Learn about the path to upgrade here](#) to learn more.

5. Select the **Mobile Credential** tab on the Add Credential card.
  6. Enter the user's **Mobile Phone Number**.
  7. Select **Save**.
- The user's mobile phone will receive an automated text with additional instructions.
- **Note:** Administrators will need to sync each affected lock or wait for automated nightly update device updates to take effect.

**Add Credential**

Enroll New Credential | Select Existing Credential | **Mobile Credential**

**Free Trial**

Enter Mobile Phone Number

Mobile Phone Number

+1 (XXX)-XXX-XXXX

Select Credential Function

The credential function determines how a device will respond when this credential is presented. Select an option and a brief description of that response will be displayed.

Unlocks the lock momentarily (with a specified relock delay period).

Normal

Save Cancel

Fig. 12.21: Add Mobile Credential

### Resend Mobile Credential Invitation

1. **Log In.**
2. Hover over the **Users** menu and select **Users** from the pull-down menu.
3. Select the appropriate user.
4. Select the mobile credential.

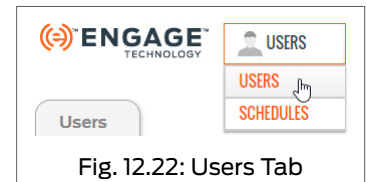


Fig. 12.22: Users Tab

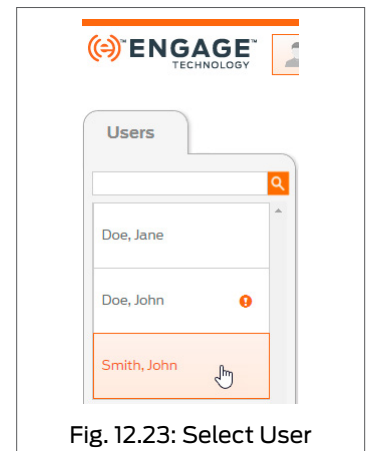


Fig. 12.23: Select User

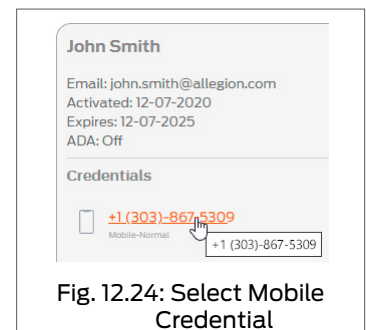


Fig. 12.24: Select Mobile Credential

- 5. Select **Resend SMS**.

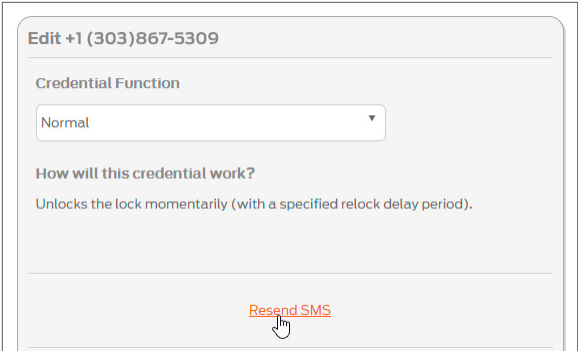


Fig. 12.25: Resend SMS

- 6. The user will receive an SMS message. The screen shows **New SMS invite sent ot the user**.

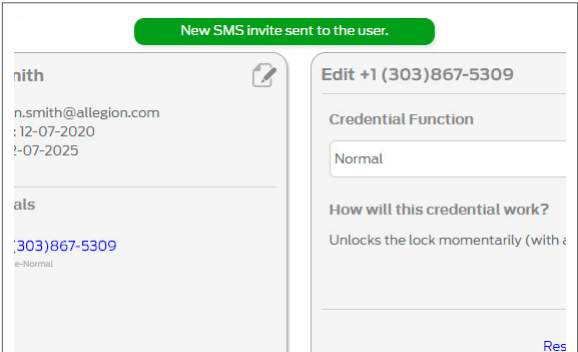


Fig. 12.26: SMS Resent

Mobile Credentials do not support the No-Tour feature and cannot be assigned to a lock using No-Tour. Each Mobile Credential assignment must use a **Sync** process to update access rights in a door. Administrators must use the Schlage ENGAGE Mobile Application or overnight Sync process to update door Mobile access.

## No-Tour Credential Programming

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

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

### No-Tour Feature

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

The ENGAGE Web Application provides a door assignment visual counter that tracks and displays the current door assignments on each smart credential.

This door assignment counter display is an easy visual way for the Administrator to know how much space is available on the credential for future programming.

Please see the important facts and screen shot below:

#### Important No-Tour facts:

- No-Tour Smart Credentials will allow a maximum of 11 door assignments to be assigned at one time.
- Each door assignment information is stored in one of the 11 available credential sectors or folders.
- A door assignment counter is displayed when assigning access.
  - Multiple devices included in a defined “Door Group” are stored in only one (1) of the 11 available credential sectors or folders.
  - Administrators will use “Door Groups” to expand the number of doors that can be programmed onto a single credential
- Access right changes are communicated at the door when the programmed smart credential is presented to the device.
- User Scheduled access assignments are commonly used to control individual door access that is limited to a day or days, time of day, or a specific maintenance schedule.
- While programming access, the status of each credential sector is displayed as:
  - a. **Assigned** - Used, already assigned and the credential has been programmed
  - b. **Blocked** - Used, already assigned however access to this door is “DELETED”
  - c. **To be assigned** - Planned access assigned, however the credential is not yet programmed
  - d. **Free Space** - Unused, available for new access assignment

The screenshot shows the ENGAGE Web Application interface. The top navigation bar includes tabs for USERS, DEVICES, AUDITS, and ADVANCED, along with a 'NO TOUR ENGAGE 6.1' dropdown. The main content area is titled 'Assign User to Locks' and features a table of locks. The table has columns for Name, Expiration, and Schedule. The 'Name' column lists various locks, including BE467 502B, CTE 083 Lobby, CTE 103 S Laundry, CTE 137 S Laundry, CTE 141 S Garage, CTE 142 S Pool, CTE 286 S Pool, FE410 BB45, FE410 BB46, and FE410 F04A S. The 'Expiration' column shows dates, and the 'Schedule' column shows times. A 'Credential Sector Usage' section on the right displays a circular progress indicator showing 8/11 sectors filled. Annotations highlight the 'Eight doors assigned' and the 'Sector Usage now tracked and reported by ENGAGE WEB'.



## No-Tour Limitations

The No-Tour feature allows Administrators to save time and effort during daily operations, however the Administrator **MUST** be aware that door updates are dependent on the user visiting each door assigned with new or deleted access updates.

When a No-Tour user does not visit a door with updates needed, that door does not receive the new access programming.

**WARNING:** Removed accesses using No-Tour requires the updated credential to be presented at the door. A door the user fails to visit using No-Tour programming after a credential replacement or an access deletion, still allows the old or lost credential access 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.

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.

Administrators must plan for their users not to require more than 11 unique door and/or Door Group access assignments when using No-Tour functionality. Door Groups allow multiple doors to be assigned into only one sector

When door and/or Door Group assignments exceed 11, the Property Administrator is not able to use the No-Tour feature. In this case, the Administrator is required to manage access updates using the standard Sync processes per device.

## 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.

**ENGAGE TECHNOLOGY** | **USERS** | **DEVICES** | **AUDITS** | **ADVANCED** | **NO TOUR ENGAGE 6.1** | **ALLEGION**

### User Schedules

There is a maximum of 16 User Schedules provided in the free version of ENGAGE. If additional schedules or custom functionality is needed, please contact one of our Software Alliance Partners.

[+ Add New User Schedule](#)

24/7 (default)

**Contractor 1st Shift Schedule**

Access	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Begins	8:30 AM	8:30 AM	8:30 AM	8:30 AM	8:30 AM		
Ends	4:00 PM	4:00 PM	4:00 PM	4:00 PM	4:00 PM		

[Edit](#) [Deactivate](#) [Delete](#)

Deactivate - Update Locks Only  
Delete - Must update all the Credentials and Locks

Contractor Emergency Shift

Laundry Room Hours

Swimming Pool hours

Fig. 12.27: Maintenance Shift Schedule

- 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 No-Tour credential

**ENGAGE TECHNOLOGY** | **USERS** | **DEVICES** | **AUDITS** | **ADVANCED** | **NO TOUR ENGAGE 6.1**

### Users

full?, 5030

Normal, NT 5034

Normal used in  
Interaction: 5030 (top)

not 11, 16466

NT Normal, FOB 5032

NT Normal, Fresh

[+ Add User](#)

### Add New User

First Name:  Last Name:

Email Address:

ADA: ☐ OFF

Activation:  Expiration:

An expiration date of 5 years or less from the Activated date is recommended.

[Save](#) [Cancel](#)

Expire today for limited access

© 2018 Schlage Lock Company LLC [Terms and Conditions](#)

Fig. 12.28: Set Expiration for Today to Limit Access

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

- iii. different Username

### No-Tour Resident Moves Out

When a resident moves out, the Administrator may follow one of these methods for 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.

### No-Tour Door Update Policies

- Administrators should Sync all devices when removing or deleting user access to ensure all doors the user had access to are updated.
- Sync each door with No-Tour updates as a Best Practice.
  - Door updates are dependent on the user visiting each door assigned with new or deleted access updates.
  - When a No-Tour user does not visit a door with updates needed, that device does not receive the new/deleted access programming.
  - Ensuring all doors are up to date is most important when access is being deleted.

## 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.

→ **Note:** In order to add a new credential a user must first be entered into ENGAGE and there must be at least one unused Credential available.

1. **Log In.**
2. Hover over **Users** and select **Users**.
3. Select the appropriate user from the Users list.
4. From the **Users** card, select **Add Credential**.

5. The **Add Credential** card will display. Select an Existing Credential from a list of existing credentials.

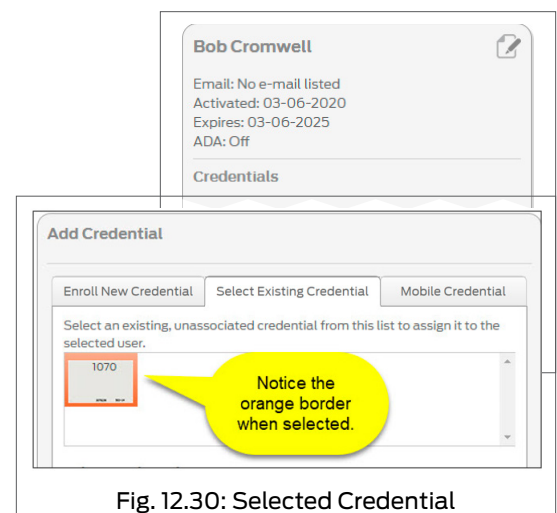


Fig. 12.30: Selected Credential

6. Under the credential section notice the Select Credential Function is set to Normal by default. Credential functions are: (See Appendix C)
  - Normal: Unlocks the lock momentarily (with a specified relock delay period).
  - Toggle: Changes the state of the lock from locked to unlocked, or vice versa.
  - Freeze: Freezes the lock in the current state. Lock remains frozen until Freeze credential is presented again. Disables all other credentials except for Pass Through.
  - One Time Use: Allows only one Normal access per assigned lock.
  - Pass Through: Unlocks a lock momentarily, regardless of state. Overrides a lock in Freeze and Lock Down states.
  - Lock Down: Changes the state of the lock to locked and disables all credentials except for Pass Through and Freeze. Present a Freeze to return lock to normal state.
  - Block: Denies access to the lock and records the access attempt as an audit.
7. Adjust the Credential Function as needed and click Save.
  - a. The selected credential is now added to the selected user.

**WARNING: Control Mobile Enabled Smart locks only: Control devices cannot relock, so a TOGGLE credential will act as a NORMAL credential when presented.**

**Add Credential**

Enroll New Credential   Select Existing Credential   Mobile Credential

Select an existing, unassociated credential from this list to assign it to the selected user.

1070

**Select Credential Function**

The credential function determines how a device will respond when this credential is presented. Select an option and a brief description of that response will be displayed.

Unlocks the lock momentarily (with a specified relock delay period).

Normal

Save   Cancel   Refresh List

Fig. 12.31: Save Credential to User



Fig. 12.32: Credential Added to User

## Assign Door Access to User

Assigning device/door access rights can be accomplished via the ENGAGE web or Mobile applications. The ENGAGE web application is preferred due to ease of data entry and larger display.

→ **Note:** In order to assign door access to a user, the user must first be entered into ENGAGE and have an assigned credential available.

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 pull-down.

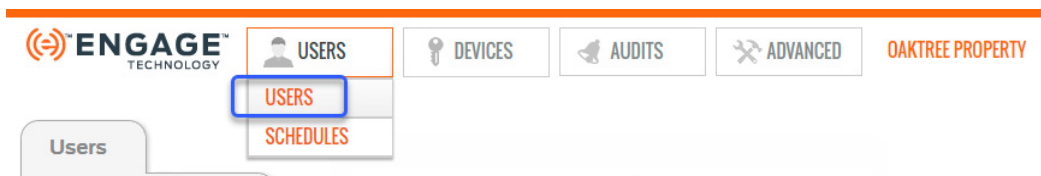


Fig. 12.33: Users &gt; Users

3. Select the **appropriate user** from the **Users** list.

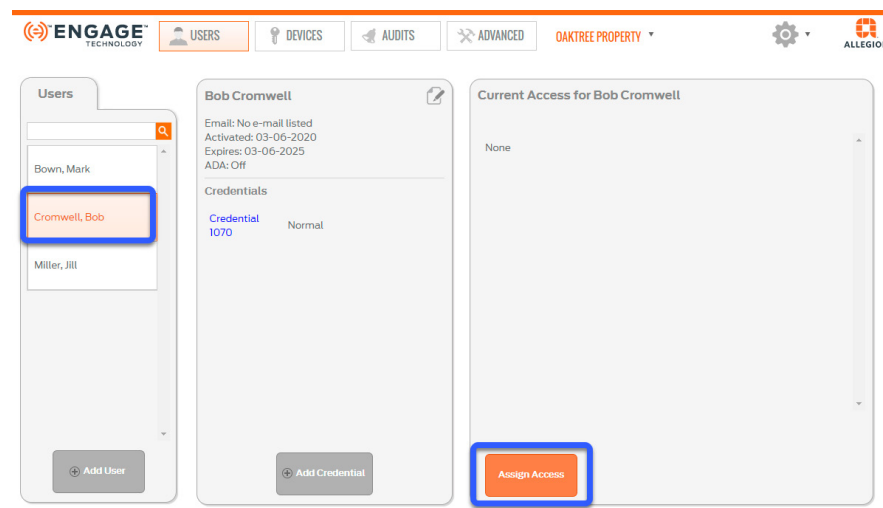


Fig. 12.34: Assign Access

4. From the users Current Access card, select Assign Access.
5. The Access screen displays the available devices that may be assigned.
  - Individual devices are shown by default under Device.
  - Device Groups are displayed under Groups.

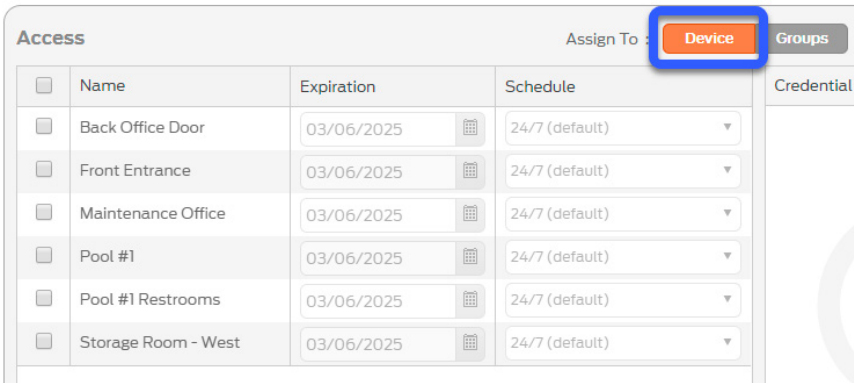


Fig. 12.35: Individual Device selections

6. From the default Device screen, check the individual devices the user requires access.
  - a. If desired, adjust the access Expiration date.
  - b. When the user does not require 24/7 access,
    - i. Select applicable access from the Schedule pull-down list.

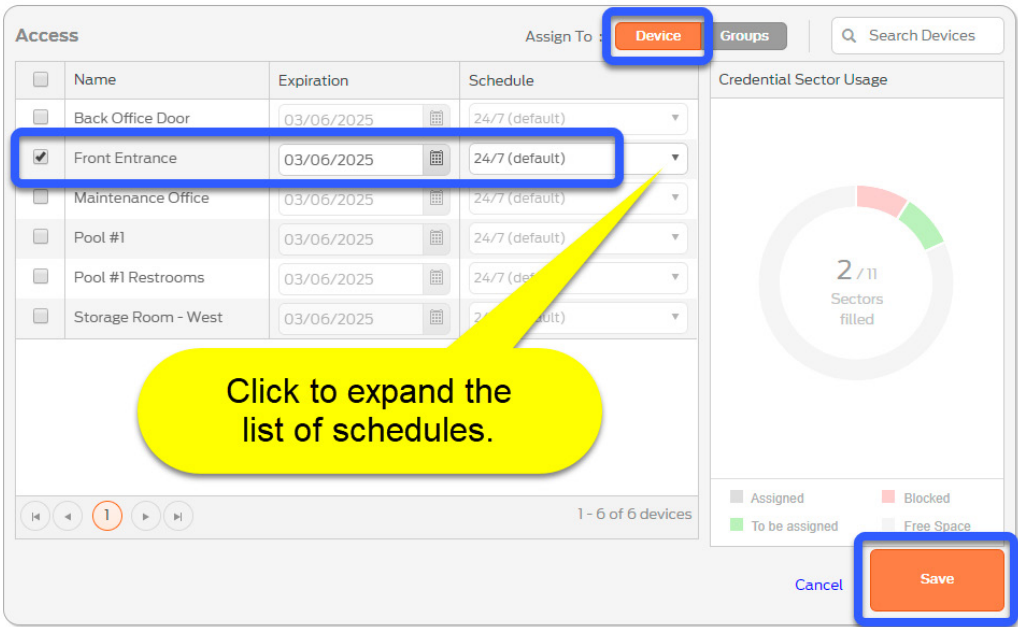


Fig. 12.36: Device Screen

7. From the Group screen, check the define Door Group(s) the user requires access.

Access

Assign To : Device **Groups**

<input checked="" type="checkbox"/>	Name	Expiration	Schedule
<input checked="" type="checkbox"/>	Pool Access for Residents	03/06/2025	Pool #1

Click to expand the list of schedules.  
This pool schedule allows access Mon-Sun from 6 am to 11 pm.

Credential Sector Usage

3 / 11 Sectors filled

Assigned Blocked  
To be assigned Free Space

Cancel Save

Fig. 12.37: Device Group selections

- If desired, adjust the pre-defined access **Expiration** date.
- When the user is not allowed 24/7 access, **Select** an applicable schedule access from the **Schedule** pull-down list.

**WARNING:** The Credential Sector Usage fills up as access assignments are defined. No-Tour programming allows ONLY 11 Door/Door Group assignments per credential. A user can have no more than 11 doors and/or Door Groups assigned to their credential. Credential programming is required after updates are made. The No-Tour feature will then make the changes when the credential is presented at the door when presented.

- In this example, the user is assigned Pool Access for Residents.

→ **Note:** By default, Expiration is set to 5 years from the date the user was first defined in ENGAGE. Administrators may adjust the Expiration date on a per lock basis at any time.

#### 8. Select Save.

- A '**Lock access updated**' and **current access** is displayed.
  - The **currently defined access** for the user displays.
    - The **Pool #1 Restrooms** and **Pool #1** access are assigned from the Door Group assignment.
    - The **Front Entrance** access is assigned as an individual device.
  - The user's credential displays an **Update** ICON and the username update **exclamation point** icon is shown.
    - Be sure to update the credential for access programming

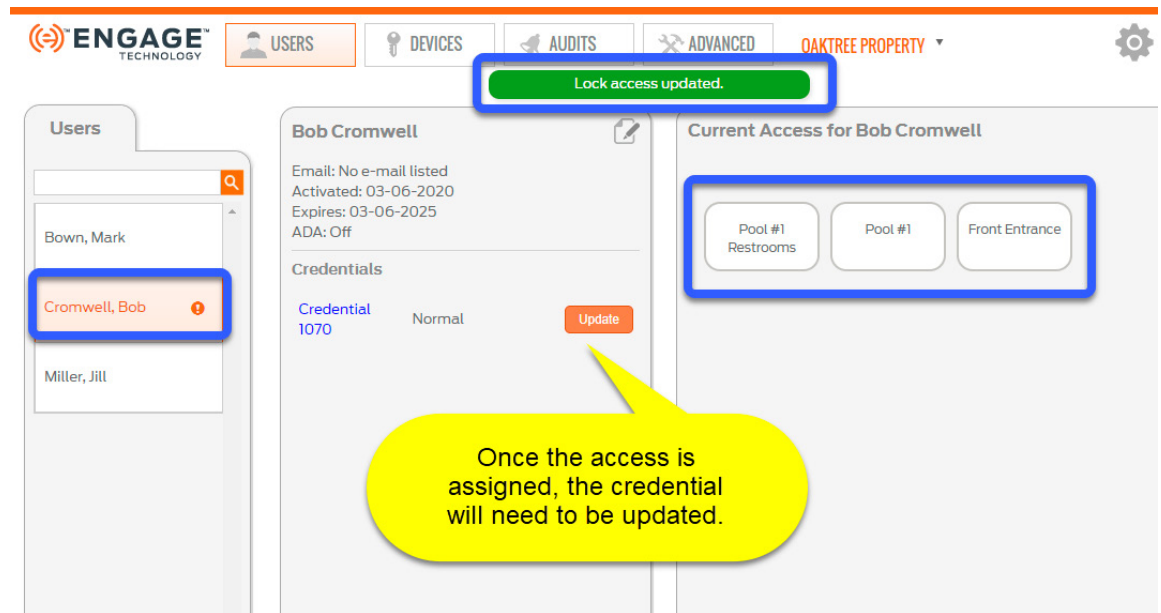


Fig. 12.38: User Lock Access

→ **Note:** Anytime the “Update” notice is presented. The credential has new or updated access rights ready for programming into the credential. The administrator must program the changes into the users’ credential before the updates can be carried to the effected doors by the user. Alternatively, the Administrator may choose to wait until “Tomorrow” when automated “Overnight Updates” can be accomplished.

### Update Credential: No-Tour Programming

Once access updates have been made to a user’s access rights, the user’s credential must be programmed with the changes or the newly assigned access rights will not be honored.

1. Obtain the users’ No-Tour credential to be programmed with new changes.
2. Ensure the MT20W credential reader is powered up ready for use with the “Blue” LED illuminated on solid.
3. From the appropriate users’ account, click the **Update** button.
  - a. This starts the **Update Credential** process.

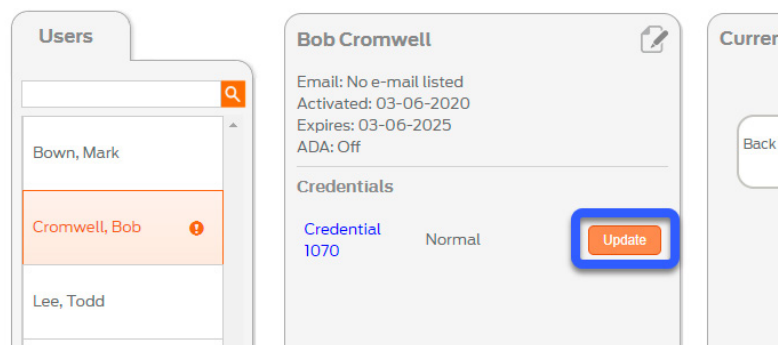


Fig. 12.39: Update Button

4. Follow the ENGAGE “Update Credential” instructions provided.
  - a. Place the users’ credential (or fob) on the reader.
  - b. Wait until the MT20W beeps and blinks **GREEN** 3 times
  - c. Then click **Next**.



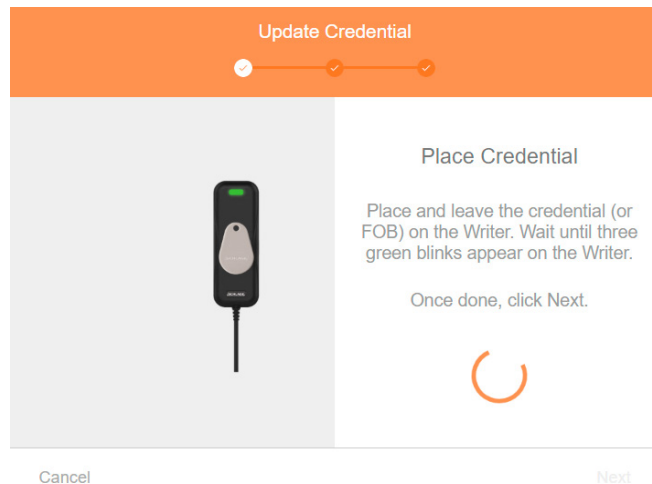


Fig. 12.40: Update Credential

5. The new credential information will be **retrieved** and when complete, the credential will be updated **successfully**.
  - a. Click **Finish** and **remove** the credential from the reader.
  - b. The user's credential and User account has now been updated.

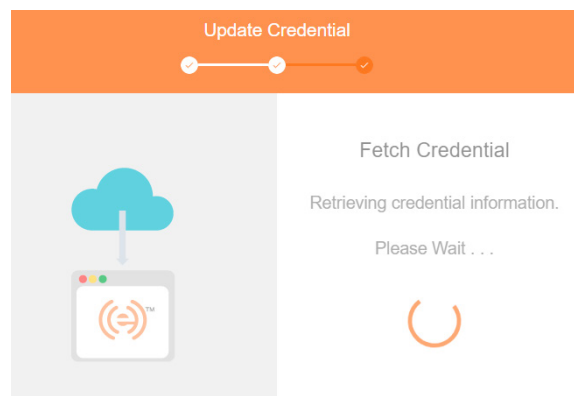


Fig. 12.41: Retrieving Information

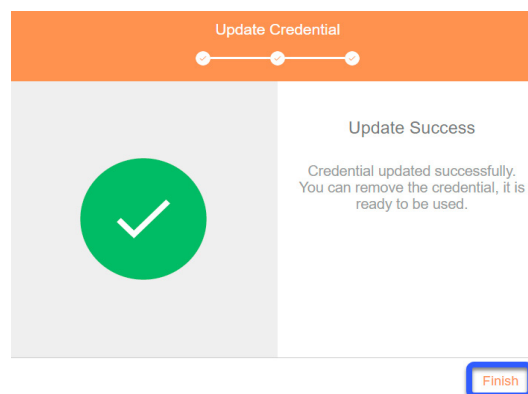


Fig. 12.42: Update Success

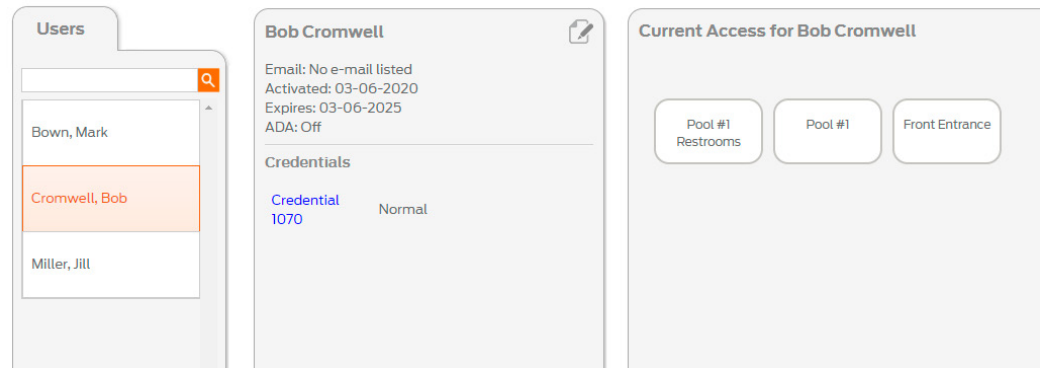


Fig. 12.43: Updated User Account

**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.

### 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

- c. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
6. Select **Advanced** menu, then the **Credentials** tab.

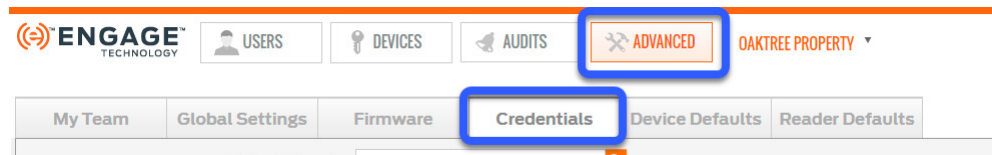


Fig. 12.44: Advanced &gt; Credentials

7. In the **Badge ID Search** field;
  - a. Enter the numbers after the dash located on the credential. In this case **1070**
  - b. Click the **magnifying glass icon**.

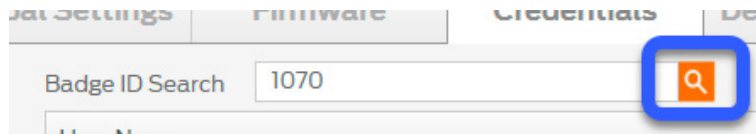


Fig. 12.45: Badge ID Search

8. Results:
  - a. **If found**, name of owner will appear.
  - b. **If not found**, error message appears.
    - i. Click **OK** and try again.



Fig. 12.46: ID Found

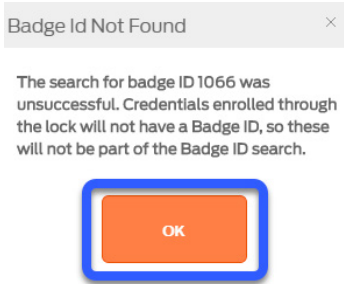


Fig. 12.47: ID Not Found

**WARNING:** If a credential is enrolled using an installed device ([enroll at a door](#)) the credential is NOT searchable in the ENGAGE application. Only credentials enrolled [individually](#) or [in bulk](#) using the MT20W or MT20 credential enrollment readers are searchable in the ENGAGE application.

## Mobile Credential Overview

Mobile Access Credentials will allow the physical access credential cards or fobs normally carried by a user to be replaced with a Mobile Credential that is embedded in the user’s Mobile phone and uses Bluetooth communication to work with ENGAGE Mobile enabled devices.

Mobile Access Credentials are available for both iOS and Android Mobile devices and require a free Mobile application to be used to manage the Mobile Credential on your Mobile phone.



Fig. 12.48: Mobile Access Credential

Users with Mobile Access Credential assignment will no longer need to use physical credentials to gain access to their assigned openings, however both credential types (Physical and Mobile) may be assigned to the same user if desired.

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

When Mobile Credential access is desired, the Administrator must ensure that the devices in the property, where Mobile Credential use is desired, are Mobile Device enabled.

**WARNING:** Be aware that ENGAGE devices were not initially Mobile Enabled. The devices on your property may need to be updated to include Mobile Access Credential support. The original wall mounted MT readers used with CTE cannot be upgraded for Mobile Enabled MTB compatibility. Control, NDE80 and LE devices may be updated with update kits to enable Mobile Device compatibility

Complete lock replacements are not necessary, each product has an upgrade kit to replace the critical components and reuse most of the original lock.

### Enroll New Mobile Access Credential

Administrators must enroll a user Mobile Access Credential within the ENGAGE system.

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.
3. Select the appropriate user from the Users list.
4. From the Users card, Select Add Credential.
5. From the Add Credential card, Select Mobile Credential.
6. In the Mobile Phone Number field, enter the user's Mobile phone number.
7. When finished, click Save.

The screenshot displays the ENGAGE web application interface. At the top, there is a navigation bar with the ENGAGE logo and several menu items: USERS, DEVICES, AUDITS, and ADVANCED. The 'USERS' menu is currently selected. Below the navigation bar, the 'Users' section is visible, showing a list of users. The user 'Test, Test' is highlighted with a blue box. To the right of the user list, the 'Add Credential' button is also highlighted with a blue box. The 'Add Credential' modal is open, showing the 'Enroll New Credential' tab. The 'Mobile Credential' option is selected, and the 'Free Trial' offer is displayed. The 'Enter Mobile Phone Number' section is highlighted with a blue box, showing a text input field with a dropdown menu for the country code (set to '+1') and a text input field for the phone number. The 'Save' button is highlighted with a blue box at the bottom of the modal.

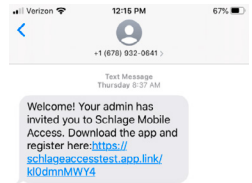
Fig. 12.49: Mobile Access Credential

→ **Note:** The Mobile Access Credential introductory offer is a “Free Trial” through 2020 to encourage early adoption. Pricing for Mobile Credentials is pending and will be a “pay-as-you-go” pricing structure.

## Download and Install the 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

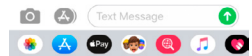
User will receive a text message and instructed to download the application from the App Store or the Google Play Store.



1. Download the **Schlage Mobile Access** application and the user Mobile Credential

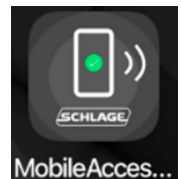
→ **Note:** The User will receive an automated TEXT message with additional instruction after selecting **Save** in the step above:

→ **Note:** This link is unique for the User and will take the User to the appropriate "Application Store" to download the Schlage Mobile Access application. If the user already has the **Schlage Mobile Access** application downloaded, this link will just open the application.



2. Once the Schlage Mobile Access application is installed, locate the **Schlage Mobile Access** icon on the Mobile device application screen and open the application.

→ **Note:** Internet connection is required while downloading the Mobile application and the Mobile credential details, completing this setup process. After initial setup, internet connection is no longer required. Internet or cell service is not required when using the Schlage Mobile Access application for general access and daily use.

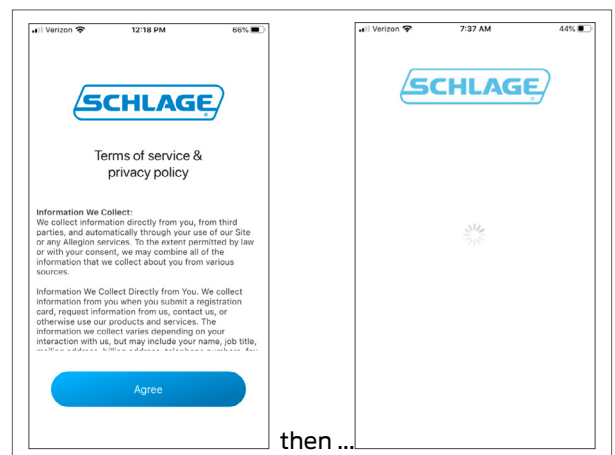


3. The User must **Agree** to the Terms of Service and Privacy Policy

- Wait a few moments while the Mobile Credential data is being downloaded to the Mobile phone.

→ **Note:** The Mobile Credential is being downloaded during the spinning indication. Be patient, this could take up to 15 seconds to complete

- The user is then required to allow additional Mobile Phone services on their Mobile phone. Both iOS and Android devices will require Bluetooth capabilities and will ask to enable Bluetooth. Android devices (only) will also require Location Services to be enabled.



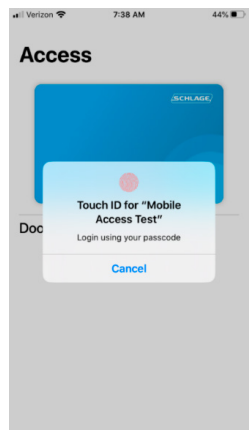
- Schlage Mobile Access application will require the user to set up one form of application security: Passcode, TouchID, or FaceID

→ **Note:** Mobile devices used with the Schlage Mobile Access application are required to have at least one level of security to protect against a misplaced Mobile phone.

4. Once the Schlage Mobile Application is downloaded and successfully setup on the Users Mobile device, the user will have Mobile Credential access to any Mobile Enabled doors.

- Remember, Doors must be updated (**Sync**) with the new access permissions

→ **Note:** The user must download and install the Schlage Mobile Access application in order to use an assigned Mobile credential. Mobile Credentials will be initially provided free of charge. This Free trial period will end at some point in the future, but for now enjoy the Mobile Credential convenience for free. Only one Mobile Credential can be assigned to a user at a time. Additional physical credential assignments are allowed. Users intending to receive a Mobile Credential must use a compatible smart phone device and compatible Operating System Software: Android devices with **6.0** Operating System or higher; iOS devices with **11.1** Operating System or higher.



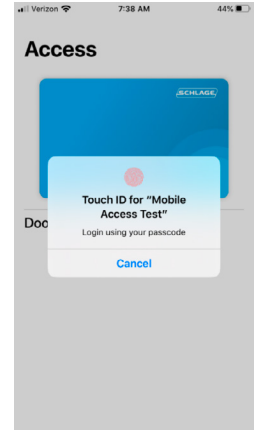
To favorite a door, swipe right and tap the heart icon. Favorite doors will show up at the top of the list.

### Use the Access Mobile Application to Access Openings

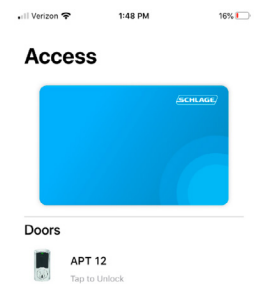
After users have downloaded, installed and setup the Schlage Mobile Access application, they can begin to access assigned doors using their new Mobile Credential.

To access an assigned door, users will follow these simple steps.

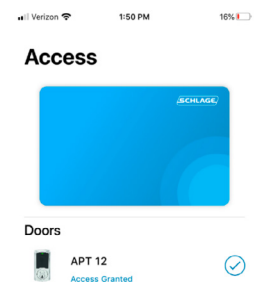
5. **Open** the Schlage Mobile Access application on their Mobile phone.
  - Notice one level of security is required.
6. **Approach** an assigned door to within a few feet



7. **View** the available Mobile Enable devices that are nearby. (Apt 12)
  - A screen "Refresh" may be needed
8. **Select** the desired device by its "Friendly Name" (Apt12).
  - The name is shown as entered by the Administrator in ENGAGE



9. **Wait** a moment for the door to momentarily unlock and enter.
  - Mobile Credentials are NORMAL function and the door will automatically relock again after the programmed Relock Delay period has expired.



## Device Groups Overview

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

Creating a Device Group reduces the number of sector (or folder) assignments on a user 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.

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.

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

### Create a Device Group

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Select the Devices menu, then Device Groups in the pull-down list.



Fig. 12.50: Devices > Device Groups

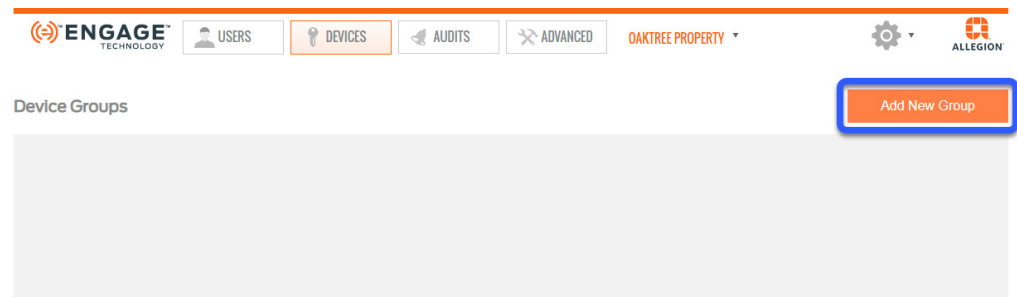


Fig. 12.51: Add New Device Group

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

Add New Device Group

Name

Pool Access for Residents

Description

Residents have access to the pool door and pool restroom doors. This access DOES NOT include doors for the pool storage or maintenance rooms.

Save

Fig. 12.52: Descriptive Device Group

5. **View** the newly created Device Group in the **Device Groups** list.
- Doors still need to be assigned into the Door Group

ENGAGE TECHNOLOGY

USERS

DEVICES

AUDITS

ADVANCED

OAKTREE PROPERTY

Settings

ALLEGION

Device group added successfully

Device Groups

Add New Group

Pool Access for Residents

Pool Access for Residents

Residents have access to the pool door and pool restroom doors. This access DOES NOT include doors for the pool storage or maintenance rooms.

Assigned Devices

No devices assigned to this group

Fig. 12.53: Saved Device Group

Assign Doors to Device Group

1. From the newly created **Device Group**, select the plus sign (+) to assign individual doors into this door group.

Pool Access for Residents



+

Residents have access to the pool door and pool restroom doors. This access DOES NOT include doors for the pool storage or maintenance rooms.

Fig. 12.54: Assign Doors

2. From the **Assign devices** screen, select the appropriate door(s) to be assigned to the group.



-  **Select** a desired device from the **Unassigned Devices** list.
- Click the greater than sign  to move device to the right and into the **Assigned Devices** list.
- Continue to add devices to the **Assigned Devices** list as needed.
- When finished, click **Save**.

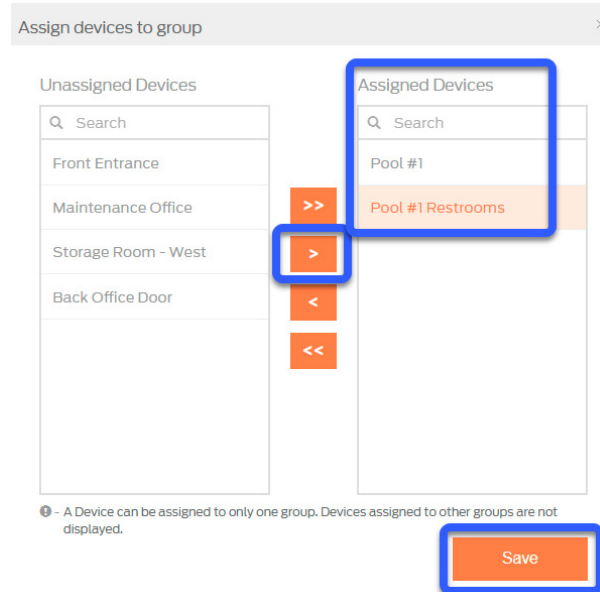


Fig. 12.55: Assign Devices Screen





	<b>Include all</b> Unassigned Devices to the Assigned Devices list.
	<b>Include one</b> Unassigned Device to the Assigned Devices list.
	<b>Exclude one</b> device from the Assigned Devices list.
	<b>Exclude all</b> devices from the Assigned Devices list.

Fig. 12.56: Symbols

**WARNING:** A device can be included in **ONLY** one Device Group. Devices cannot be assigned into multiple Device Groups. Devices already assigned to another Device Group will not be listed for selection. 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.

3. A 'Devices for group updated successfully' message appears.
  - The Device Group also now displays the **Assigned Devices**.

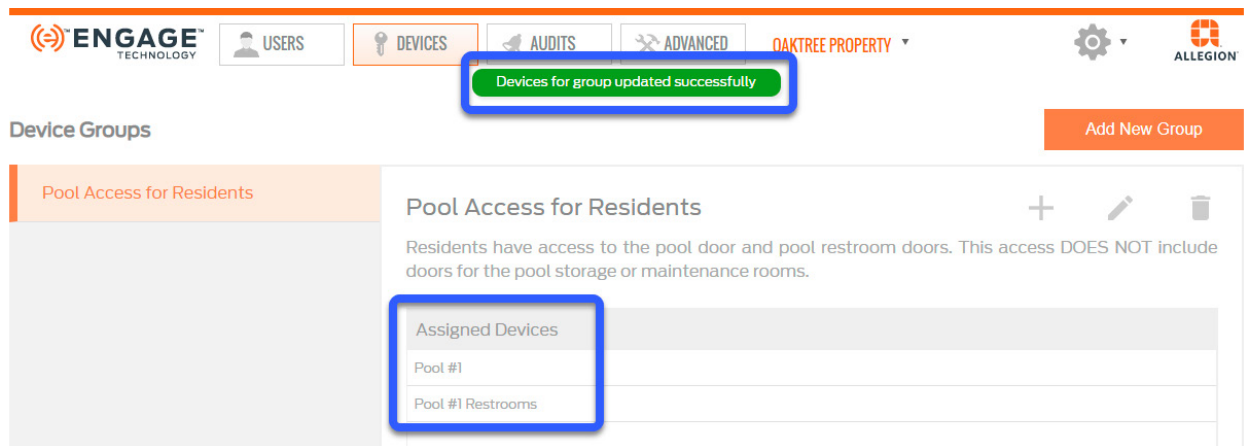


Fig. 12.57: Assigned Devices in Device Group

### Next Steps for Assigned Devices

After devices have been assigned to a Device Group, each device added to the Device Group must be updated or Sync process performed.

Also, each device that was previously assigned to a Device Group and subsequently deleted must be updated or Sync process performed.

Perform the following steps to update credentials and device assignments.

1. Assign the Device Group to the appropriate users.
2. Update the User credentials with the new Door Group assignments.
3. Sync all affected doors to program new Door Group definitions to the doors.

**WARNING:** User Credentials programmed to the Device group do not allow access until a device Sync is successfully completed at the door AND the User Credential has been programmed with the new access. Any device/lock deleted from a Device Group will still allow access until a device Sync is successfully completed to remove the lock from the Device Group. LE, NDE, and CTE devices that are connected to the local Wi-Fi network may be updated with the newly defined Device Group assignments during the next successful nightly Wi-Fi update.

## 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.

Administrators will want to follow these processes to keep their credentials ready for immediate reuse.

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 “Door Group(s)” 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 Door 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 ENGAGE 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.

## 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. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Hover over **Users** menu and select **Users**. pull down
3. Select the appropriate user from the **Users** list.
4. From the **Current Access** card, select **Assign Access**.

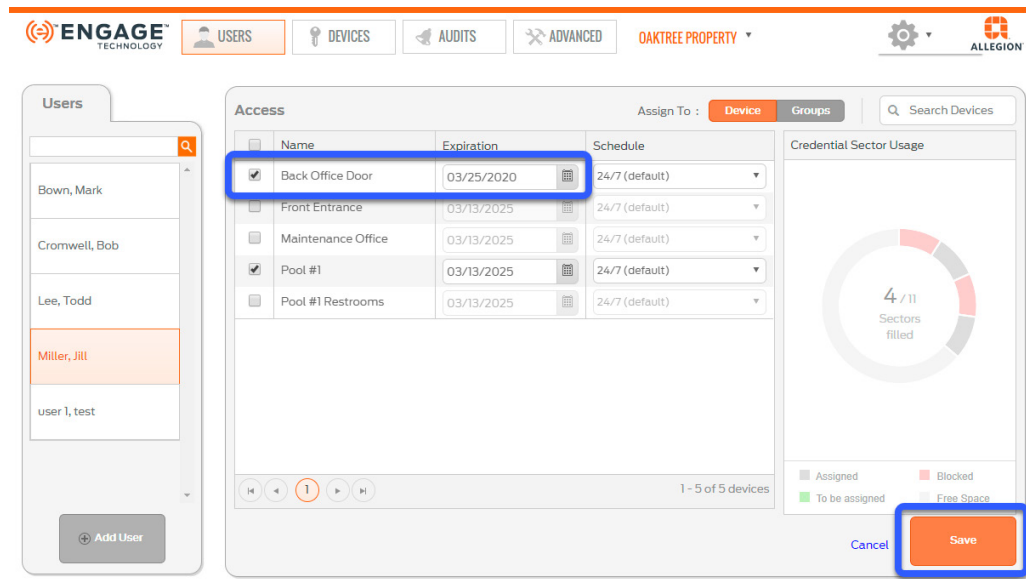


Fig. 12.58: Set Expiration Date to Expire “Today”

5. From the **Assign To:** button: select **Device**, set each of the assigned individual lock **Expiration** to the current “Today’s” date.
6. From the **Assign To:** button: select **Groups**, set each of the assigned Door Groups **Expiration** to the current “Today’s” date.
7. **Select Save** to update the credential details.
8. To complete this process, the credential must be updated with “today’s” expiration setting and then stored away until “Tomorrow”.
  - a. Follow the [update the credential](#) 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.

## 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.

**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.

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Hover over **Users** and select **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.

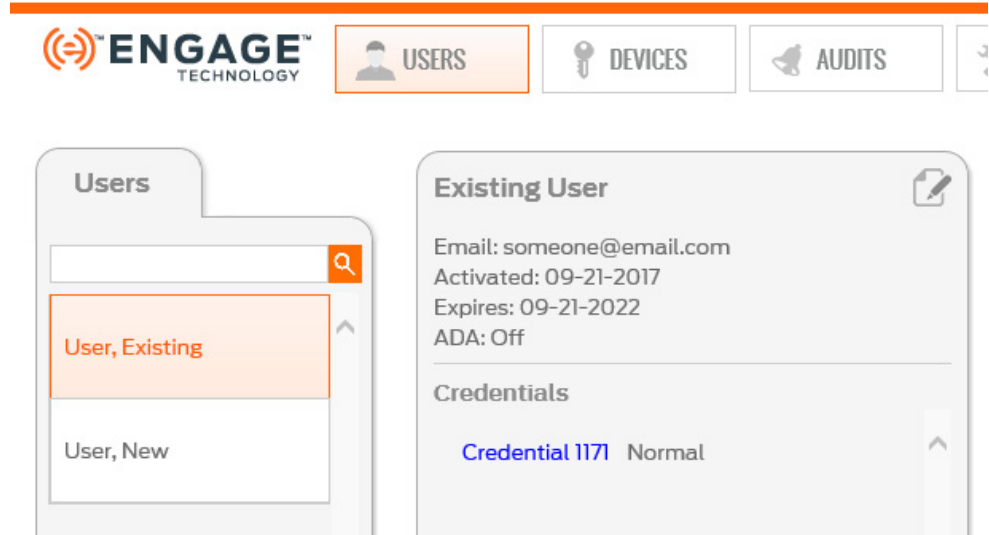


Fig. 12.59: Select Credential

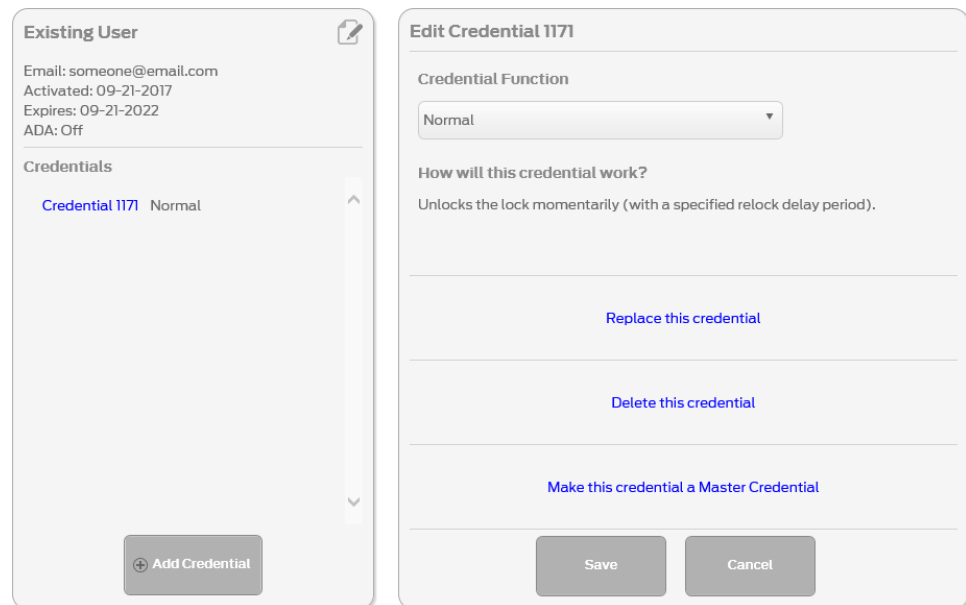
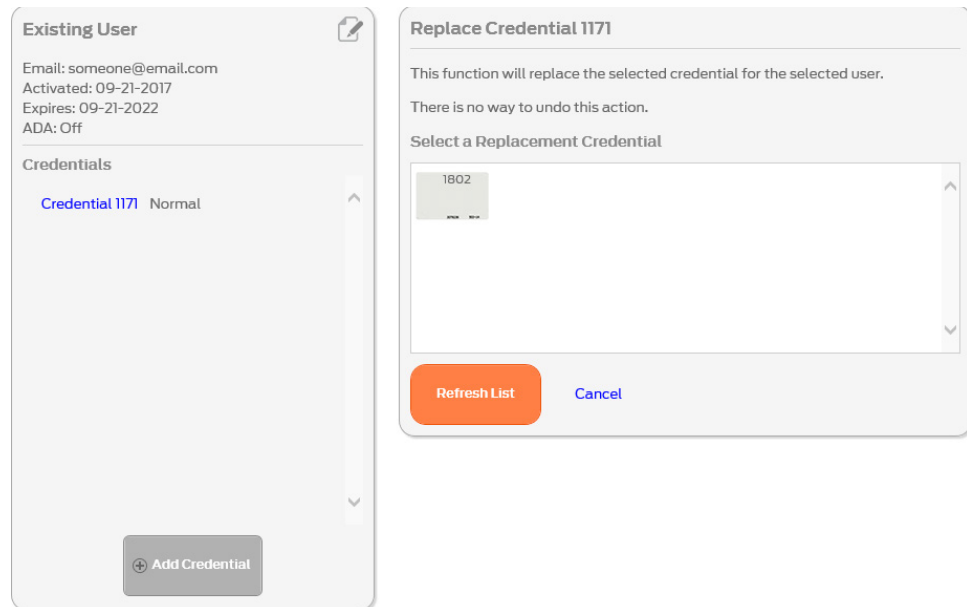


Fig. 12.60: Edit Credential Card

5. Select **Replace this credential**



**Existing User**

Email: someone@email.com  
Activated: 09-21-2017  
Expires: 09-21-2022  
ADA: Off

**Credentials**

**Credential 1171** Normal

**Replace Credential 1171**

This function will replace the selected credential for the selected user.  
There is no way to undo this action.

Select a Replacement Credential

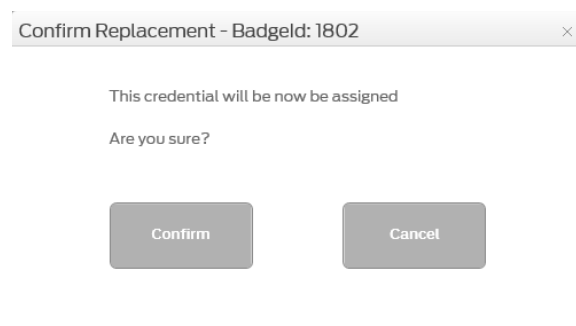
1802

Refresh List Cancel

→ **Note:** If no credentials are available for replacement, you must enroll a credential now.

6. **Select** a Replacement Credential from stock list.
  - In this case we chose the only available, Credential #1802.

**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.



Confirm Replacement - Badgeld: 1802

This credential will be now be assigned

Are you sure?

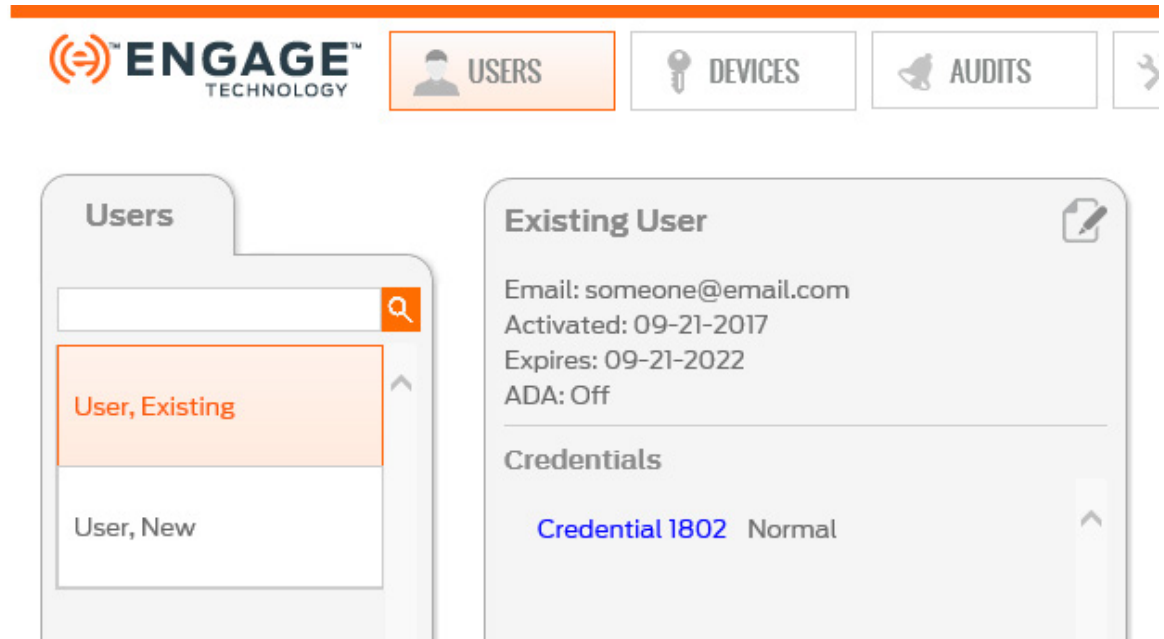
Confirm Cancel

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

Credential Replaced Successfully

9. The new **Credential 1802** is now listed under the **Existing User** Credentials and the old "Replaced" credential (1171) has been removed from the list.

Update



**WARNING:** The **ICON** **Update** by the credential indicates the credential now needs programming with the Schlage MT20W.

### Resident Move Out Processes

When a resident moves out, it is important to recover the credentials and plan for the credentials next use.

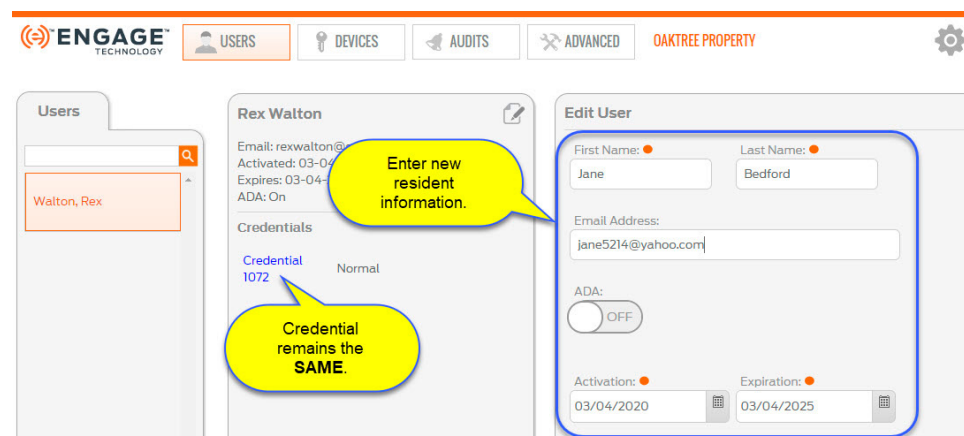
The Administrator may follow one of these methods for credential reuse.

#### New User Waiting for Space & 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. In the ENGAGE application under the previous resident's User record, edit and remove the previous resident's name and reenter the name of the new resident.
2. Edit the Email Address, ADA, and the Activation and Expiration dates as needed.
3. Click **Save**.

Fig. 12.61: Update Resident Name



4. Hand the updated 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.

#### **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 Door Assignments" section above.


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.

#### **Remove User and Access from ENGAGE**

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

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

1. Open the ENGAGE™ Web Application.
2. Select the USERS tab and the specific User to have be removed and credential deleted on the Users tab.
3. Follow the "Clearing access assignments on existing credentials" section to set the credential to expire "Tomorrow".
  - This will make all 11 door assignment sectors available when the credential is reused.
4. After the credential has expired, the user may now be Deleted.
5. Select the user to be deleted. (Existing User).

The screenshot shows the ENGAGE Technology interface. At the top, there is a navigation bar with the ENGAGE logo and three tabs: 'USERS' (selected), 'DEVICES', and 'AUDITS'. Below the navigation bar, there are two main panels. The left panel, titled 'Users', contains a search bar and a list of users. The 'User, Existing' entry is highlighted with an orange background and an exclamation mark icon. The right panel, titled 'Existing User', displays user details: Email: someone@email.com, Activated: 09-21-2017, Expires: 09-21-2022, and ADA: Off. Below the details is a section titled 'Credentials' which lists 'Credential 2886' with a 'Normal' status and an exclamation mark icon.

6. Select the credential to be deleted from the Credentials list to continue. (2886)

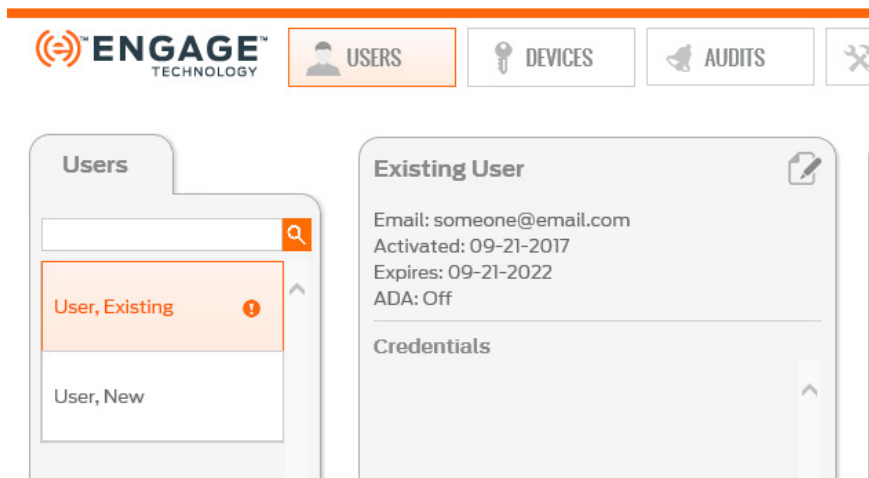
The screenshot shows the 'Edit Credential 2886' card. The card displays the user details from the previous screen. Below the details is a section titled 'Credentials' which lists 'Credential 2886' with a 'Normal' status and an exclamation mark icon. At the bottom of the card is a button labeled 'Add Credential'. The right panel, titled 'Edit Credential 2886', displays the 'Credential Function' dropdown menu set to 'Normal'. Below the dropdown is a section titled 'How will this credential work?' which states 'Unlocks the lock momentarily (with a specified relock delay period)'. Below this section are three buttons: 'Replace this credential', 'Delete this credential' (selected), and 'Make this credential a Master Credential'. At the bottom of the card are two buttons: 'Save' and 'Cancel'.


7. Select Delete this credential in the Edit Credential card.



The screenshot shows two side-by-side panels. The left panel, titled 'Existing User', displays user information: Email: someone@email.com, Activated: 09-21-2017, Expires: 09-21-2022, and ADA: Off. Below this is a 'Credentials' section with a list containing 'Credential 2886' with a 'Normal' status and a red exclamation point icon. At the bottom is an 'Add Credential' button. The right panel, titled 'Delete Credential 2886', contains a warning: 'This function will delete the selected credential from the selected user. There is no way to undo this action. If a credential is accidentally deleted, simply recreate it. To help prevent accidentally deleting, please enter 'DELETE' into the confirmation field below.' It features a 'Confirm:' label, a text input field containing 'delete', and 'Delete' and 'Cancel' buttons.

8. Type the word 'delete' into the Confirm: Field.
9. Select the Delete button.
10. VERIFY SUCCESS: When successfully deleted, the Credential is no longer listed under Credentials.



**WARNING:** Deleting a credential requires all devices that previously had access with that credential, to Sync, overnight updated or perform No-Tour programming before the deleted credential is denied access at the door. ENGAGE Web Application displays the exclamation point "Update" ICON  to indicate which doors with deleted access, require programming.

### Delete User Access Rights

When a user needs to modify access to the currently existing access assignments to remove an individual door access.

Additionally, Sync is required for each door the credential originally had access to.

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Select Users menu, then the Users pull down.

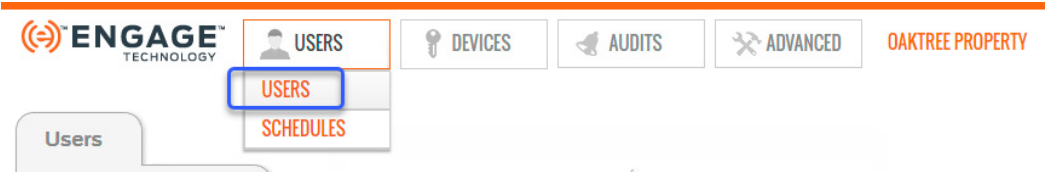


Fig. 12.62: Users > Users

- 3. Select a User for the removal of access.
- 4. Select Assign Access.

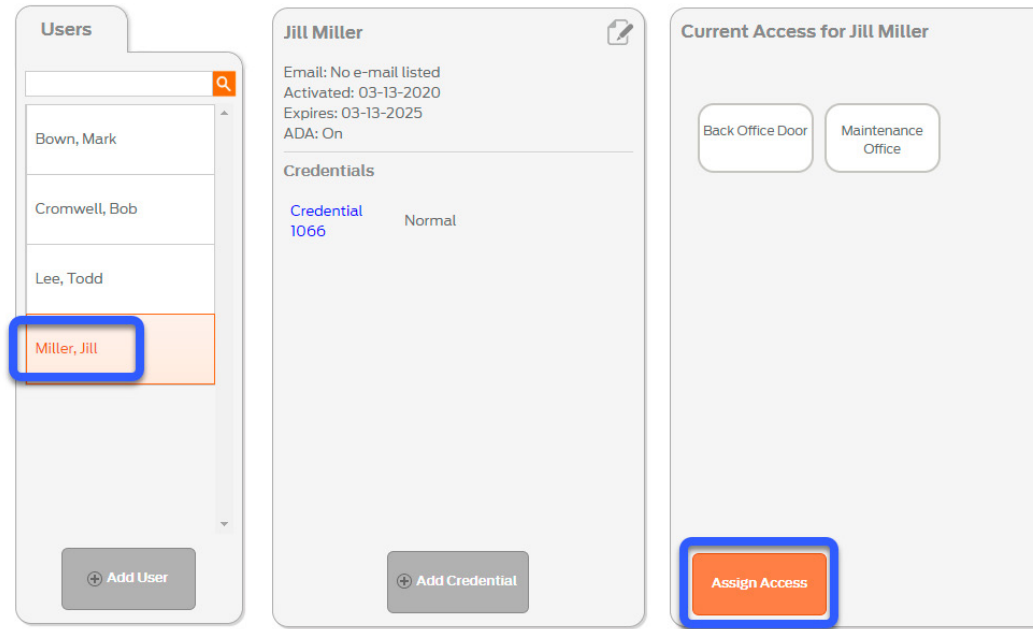


Fig. 12.63: User Account

- 5. From the Device screen, uncheck the name of the device to remove access to the opening(s).
- 6. If needed, continue to remove Door Group access from the Groups screen.

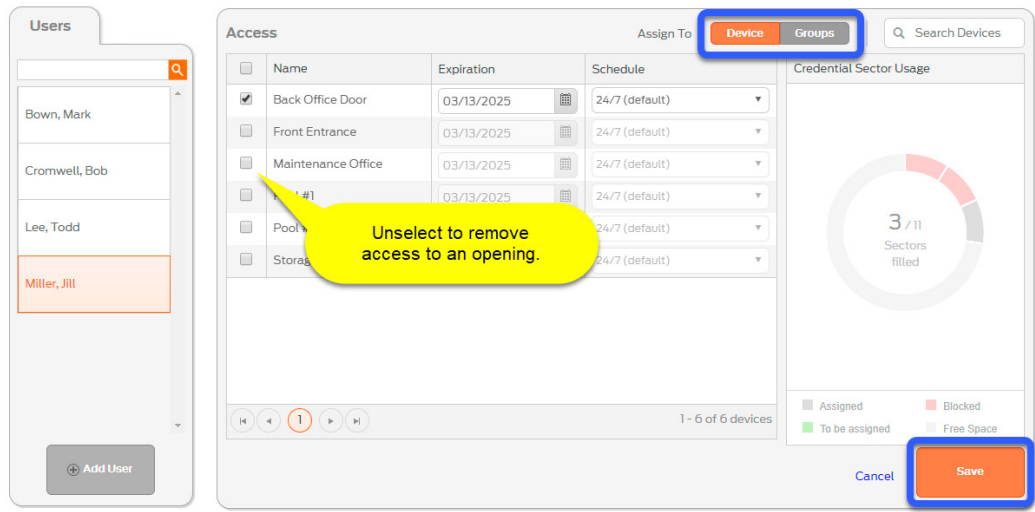


Fig. 12.64: Remove Access

- 7. When finished click Save.
- 8. A 'lock access updated' message appears.
  - a. Selected opening no longer appears as current access.

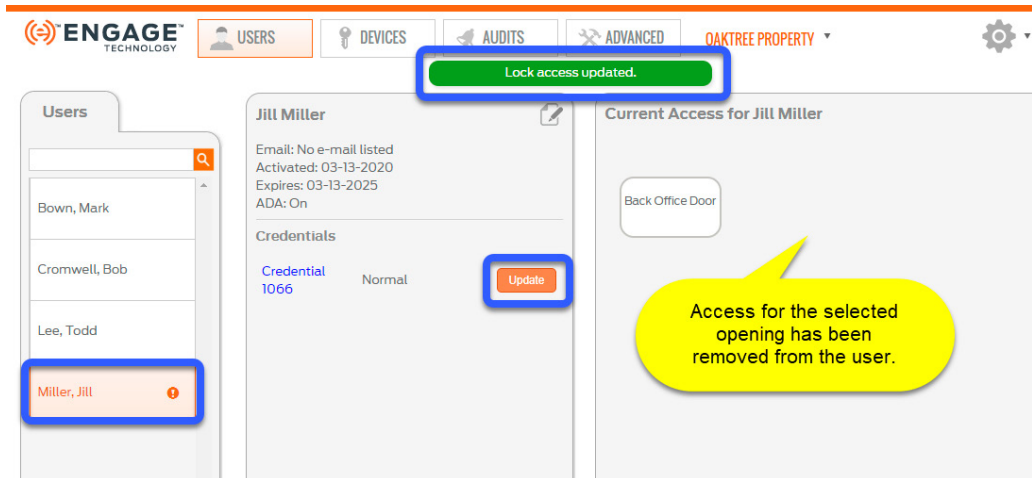


Fig. 12.65: Access Removed

**WARNING:** Deleting a credential requires all devices that previously had access with that credential, to Sync, overnight updated or perform No-Tour programming before the deleted credential is denied access at the assigned door.

#### Delete User Physical Credential

When a user no longer needs a physical credential, the credential should be cleared of current programming. Then the credential can be deleted from the user's account and stored away for reuse. Additionally, after the credential has been deleted, Door updates (Sync, overnight updates or No-Tour) is required to remove access for each door that the credential originally had access.

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account.
2. Select **Users**, then **Users**.

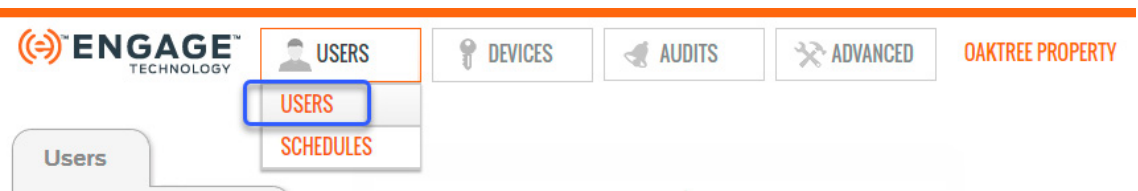
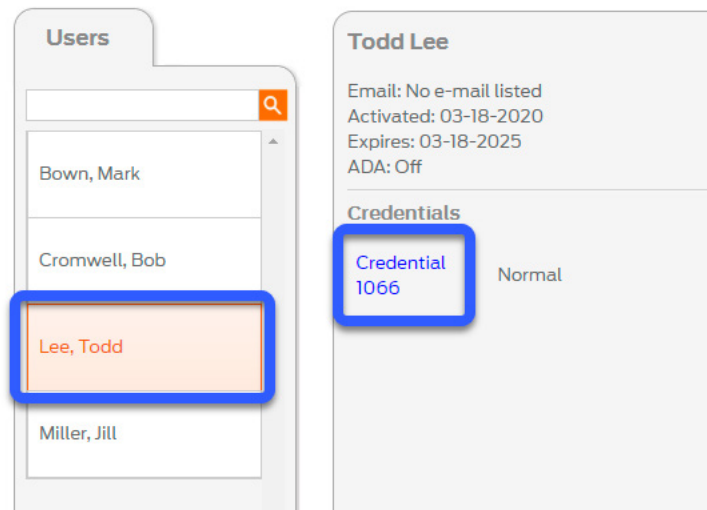
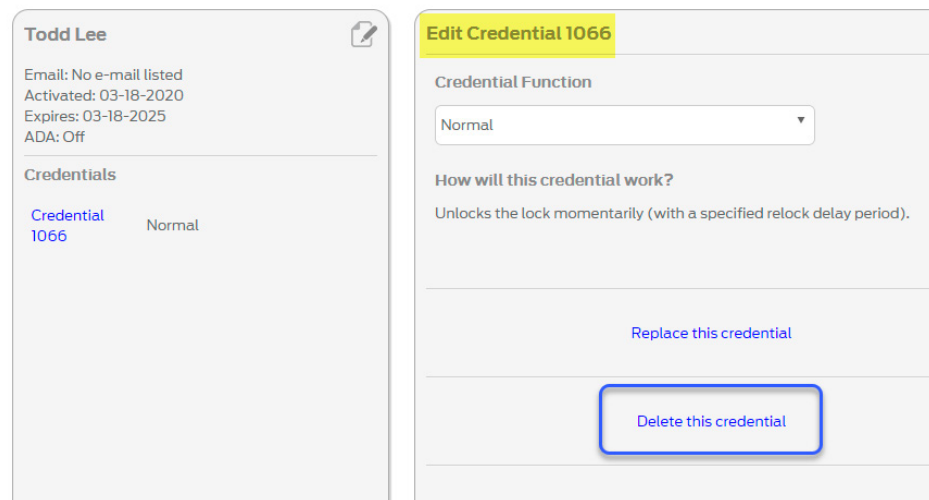


Fig. 12.66: Users &gt; Users

3. Select a **User** for deletion of a credential.
4. From the user's card, select the **credential to be deleted**.

**Fig. 12.67: User Account**

5. From the Edit Credential card, select **Delete this credential**.

**Fig. 12.68: Delete This Credential**

6. From the Delete Credential card, enter **delete** in the confirm field.
  - a. There is no way to undo a deleted credential, except to reassign the credential as new again.
  - b. When finished, **Select the Delete button**.

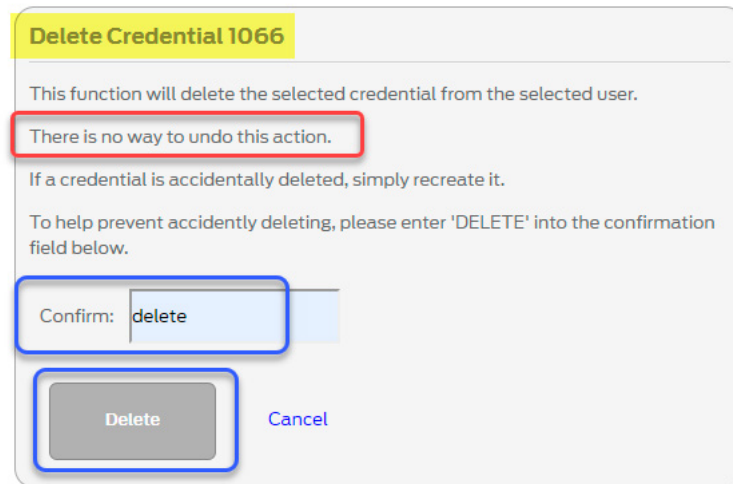


Fig. 12.69: Confirm Delete

7. A 'credential deleted' message appears.
  - a. The credential is no longer associated with the user and does not appear on the user's account.

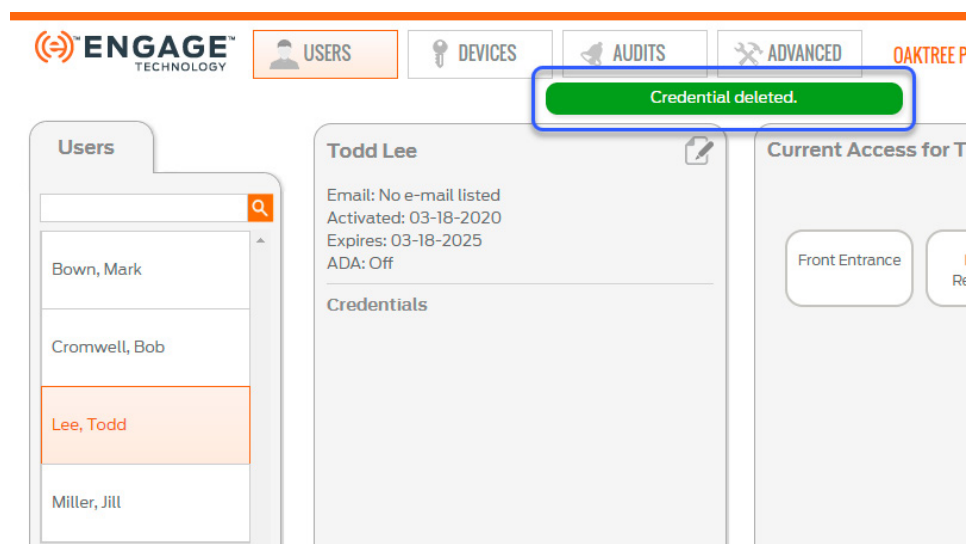


Fig. 12.70: Credential Deleted


## Using Master Credentials

### Overview

Serious consideration and consultation with local authority should be done BEFORE enabling and generating Master Credentials.

### IMPORTANT NOTES:

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

 **WARNING:** 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.

 **BEST PRACTICE:** Enable this setting before commissioning any devices.

 **BEST PRACTICE:** Destroy any Deleted Master Credentials.

## Enable Master Credential in ENGAGE

- **Add/Delete Users** to become the Master Credential holder.
- **Assign Credentials** to the User, to become the Master Credential.
- **Assign a Credential as Master.**
- Update each lock on the property by **Sync: Overnight Wi-Fi Updates**.

1. **Log In**
2. Select the **ADVANCED** menu and **Global Settings** tab.

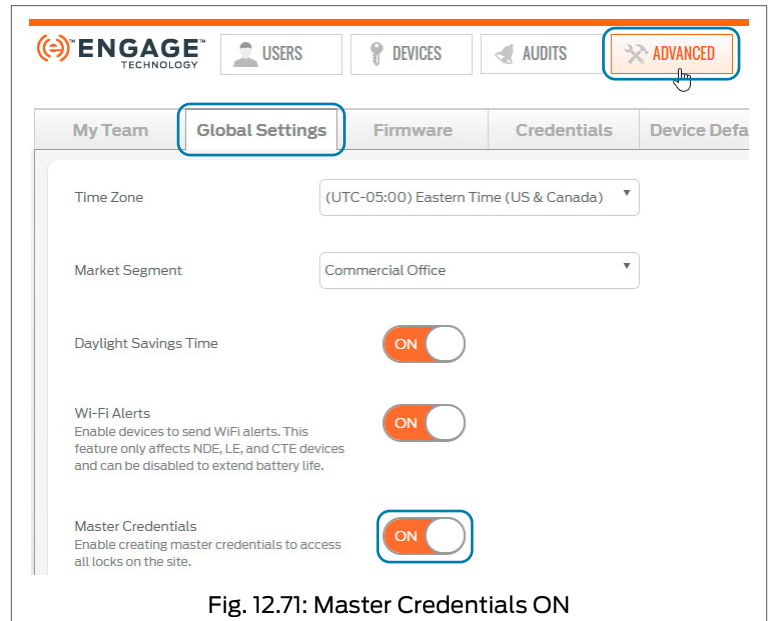


Fig. 12.71: Master Credentials ON

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.

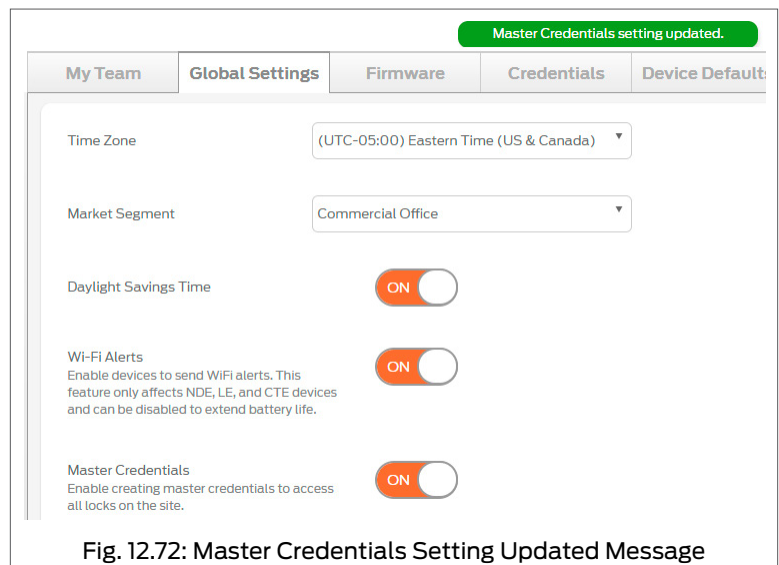


Fig. 12.72: Master Credentials Setting Updated Message

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** the **BLUE** currently assigned credential that is to become a MASTER CREDENTIAL.

If the **Make this credential a Master Credential** is NOT available, the feature has not been enabled yet. **Enable Master Credential in ENGAGE** 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.

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.

**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.

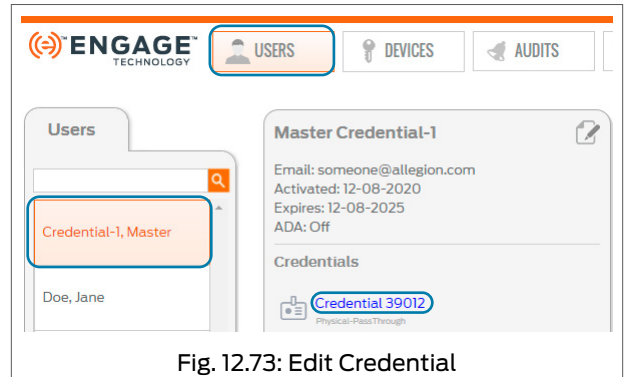


Fig. 12.73: Edit Credential

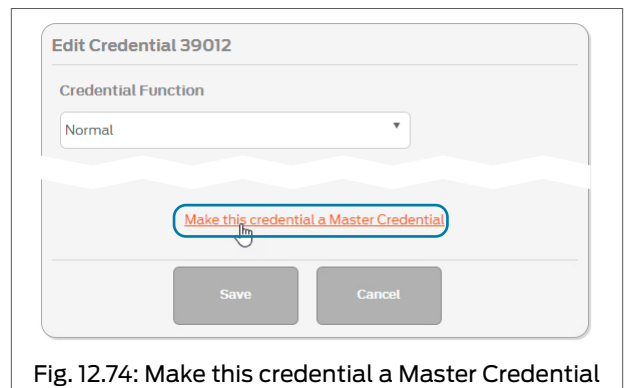


Fig. 12.74: Make this credential a Master Credential

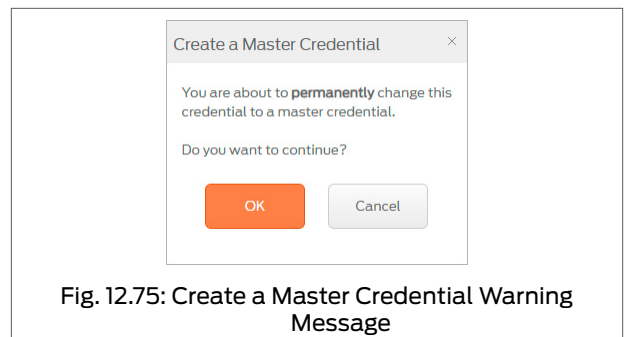


Fig. 12.75: Create a Master Credential Warning Message

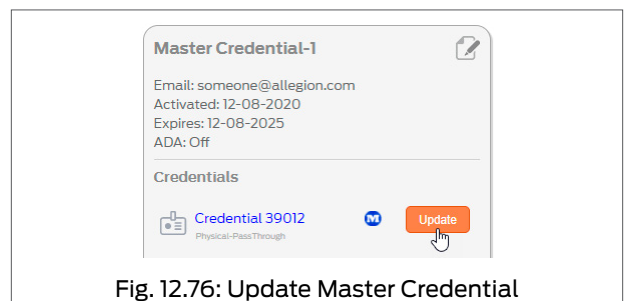


Fig. 12.76: Update Master Credential



7. Follow the instruction provided on screen, then select **Next**.

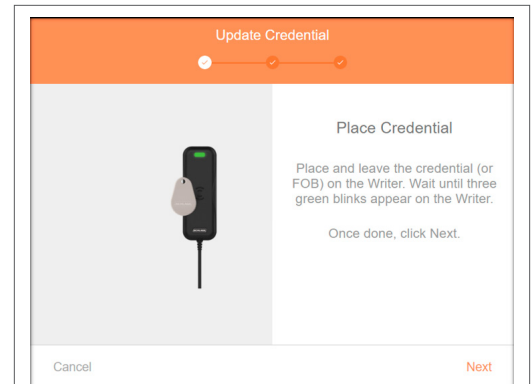


Fig. 12.77: Update Credential

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.

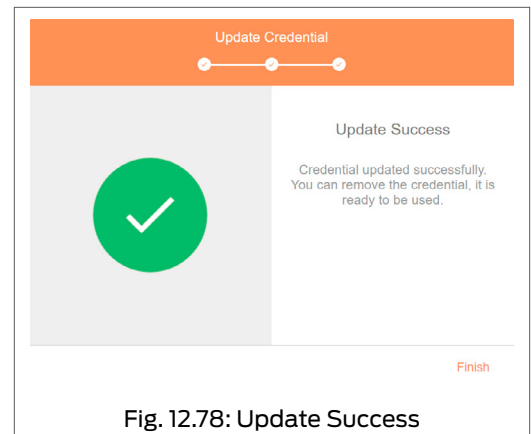


Fig. 12.78: Update Success

## View & Delete Master Credential

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.

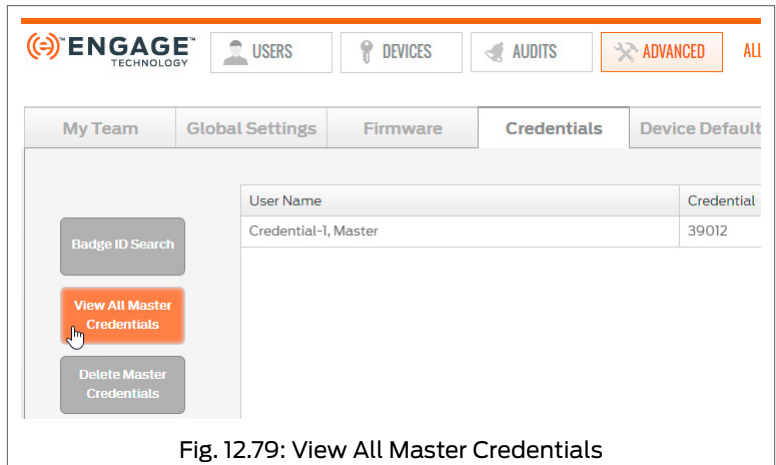


Fig. 12.79: View All Master Credentials

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

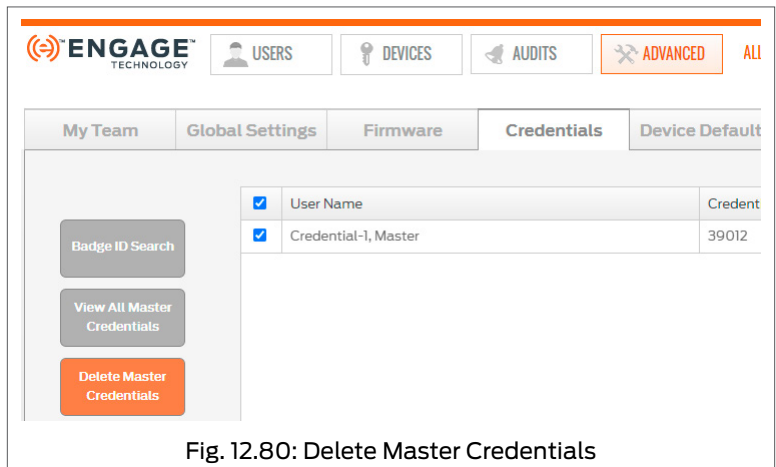



Fig. 12.80: Delete Master Credentials

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.

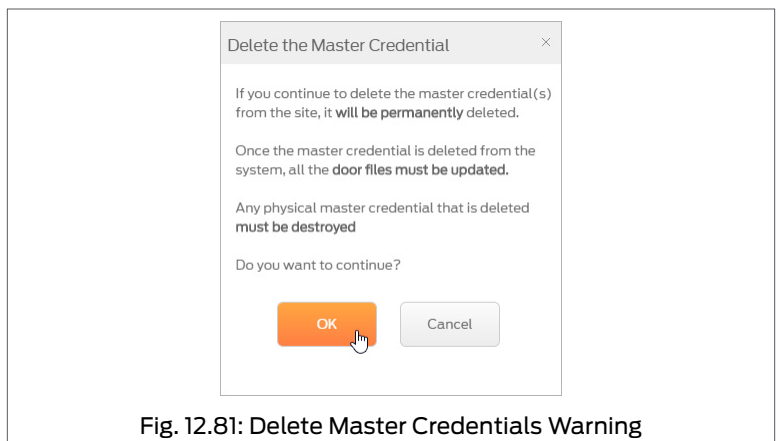


Fig. 12.81: Delete Master Credentials Warning

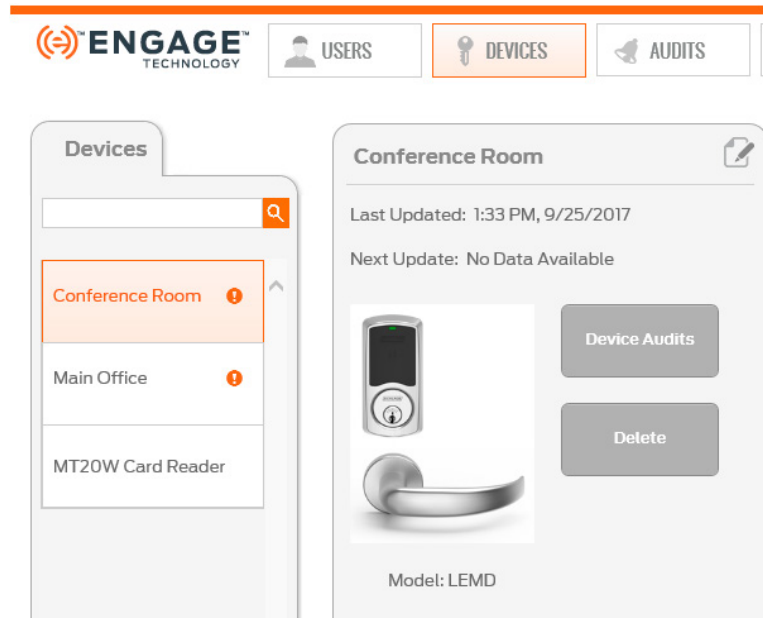
## Deleting Devices

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.

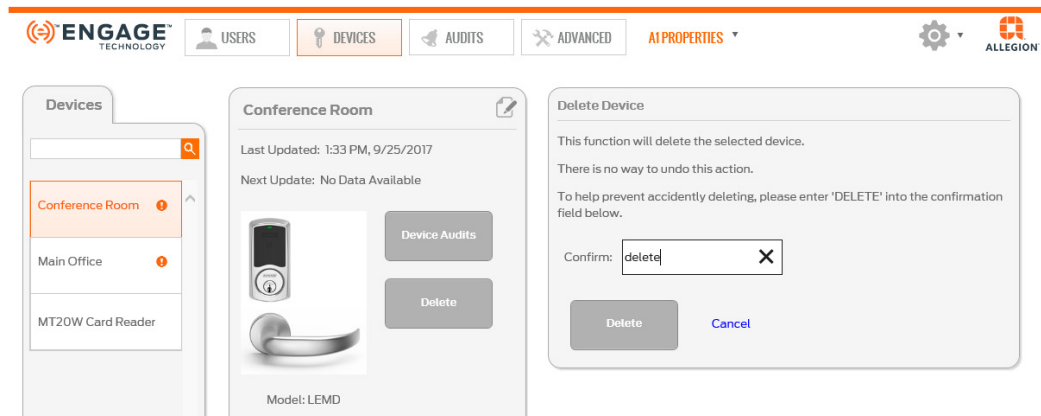
### Using the ENGAGE Web Application

1. **Open** the ENGAGE Web Application.
2. **Select** the **DEVICES** menu.
3. **Select** the specific device to be deleted from the property device list.

→ **Note:** **NOTE:** We chose **Conference Room** for deletion.



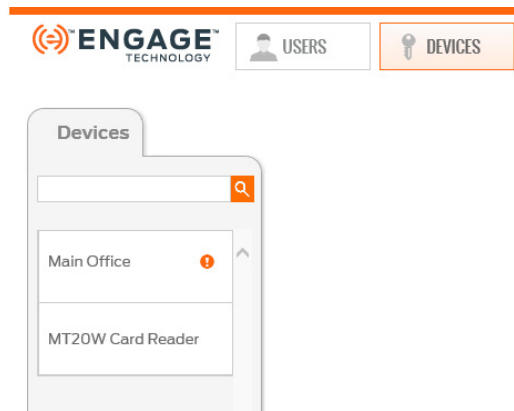
4. **Select** the **Delete** button.



5. **Confirm** the process by typing the word **'delete'** into the Confirm: box.
6. **Select** the **Delete** button to continue.
7. **View** the momentary **Device deleted.** success message.

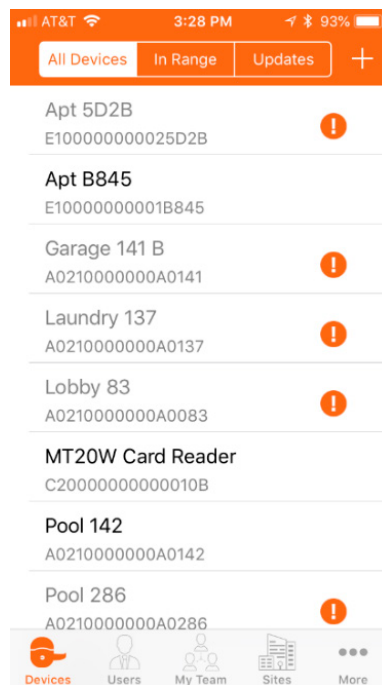
**Device deleted.**

8. **Verify** the **Conference Room** device is no longer listed in the **DEVICES** screen.

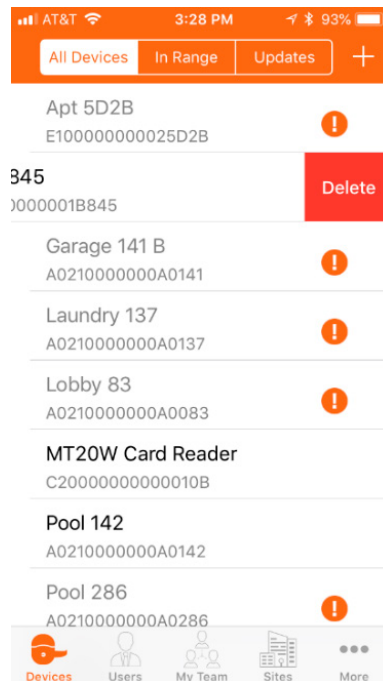


### Using the ENGAGE Mobile Application

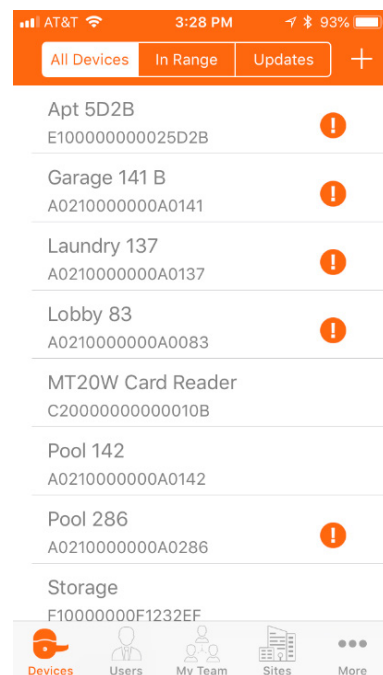
1. **Open** the ENGAGE Mobile Application.
  - NOTE: iOS Mobile Device screens are shown
2. **View** the **Devices** menu.
3. Find the device to be deleted in the list.
  - In this case we chose the **Apt B845** device for deletion.



4. **Swipe** (leftward) on the device name to enable (or uncover) the **Delete** button.



5. Select the **Delete** button.
6. View, the **Apt B845** is no longer listed in the **Devices** screen.



## 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:

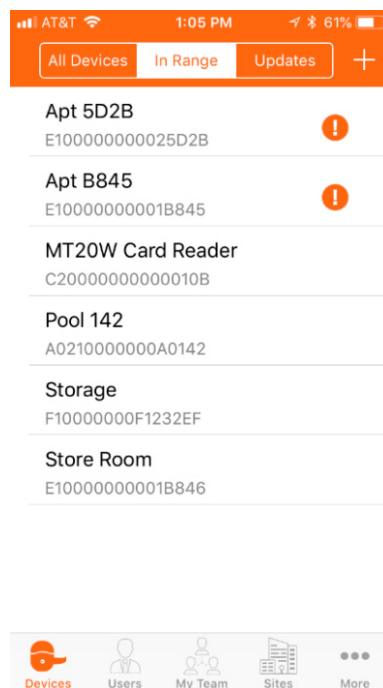
1. Schlage Control Mobile Enabled Smart Lock firmware must always be updated at the door using the ENGAGE Mobile Application.
  - Schlage Control does not support Wi-Fi connectivity
2. For Schlage NDE80, NDEB, LE, LEB and CTE devices, overnight Wi-Fi network firmware updates can be scheduled by the ENGAGE 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.

#### Firmware Updates - at the door - BLE Communication

Firmware updates are available for all devices using the ENGAGE Mobile Application. Schlage Control Mobile Enabled Smart Locks 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.

This example updates a Schlage Control Mobile Enabled Smart Lock that requires Bluetooth (BLE) for updates. All other devices may also be updated via local Bluetooth (BLE) communication shown here, when necessary.

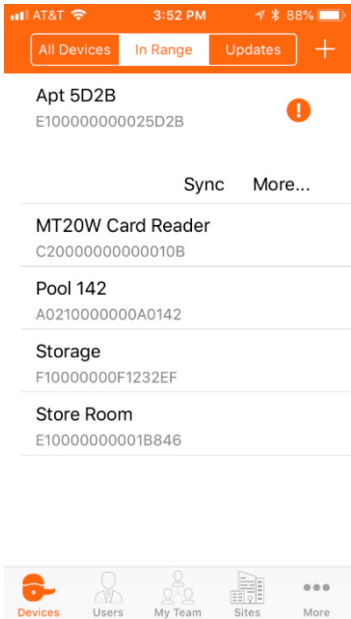
1. Log into the ENGAGE Mobile Application and view the devices In Range Screen.



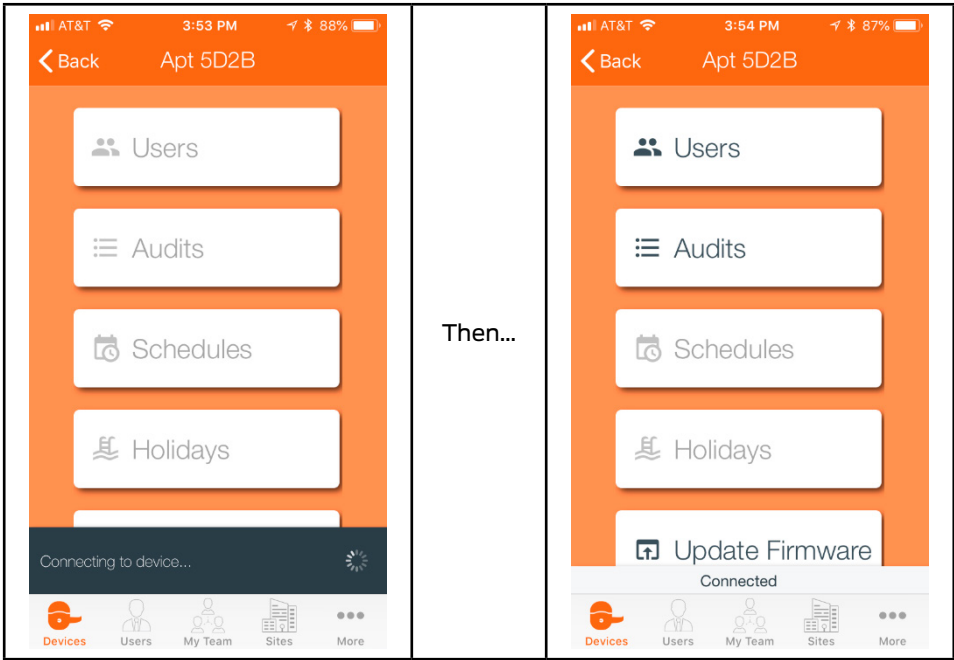
➔ **Note:** If the device you need is not presented, ensure the device is already commissioned and that you are within Bluetooth (BLE) range.

2. Select the local device to be updated with the latest firmware.

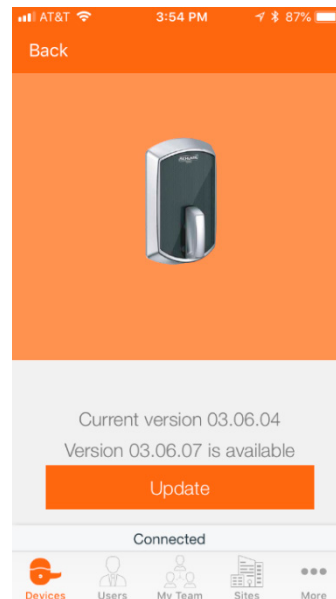
- In this case we chose a Schlage Control device, Apt 5D2B.



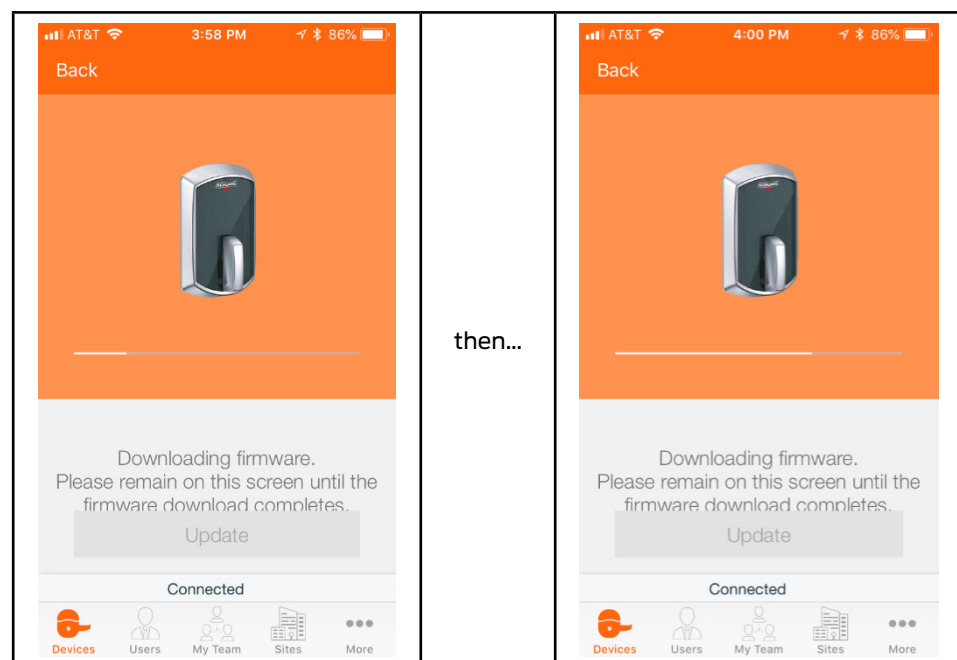
3. Select More ....



- **Note:** The device starts flashing the RED LED when connected and communicating.
4. Select Update Firmware in the connected device menu.



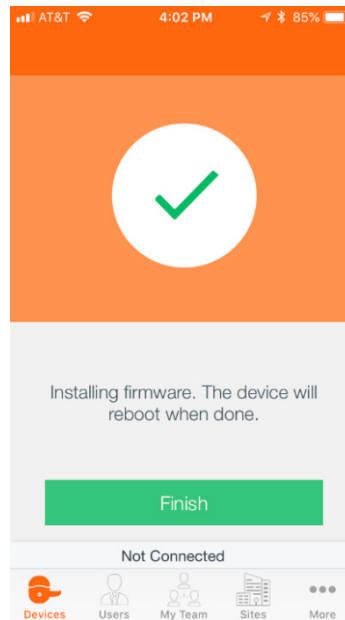
5. Select Update in the connected device menu.



**⚠ WARNING:** This is a local Bluetooth (BLE) firmware update method so the Mobile device **MUST** stay within BLE communication range while downloading firmware.

6. The following screen displays when the firmware update is successful.





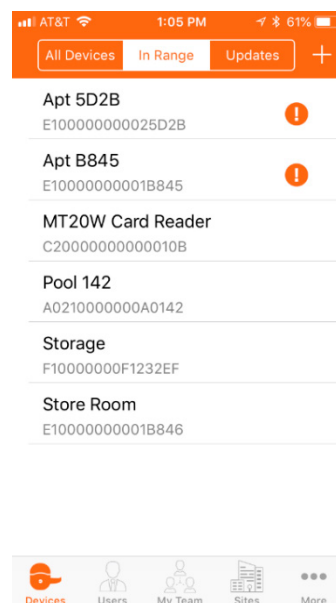
→ **Note:** The recently updated device loads the new firmware into its memory and REBOOTS itself. The firmware update and reboot process will take a few minutes – be patient.

### Firmware Updates - at the door – Wi-Fi Communication

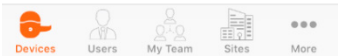
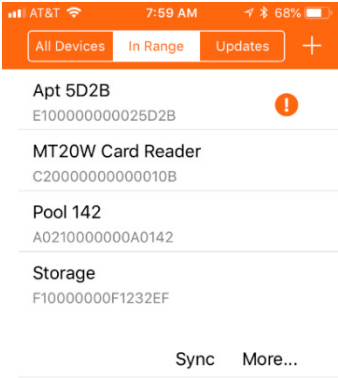
ENGAGE devices with local Wi-Fi connectivity may have firmware updates performed at the door. This method is preferred over the previously described Bluetooth (BLE) method because it uses the local Wi-Fi network for much faster communication and does not require the Administrator and the Mobile device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

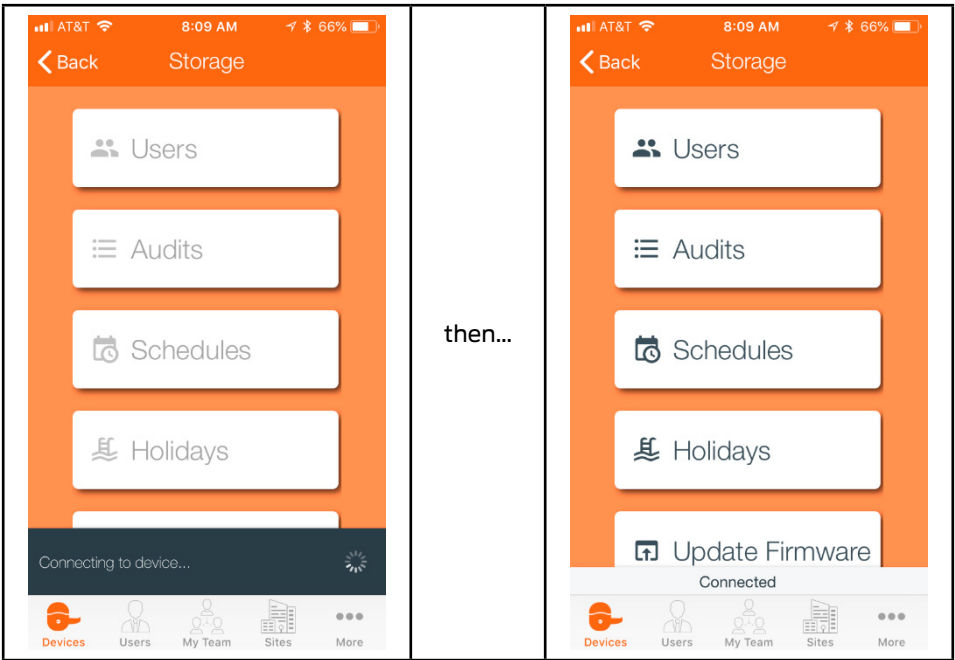
1. Log into the ENGAGE Mobile Application and view the devices In Range screen.



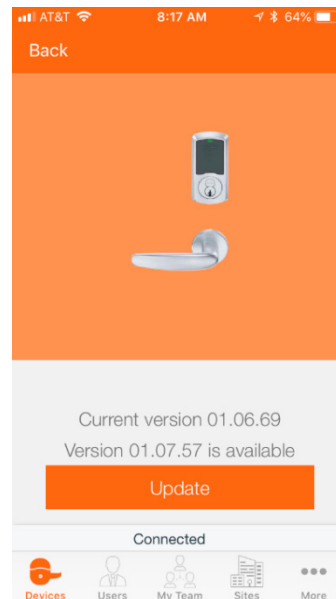
2. Select the local device to be updated with the latest firmware.
  - In this case we chose Storage which is a Schlage LE device with its Wi-Fi network connection properly enabled.



3. Select More.

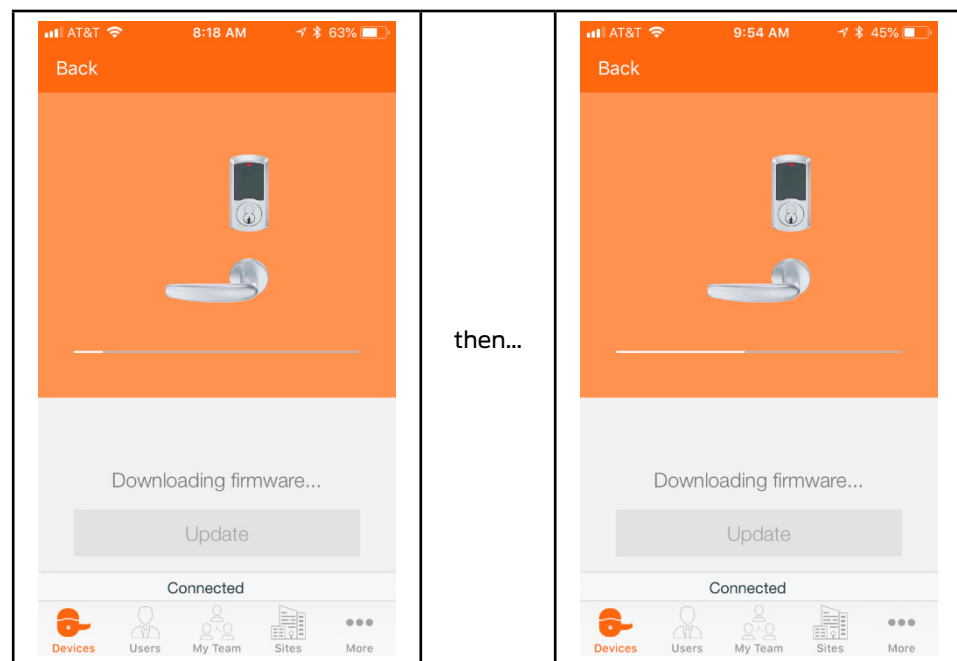


4. Select Update Firmware in the connected device menu.

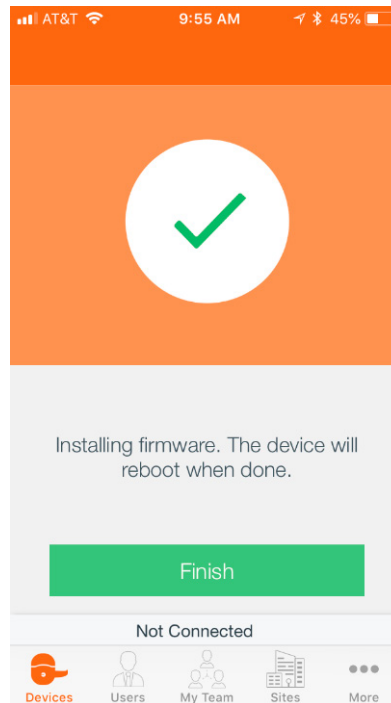


→ **Note:** Confirm the requested firmware update in the screen above. When the firmware version on the device is current a “Firmware is up to date” message is provided. Installing the firmware will take a few minutes, be patient.

5. Select **Update**.



→ **Note:** This message is provided as an indication that the firmware has been downloaded from the server to the device.



6. Select **Finish**.

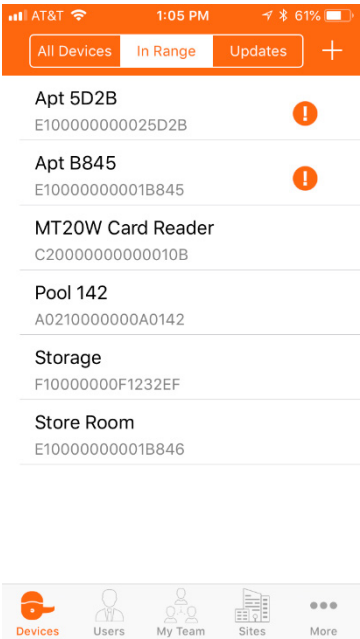
**WARNING:** After the firmware is downloaded, the new firmware will then automatically be installed into the device. The device will blink the LED RED and GREEN while installing the new firmware update. During the firmware update and while the LED are blinking, the device will be off-line and will not provide access. This process will take a few minutes, be patient. Once the firmware installation is completed, the device reboots and begins normal operation.

### Device firmware updates – at the door – Using Mobile Wi-Fi.

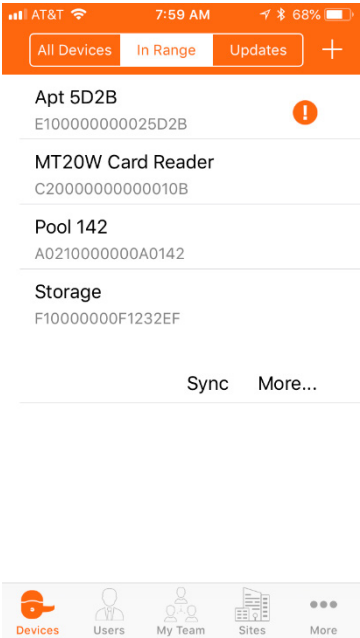
When the device does not have a Wi-Fi network connection available or the local Wi-Fi network is not enabled, the firmware download can be performed by temporarily enabling a Wi-Fi connection through the Administrator's Mobile device.

In this case the Storage device Wi-Fi has been turned OFF in Settings and is not enabled.

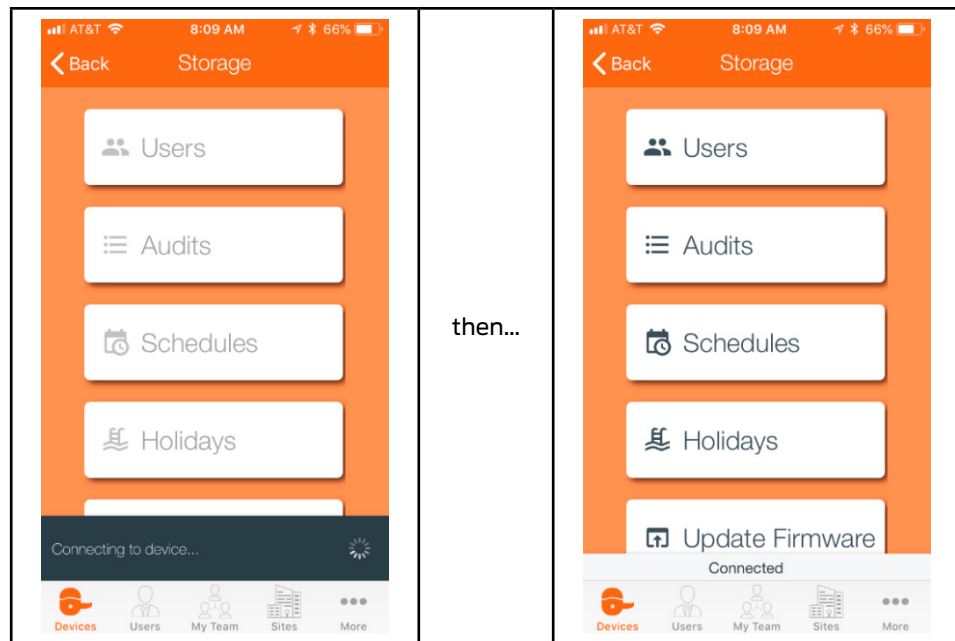
1. Log into the ENGAGE™ Mobile Application and view the devices In Range screen.



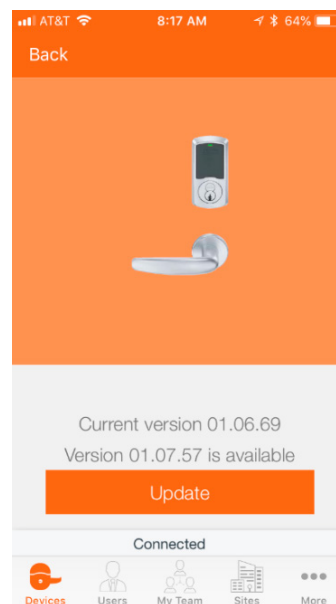
- 2. Select the local device to be updated with the latest firmware. In this case we chose Storage.  
➔ **Note:** This is a Schlage LE device with its Wi-Fi network connection disabled (OFF).



- 3. Select More ....

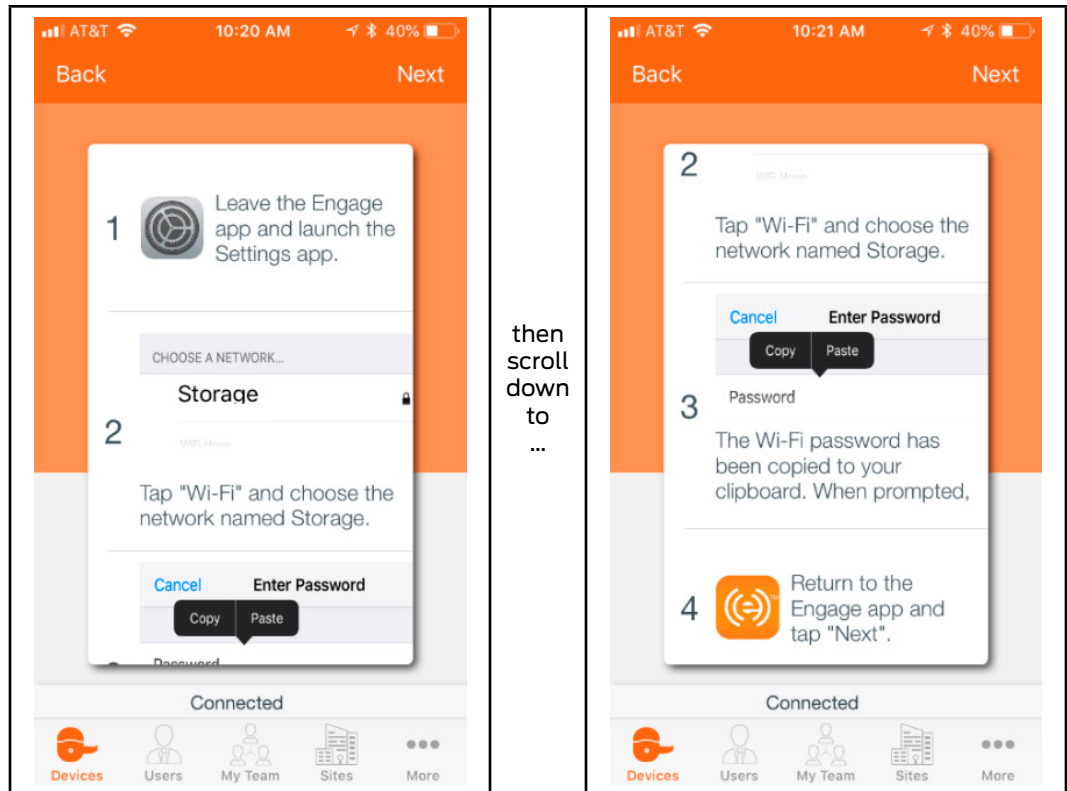


4. Select Update Firmware in the connected device menu.



5. Select **Update**.

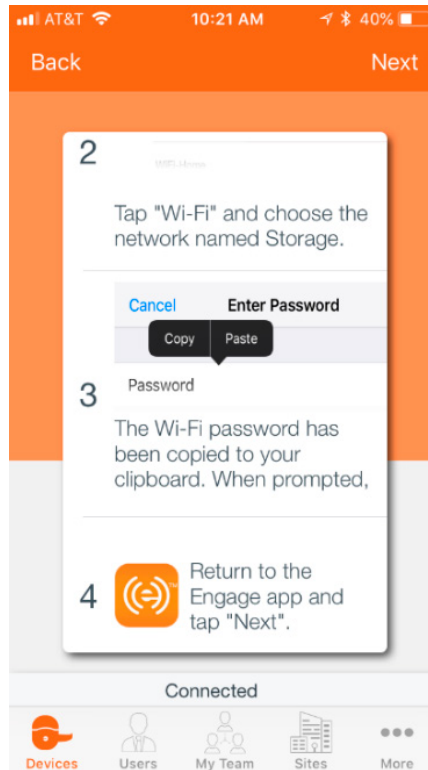
**WARNING:** Follow the displayed instruction to temporarily enable the ENGAGE device and the Mobile device to share a Wi-Fi connection.



→ **Note:** Using 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 password field. The required steps are highlighted below:

**Perform the following steps on the Mobile device:**

1. **Open** the Settings menu on your Mobile device.
2. **Select** the Wi-Fi network settings menu.
3. **Connect** to the local Wi-Fi network with the same name as the device you are connected to.
  - a. In this case we must choose **Storage**.
4. **Paste** the saved PASSWORD into the Wi-Fi settings field, using the standard Mobile device "Clipboard" paste utility.
5. **Select Join** the network.
6. **Verify** the Mobile device connects with the selected device by viewing its Wi-Fi connection information.
7. **Return** to the previous ENGAGE Mobile application screen.



8. Select **Next**.

### Completing the device Firmware updates after download

When new firmware has been downloaded into a device, the new firmware is not usable until the device installs the update into its internal memory.

Each device automatically follows a successful firmware download with an additional firmware installation process. No additional actions are required except to wait a few minutes. The firmware update process at the lock is indicated by the device blinking the LED RED and GREEN for a few minutes.

After the RED and GREEN flashing is completed, the device internal firmware update process is completed. The device will automatically perform a RESET and will begin normal operation using the new firmware.

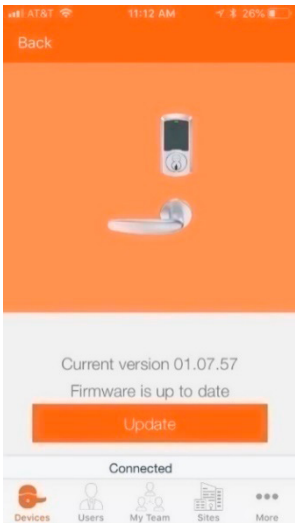
→ **Note:** ENGAGE will use the selected device to create a local Wi-Fi network between the Mobile device and the lock. The local Wi-Fi network name will be the selected device name. ENGAGE will save the Wi-Fi PASSWORD into the Mobile devices' "Clipboard". Using the Mobile device "Cut and Paste" feature,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

The required steps are highlighted below:

1. Open the ENGAGE Mobile Application.
2. Connect to the device that was updated with new firmware.
3. Select the device, then More ....
4. Select the Update Firmware menu.
5. View the displayed "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.





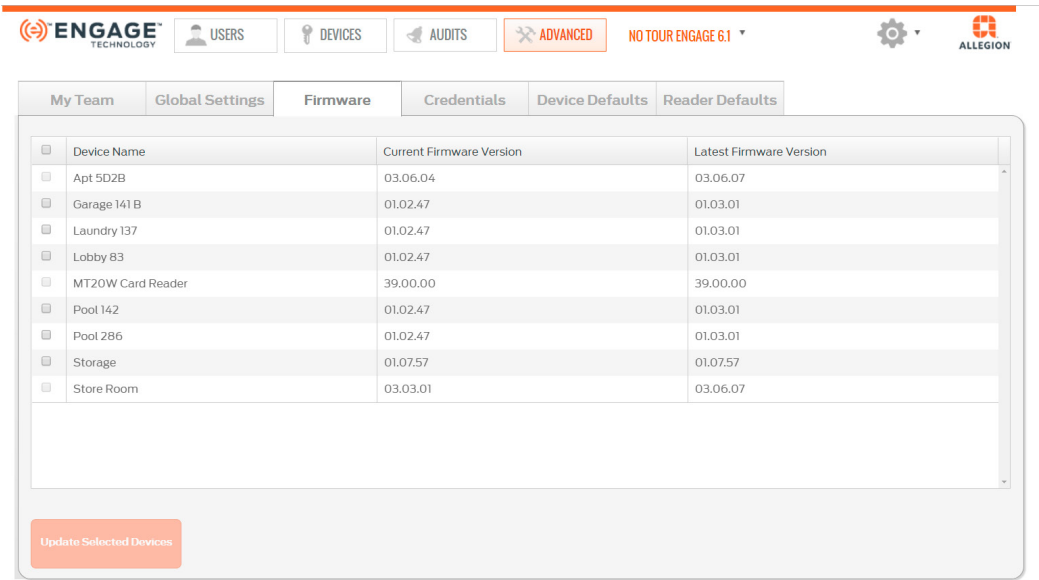
## Scheduled “Overnight” Firmware Updates

Firmware update scheduling is available for Schlage NDE80, NDEB, LE, LEB CTE, and MT20W devices using the ENGAGE Web Application.

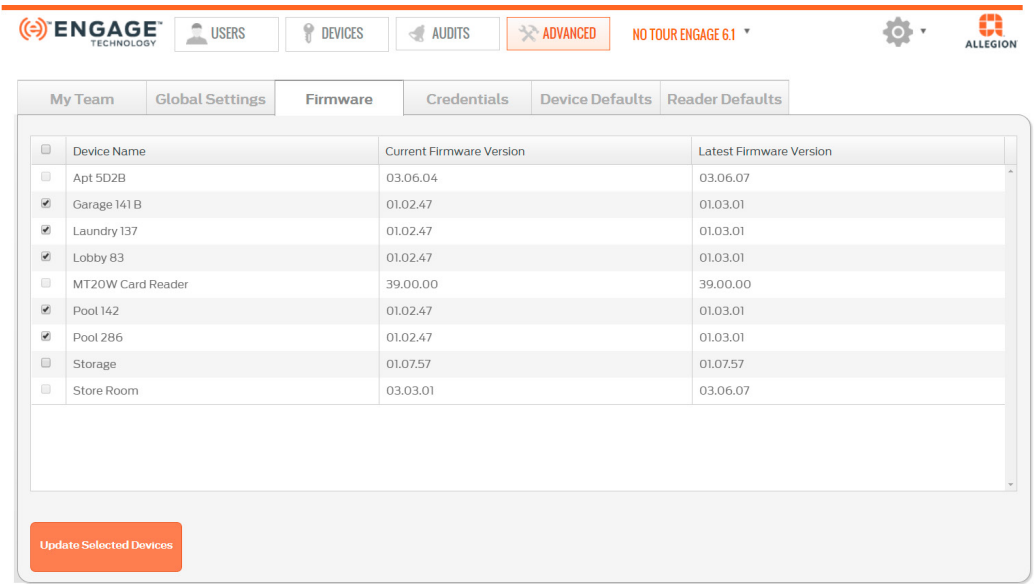
Administrators use this feature to keep their devices updated with the latest firmware revision and functionality. Administrators can save time and keep their devices updated using Scheduled automatic over-night firmware updates.

When devices support and are enabled for Wi-Fi connectivity. Follow these steps:

- 1. Open the ENGAGE Web Application.
- 2. Select ADVANCED tab.
- 3. Select the Firmware tab.



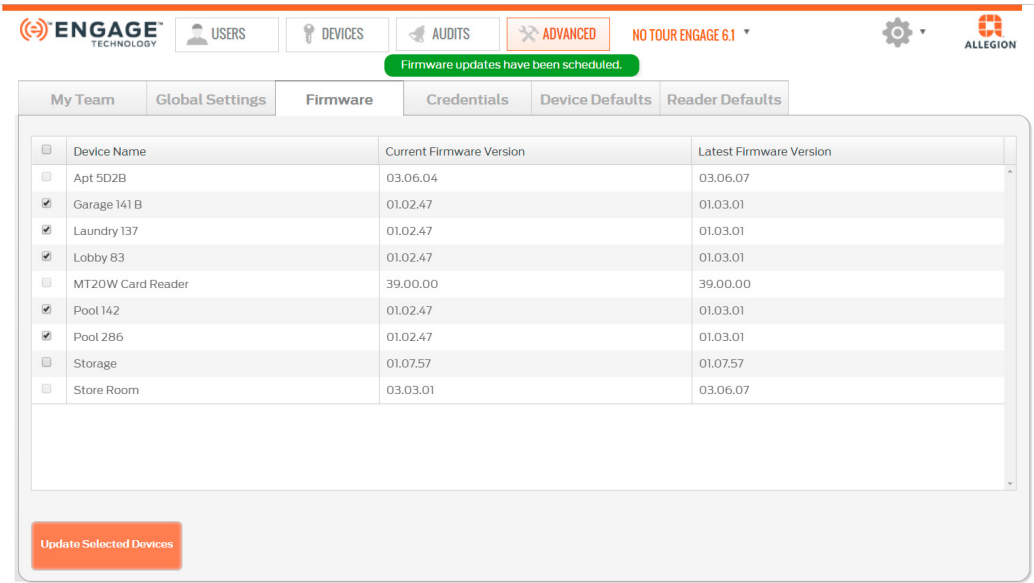
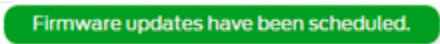
- 4. Compare the Current Firmware Version on each device to the Latest Firmware Version that is available.
  - When a firmware update is available check each Device Name box that requires a firmware update.



- ➔ **Note:** **Garage 141B, Laundry 137, Lobby 83, Pool 142 and Pool 286** firmware is not at the latest revision. Notice that the **Storeroom** has outdated firmware as well, but that device is a Schlage Control device and cannot be selected for scheduled firmware updates.
5. **Select the Update Selected Devices** button at the bottom of the screen to schedule the selected “Overnight” firmware updates and complete the schedule event.



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



7. Wait until “TOMORROW” (the next day) to review the device firmware status to confirm the process was completed over-night by again comparing the device firmware status with the “Latest” available.
- ➔ **Note:** If a selected firmware update is not successfully accomplished over-night:

- Be sure 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.

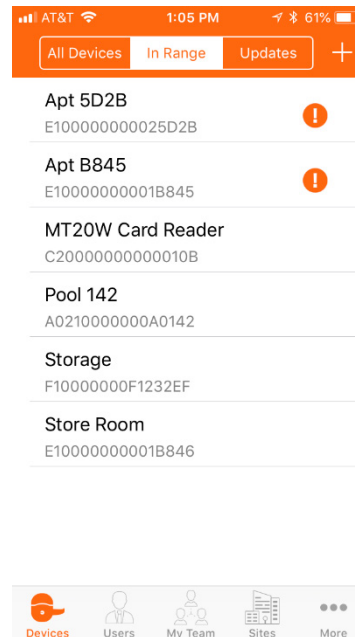
## Retrieving Audit Data from Devices

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.

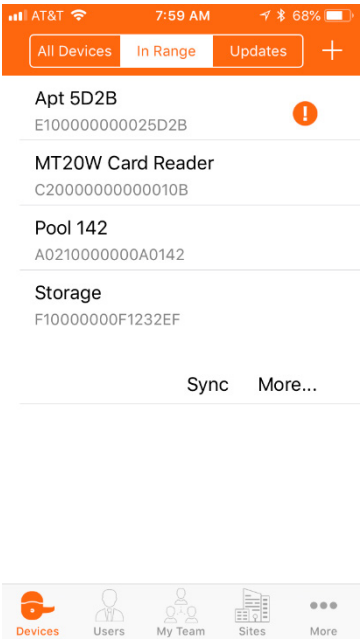
→ **Note:** For Schlage Control, audits can only be retrieved locally at the door using the Sync process and the ENGAGE Mobile Application. All other ENGAGE device audits may also be gathered remotely using over-night Wi-Fi network connections

### Audits - ENGAGE Mobile Application

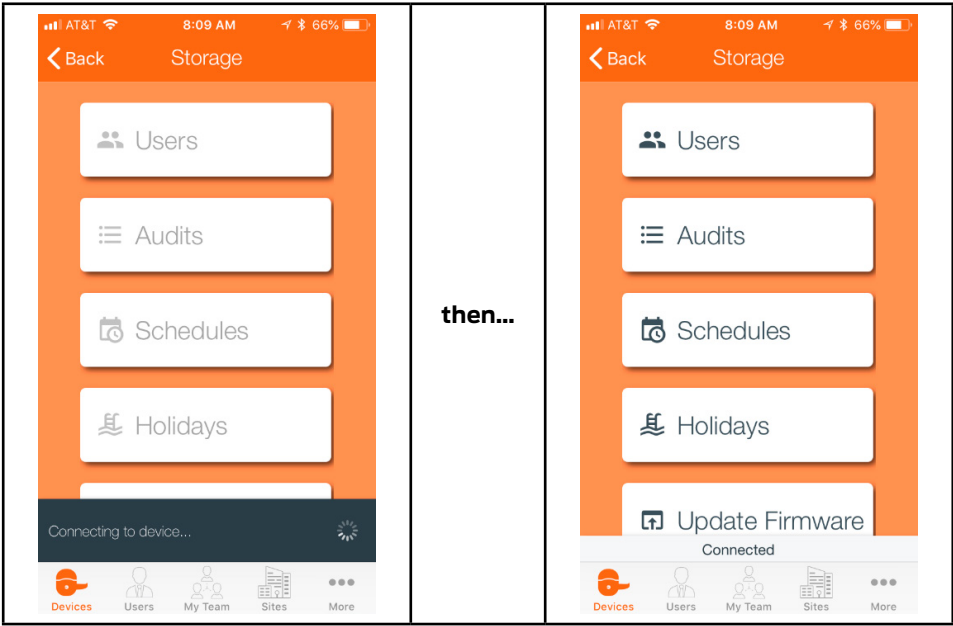
1. Log into the ENGAGE Mobile Application while nearby the device.
2. View the devices In Range Screen.



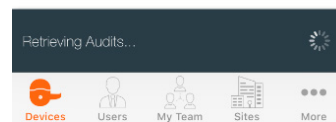
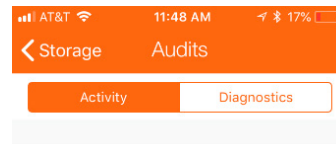
3. Select the device for audit gathering from the nearby listing.
  - In this case we chose Storage.



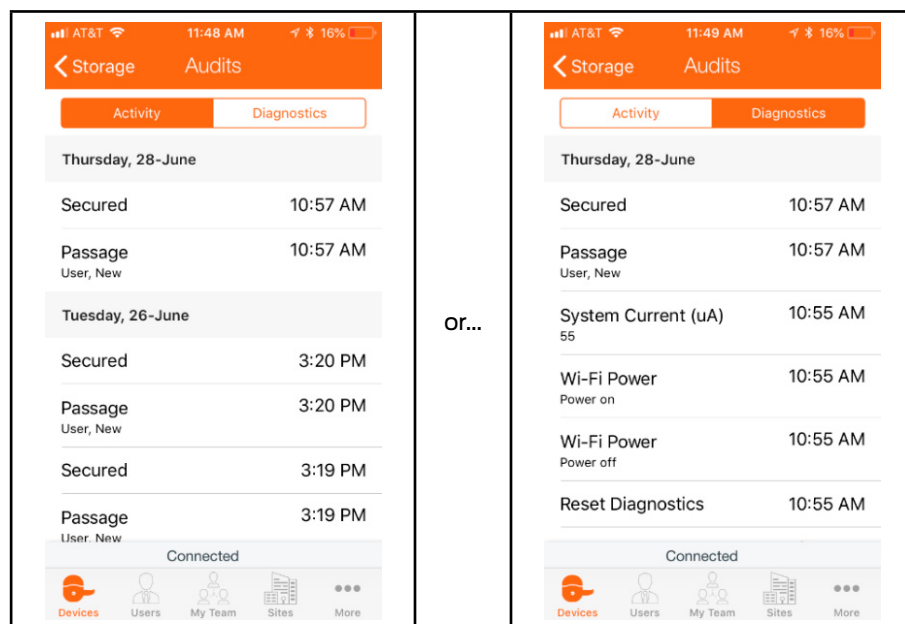
4. Select More.



5. Select Audits.

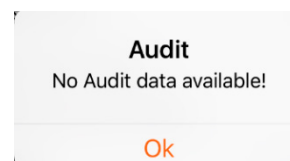


→ **Note:** Device **Activity** is the default Audit Screen. Select the **Diagnostics** tab for System Audits. Retrieved Audits are always available via the ENGAGE Web Application



**6. View, the retrieved Audits**

- Audits are also now available for viewing on the ENGAGE Web Application



**7. When you receive this message after selecting “Get Audits”**

- There are no new Audits available
- All existing device and user audits have been retrieved.

### Audits – ENGAGE Web Application

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 setup.

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:** When Wi-Fi network settings are properly installed and working, nightly updates will be gathered automatically. No special action is required. Use the ENGAGE Mobile Application “Test Wi-Fi” feature to verify network settings and proper communication.

**WARNING:** 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

## Viewing Audit Information

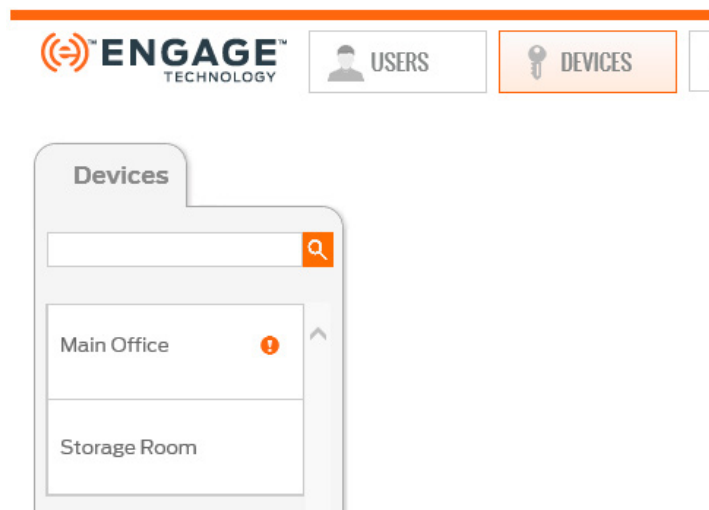
Device and User Audits are information collected by the lock when any action is taken at the door. Device Audits provide details about the lock itself with diagnostics information while User Audits provide user access details.

For Schlage Control Mobile Enabled Smart Locks, audits can only be retrieved locally at the door using the ENGAGE Mobile Application. All other Schlage ENGAGE devices may have audits gathered at the door, or remotely by taking advantage of these devices’ Wi-Fi network connection and nightly “Call in” feature.

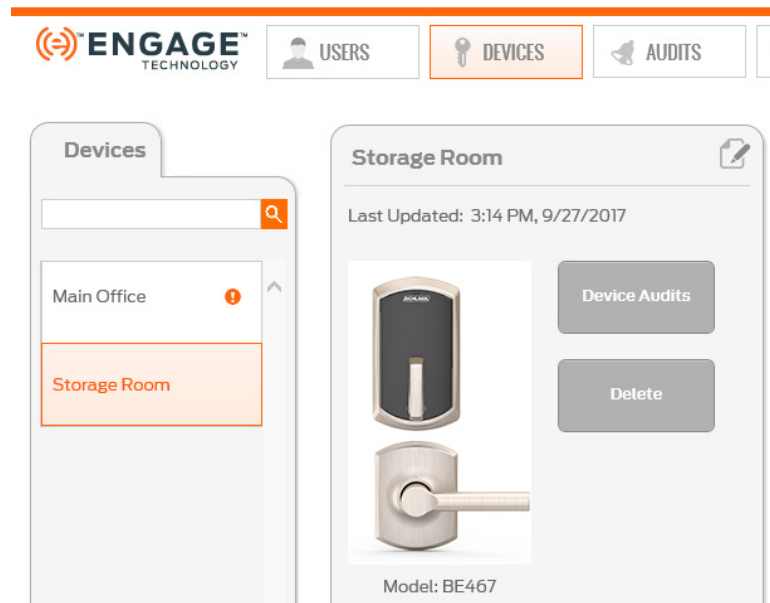
Audits may be reviewed by either the ENGAGE Web or Mobile Applications, however audit data may be filtered and exported for easier review and data analysis while using the ENGAGE Web Application.

### Audits Individual Device - ENGAGE Web Application

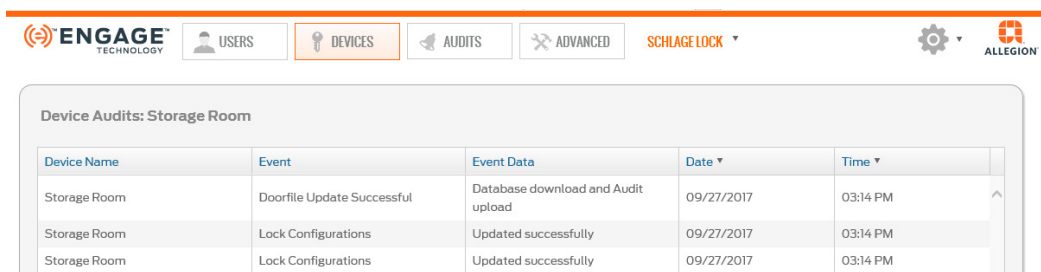
1. Open the ENGAGE Web Application.
2. Select the DEVICES menu and the Devices pull-down.



3. Select the desired lock from the list – we chose Storage Room.



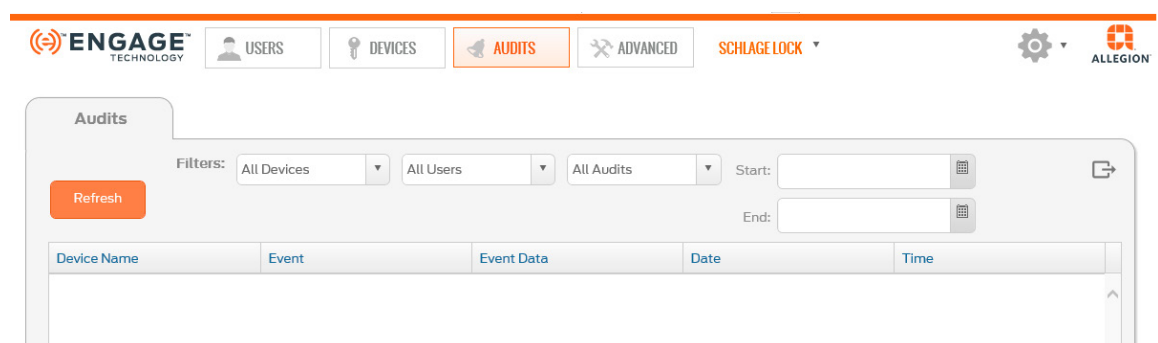
4. Select Device Audits button.



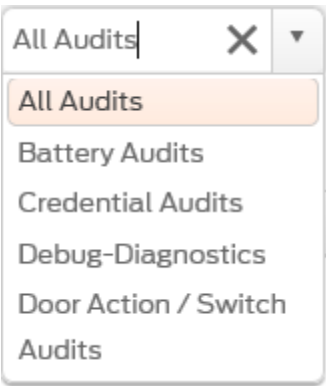
5. View the available device Audits  
 ➔ **Note:** Use the column headers to quickly sort and find the displayed Audit data.

### Audits Property Wide - ENGAGE Web Application

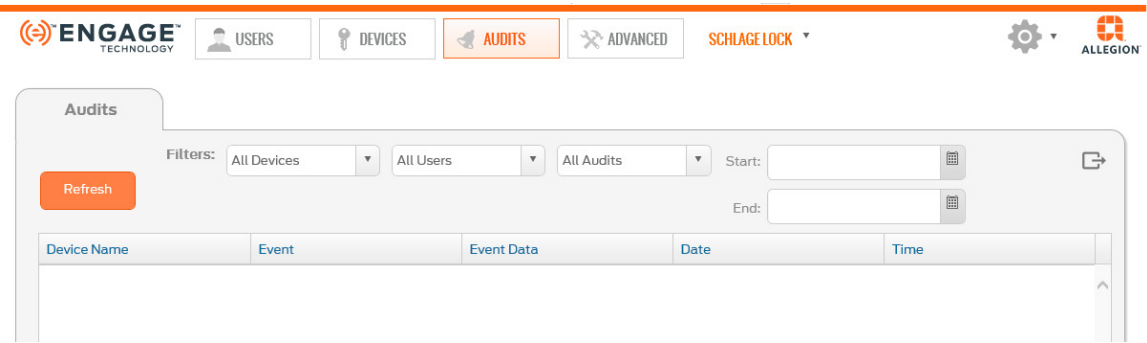
1. Open the ENGAGE Web Application.
2. Select the AUDITS menu and the Audits pull-down tab.



3. 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



- 4. 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.

**Device Wi-Fi Network Connectivity**

Device Wi-Fi connectivity is normally setup 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 the Wi-Fi connection” feature from the ENGAGE Mobile Application.

Follow these steps to update or enable Wi-Fi connectivity in any ENGAGE Wi-Fi enabled device.

**New Wi-Fi Network Setup**

1. Open the ENGAGE Mobile application and log into your account.
  - An Android device is used in this example
2. From the Device menu, Select a nearby device. (Pool #1)



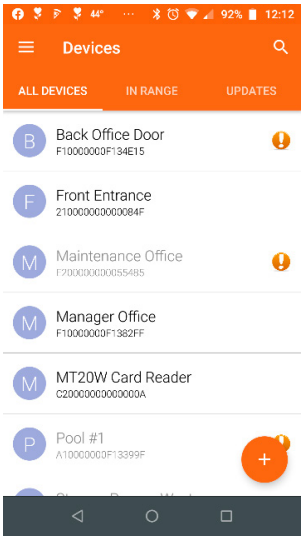


Fig. 12.82: Device

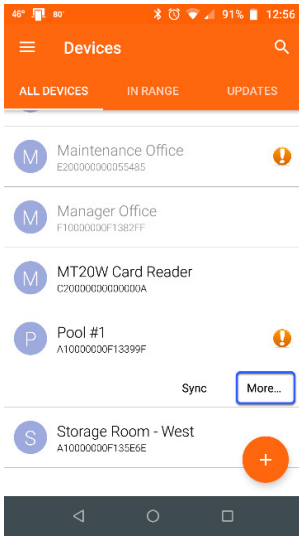


Fig. 12.83: More

→ **Note:** The “ALL DEVICES” menu shows all devices commissioned in ENGAGE with devices in BOLD are nearby and in Bluetooth communication range. The “IN RANGE” menu shows ONLY those devices that are nearby and in Bluetooth communication range. **Select More** to connect with the nearby device

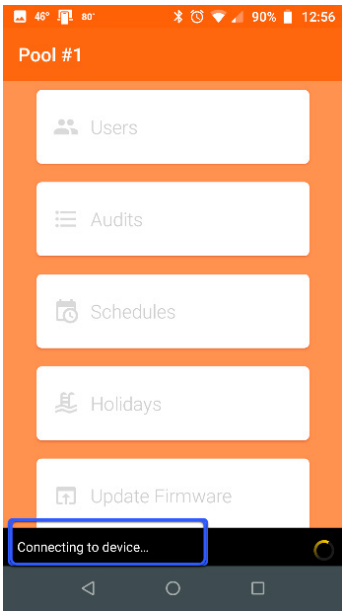
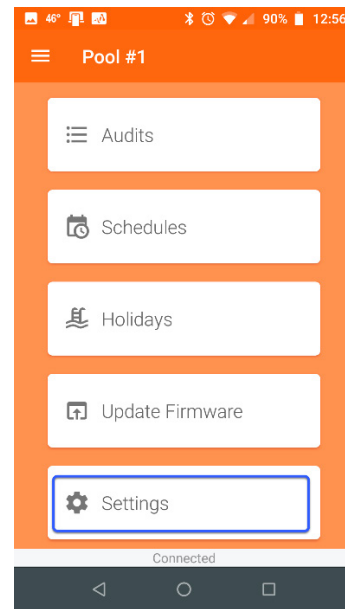
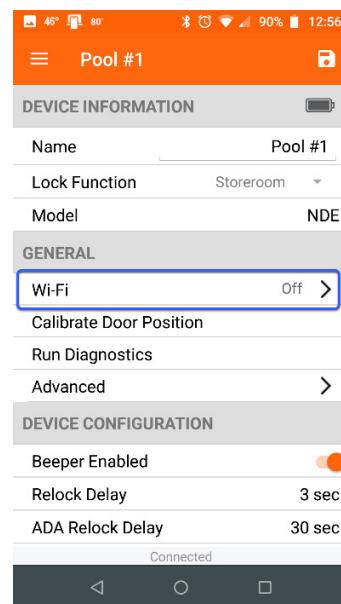


Fig. 12.84: Connecting



Then

3. Once connected, **scroll** down and **Select Settings**.



4. **Select Wi-Fi** menu under **GENERAL**.

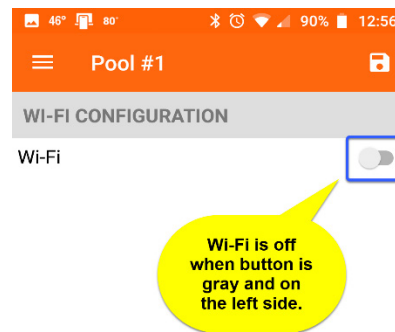
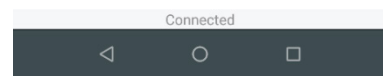
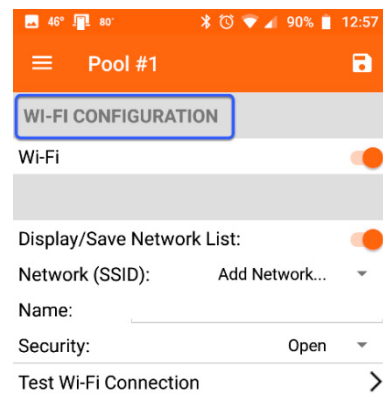


Fig. 12.85: Wi-Fi



Then

1. **Move** the **Wi-Fi** slider to the right to enable Wi-Fi connectivity
2. **View** the full Wi-Fi Configuration menu. By default, the **Display/Save Network List** is enabled.  
 → **Note:** 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 sitting up new Wi-Fi enabled devices
3. **Select Add Network.**

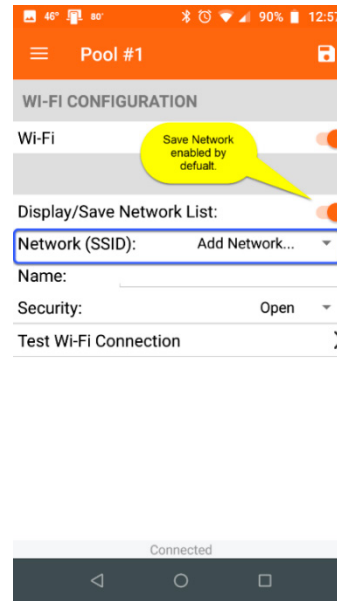


Fig. 12.86: Wi-Fi

4. **Enter** the Wi-Fi network details:
  - a. Name (SSID)
    - i. Security selection, password may be required
5. Select **SAVE**



→ **Note:** Select **Test Wi-Fi Connection** to initiate the test to verify that the Wi-Fi network is available, and the device Wi-Fi details settings are correct.

### 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.

To save an available Wi-Fi network, use the following steps.

1. Open the **ENGAGE Mobile app** and **log into your account**.
  - **The Android device is used in this example.**
2. From the **Device or In Range** screen, **select a device**.
3. From the desired device, select **More**.

a. Device will connect.

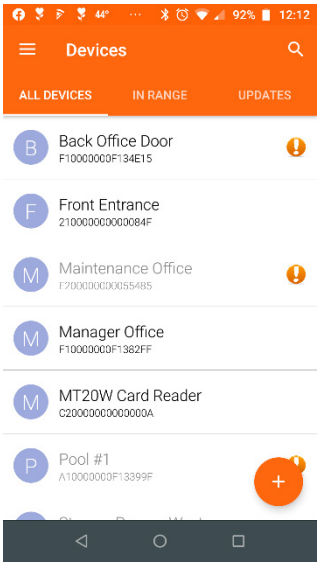


Fig. 12.87: Device

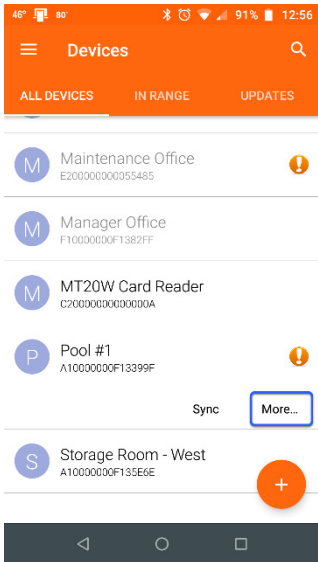


Fig. 12.88: More

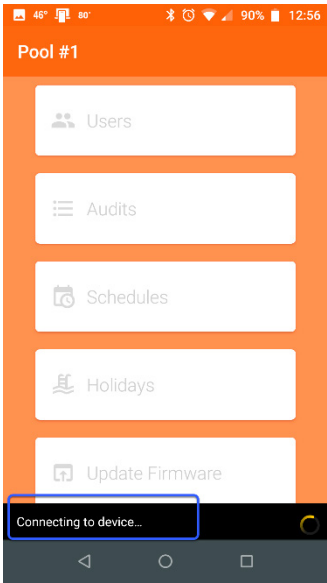


Fig. 12.89: Connecting

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

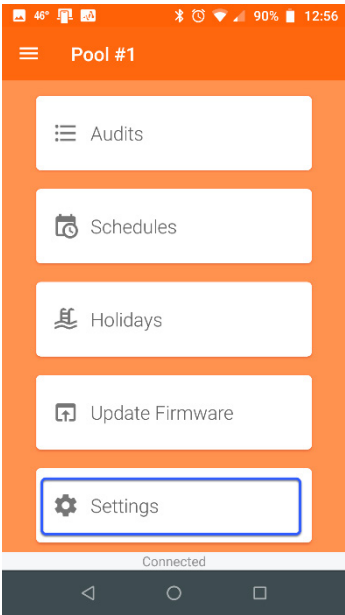


Fig. 12.90: Settings

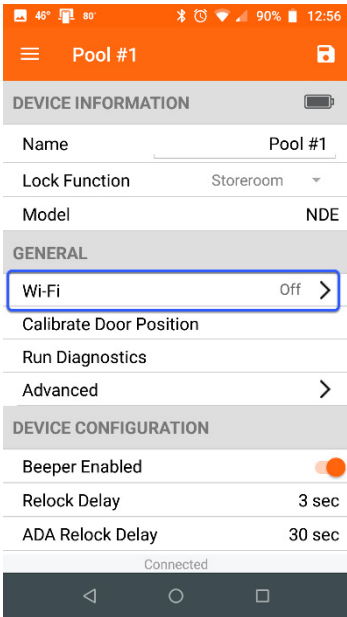


Fig. 12.91: Wi-Fi Option

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

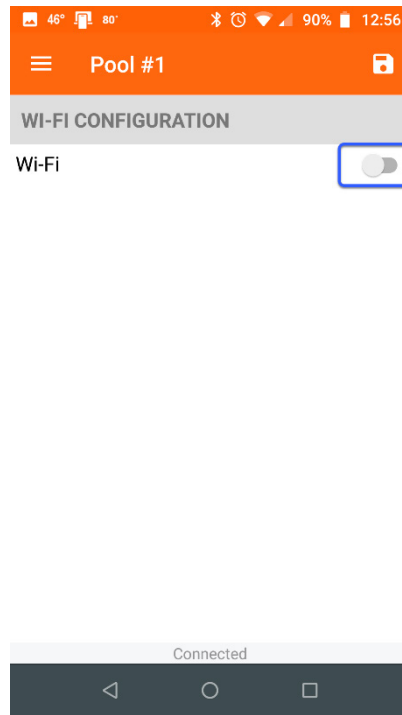


Fig. 12.92: Wi-Fi

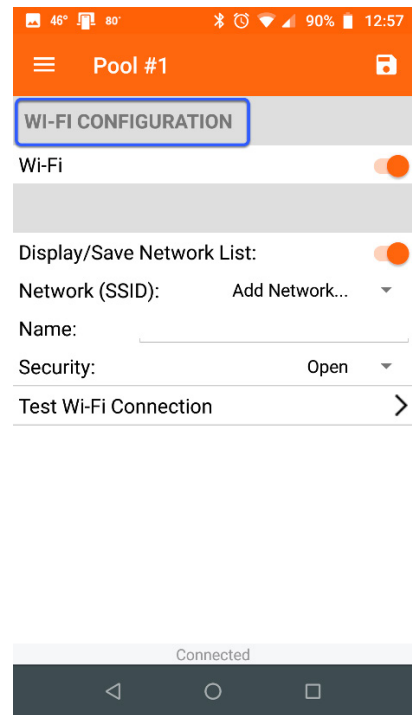


Fig. 12.93: Wi-Fi Configuration

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

#### 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.

To select and test a saved Wi-Fi network, use the following steps.

1. Ensure you have already saved an available network.
2. Select the desired device and from the Wi-Fi Configuration screen,
  - a. iOS: select Show Saved Network.
  - b. Android: select Add Network.

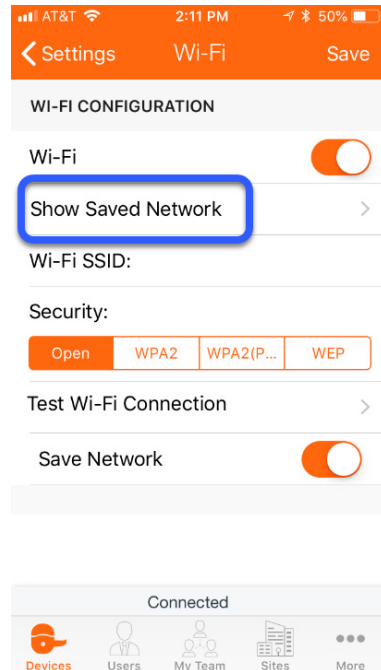


Fig. 12.94: iOS

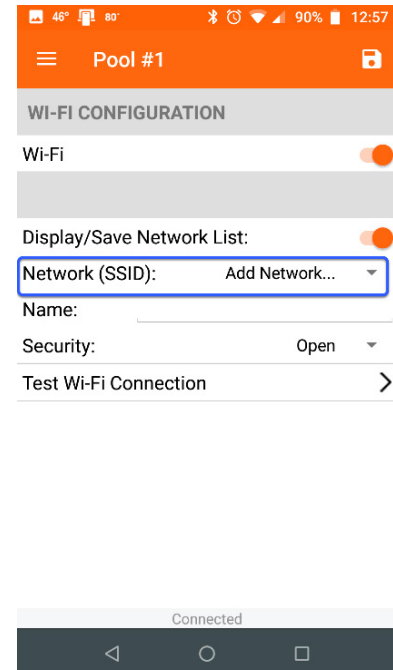


Fig. 12.95: Android

**WARNING:** 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.



Fig. 12.96: iOS List

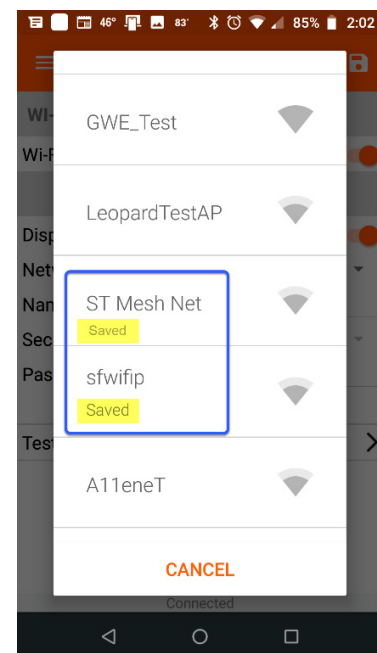


Fig. 12.97: Android List

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



Fig. 12.98: iOS Saved



Fig. 12.100: iOS Test

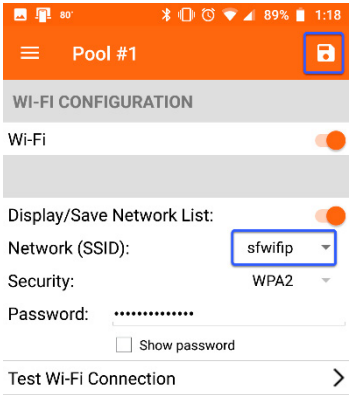


Fig. 12.99: Android Saved



Fig. 12.101: Android Test

4. Select Test Wi-Fi Connection
- To test to verify that the Wi-Fi network is available, and the device Wi-Fi details settings are correct





Wi-Fi connectivity test could take several minutes



Wi-Fi connectivity test could take several minutes

Approximate time remaining

02 : 51

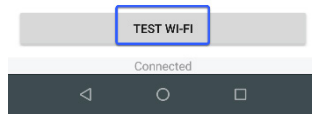


Fig. 12.102: Test Wi-Fi



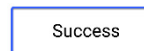
Fig. 12.103: Time Remaining

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

5. **View**, the device has successfully connected to the host.



Wi-Fi connectivity test could take several minutes



Device successfully connected to the host



Fig. 12.104: Wi-Fi Test Success

→ **Note:** The device now has its Wi-Fi connection verified and it will call into **Sync** every night to apply any door file updates and retrieve device audits. This device can now be enabled for automated firmware updates and nightly call-in updates using the ENGAGE Web Application.

→ **Note:** Warning: 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

## Sync – Manual Updates at the Door

The ENGAGE Sync feature updates devices using the latest ENGAGE system settings and programmed access rights. Sync also captures and returns the latest Device and User Audits for review by the Administrator.

Sync may be accomplished using the ENGAGE Mobile Application and local Bluetooth communication while standing nearby the device, or Sync may be accomplished remotely each night when Wi-Fi enabled devices are set up for over-night Call-In.

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



See the Web and Mobile device displays for the “Back Office” device listing below.

This exclamation point is the Administrators indication that device has updates (Device or Access) changes that have been made in ENGAGE, and the new updates need to be communicated to the device “Sync” performed to receive the updates.

Administrators should work to keep all devices updated with the latest’s access and device settings. The manual process to Sync a device at a door only takes a few seconds and the Sync Call In happens automatically overnight.

**WARNING:** The manual Sync process is required for all Control Mobile Enabled Smart Locks because the Control Mobile Enabled Smart Lock does not support Wi-Fi connectivity and cannot take advantage of the automated ENGAGE Nightly Wi-Fi “Call-In” feature.

Frequent Sync processes will be needed for Control Mobile Enabled Smart Locks to prevent lost Device and User Audits. Control Mobile Enabled Smart Locks will store the last 1000 events that happen at the door. New Audit events will overwrite the oldest events when Sync is not performed in a timely fashion and the Audit memory can overflow.

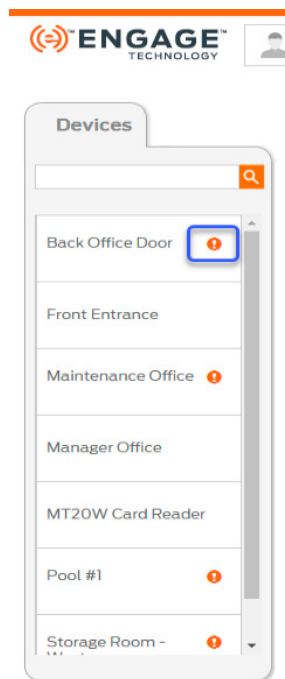


Fig. 12.105: Web App

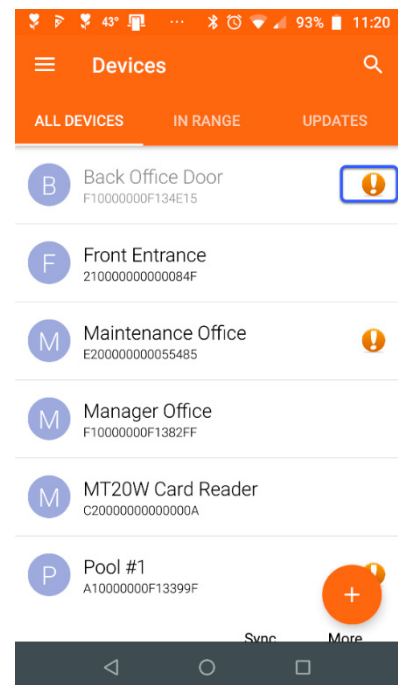


Fig. 12.106: Mobile App

### Sync: Overnight Wi-Fi Updates

When Wi-Fi enabled devices are used, and setup properly, the nightly Wi-Fi “Call-In” process (Sync) is automatically enabled. No additional action is required by the Administrator 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.

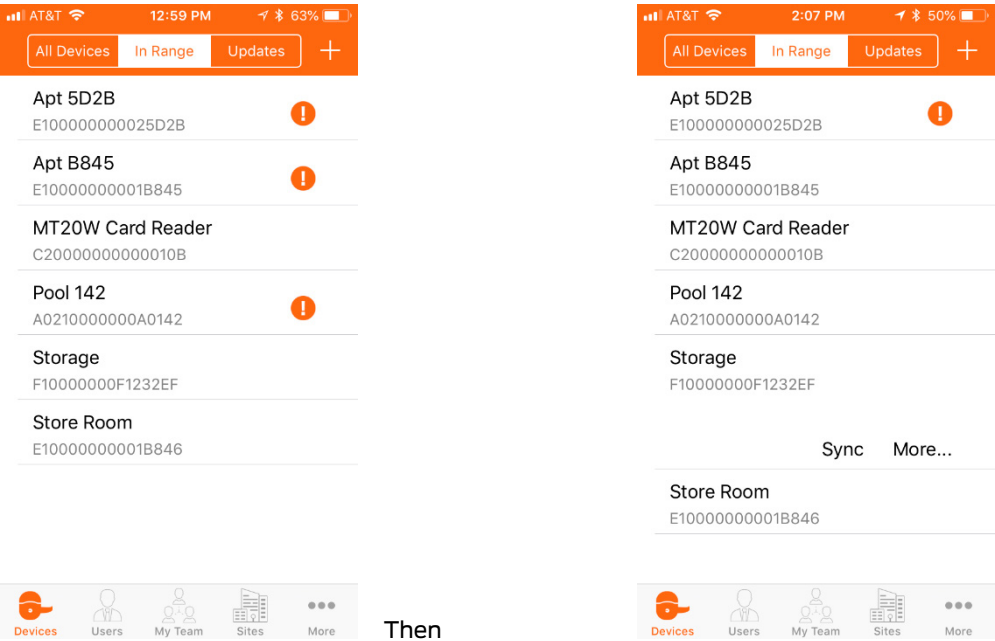
→ **Note:** Administrators will want to take advantage of their Wi-Fi enable devices to keep them up to date and to have the latest Audit information handy. Overnight Sync can be easily scheduled for Firmware Updates, for more information, refer to the [Schedule Firmware Updates](#) section

Best practice is to set up the device Wi-Fi connectivity to enable nightly call-in, during the normal device installation and commissioning process. However, when the local Wi-Fi is not ready to be used (not installed) or may not be available during the commission process (out-of-service) the

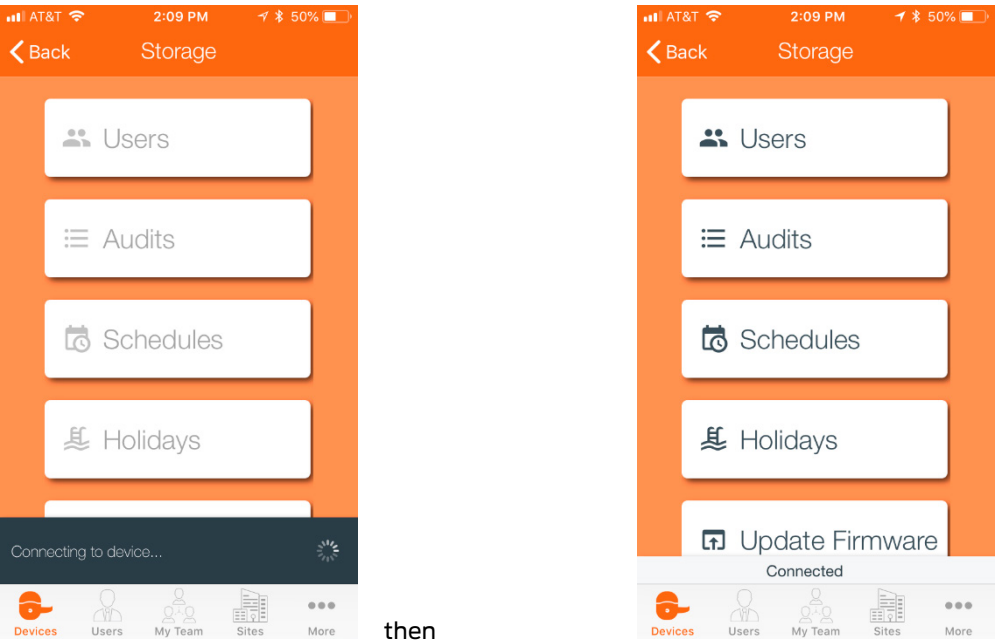
administrator can skip the Wi-Fi setup during commissioning and can apply the Wi-Fi settings and enable the nightly Call, later.

Follow these steps to enable (or update) Wi-Fi connectivity after a device is commissioned without enabling the Wi-Fi or when adjusting Wi-Fi settings.

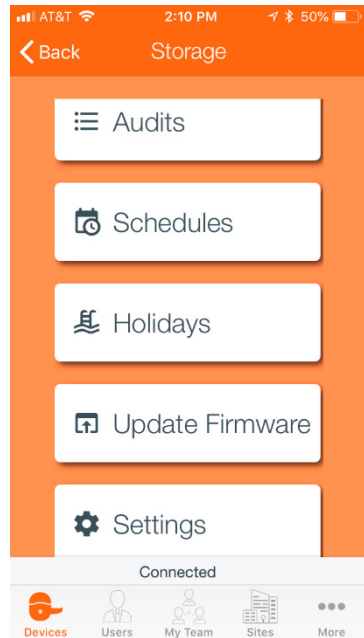
- 1. **Open** the ENGAGE Mobile application and log into your ENGAGE account.
- 2. From the **Device** screen, **select** an “In Range” device to enable its Wi-Fi network connection.
  - We chose Storage, which is a Schlage LE device.



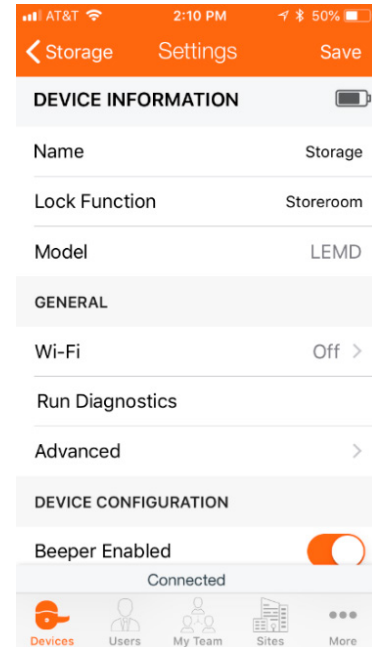
- 3. **Select More ...** to communicate (connect) with the Storage device



- 4. **Scroll** down the screen to reveal the **Settings** menu at the bottom.

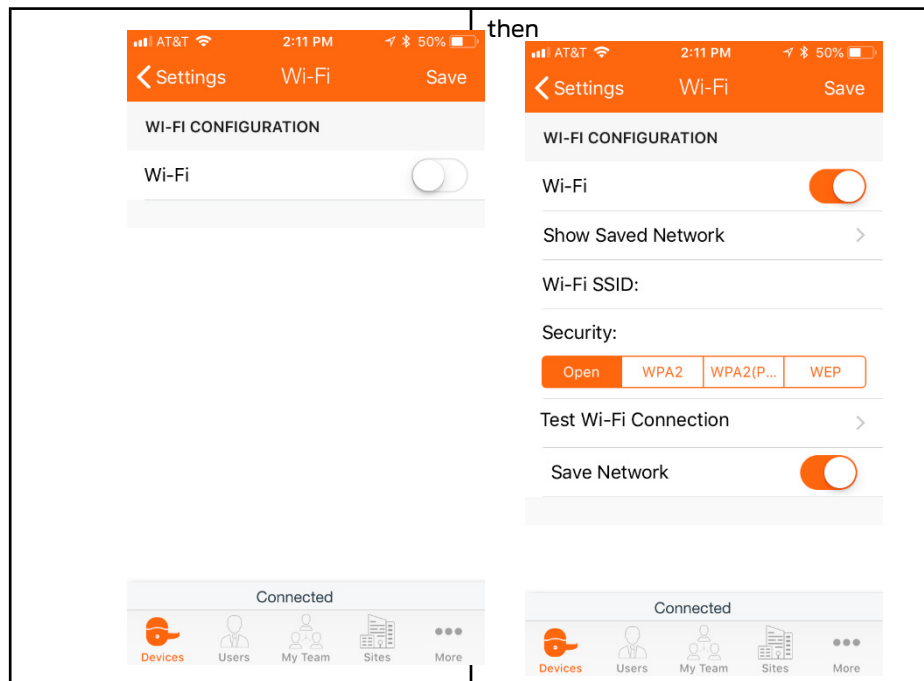


then



5. **Select Settings.**

6. **Select the Wi-Fi menu (under GENERAL).**



7. **Slide the Wi-Fi button to display the Wi-Fi setup menu.**

→ **Note:** The **Save Network** button is enabled by default

Wi-Fi network Security settings are automatically stored by the Mobile device and made available for menu selection (easier setup) on new Wi-Fi enabled devices.

8. **Select the Wi-Fi Security method to be used with your property.**

9. **Enter the required Wi-Fi configuration settings.**

- Passwords and/or Usernames may be required, based on the Security method selected.
- In this case we chose **WPA2(PEAP)** Wi-Fi Security and **610baLWLAN** Wi-Fi SSID

10. **Select Save** in the top right-hand corner of the Wi-Fi screen to accept the latest settings.

→ **Note:** Selecting Save also stores the Network details for selection later. Using a saved network setting can speed installation and setup time by preventing input errors. A Saved network must be locally available at the door when selected for a device. Some properties may have more than one Wi-Fi network SSID.

**WARNING: When the Wi-Fi Connection fails, recheck the following items:**

- Confirm that the network name (SSID) was entered correctly
- Confirm the network security is at the correct setting (Verify with the local IT Administrator)
- Confirm the PASSWORD entered was correct
- Verify the local Wi-Fi network is ON and available at this location

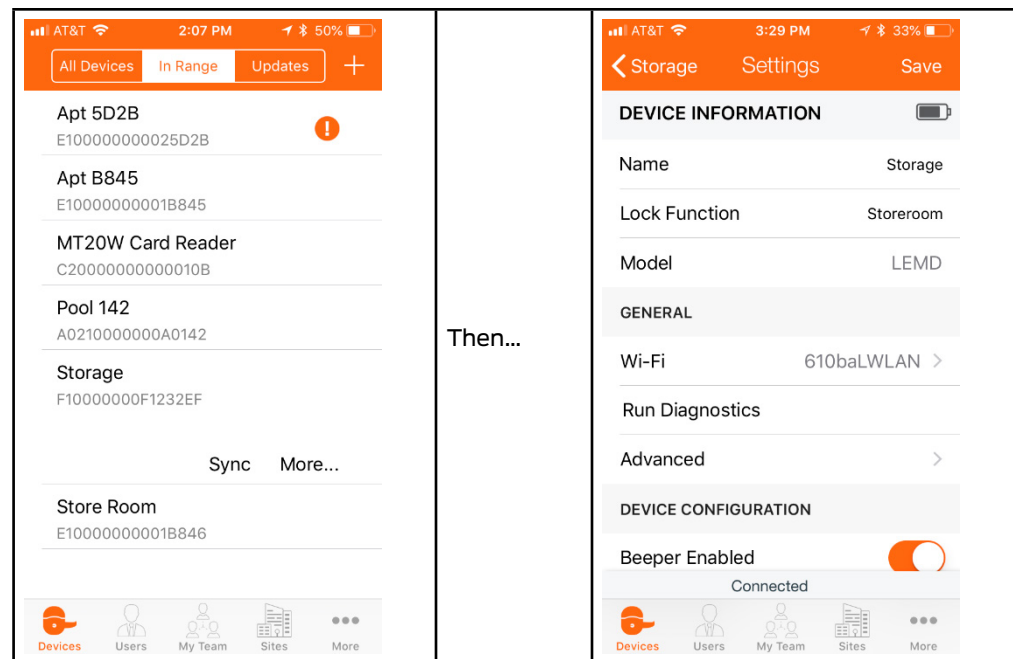
Alternatively, verify local Wi-Fi network settings using a Mobile phone to connect to the same Wi-Fi network intended for the device.

### Wi-Fi Network Connection VERIFY SUCCESS

The current Wi-Fi connectivity and connection settings can be immediately verified anytime the Administrator wants to make sure things are operating properly.

To verify Wi-Fi connectivity, follow these steps for any Wi-Fi enabled ENGAGE device.

1. Open the ENGAGE Mobile application and log into your account.
2. From the Device screen, select the "In Range" device to test its Wi-Fi network connection.
  - We chose **Storage**, which is a Schlage LE device.
3. **Select More ...**
4. View the currently assigned Wi-Fi SSID is (**610baLWLAN**)

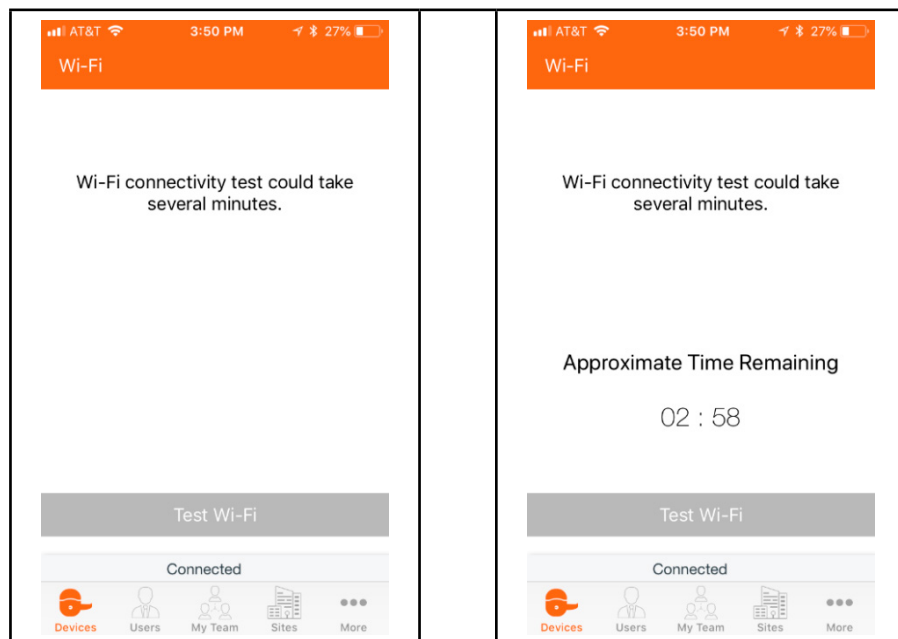


5. **Select the Wi-Fi menu under the General heading.**



→ **Note:** This example is for WPA2 (PEAP) network security. Username and Passwords are unique for this Wi-Fi network security

**6. Select Test Wi-Fi Connection menu.**



**7. Select Test Wi-Fi menu to initiate the test.**

→ **Note:** The device LED flashes AMBER while testing the Wi-Fi network connection. Be patient, this test can take a few minutes to complete

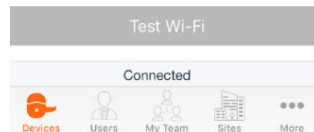
Once the Wi-Fi connections is completed, the Administrator will see the Success message below.



Wi-Fi connectivity test could take several minutes.

#### Success

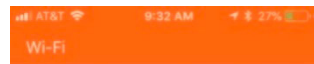
Device successfully connected to the host



#### 8. Acknowledge the Success message.

→ **Note:** The device now has its Wi-Fi connection verified and will now automatically “Call-In” each night for updates and Audits. This device may now be scheduled for firmware updates overnight. Device Audit information for this device will now include Wi-Fi signal strength and connection information.

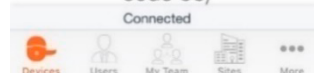
Should the Wi-Fi test fail, this Failure message will be displayed.



Wi-Fi connectivity test could take several minutes.

#### Failure

Failed to connect to access point. Confirm the Wi-Fi network User Name and Password and try again. (ref. code 55)



#### **WARNING:** When the Wi-Fi Connection fails, recheck the following items:

- Confirm that the network name (SSID) was entered correctly
  - Confirm the network security is at the correct setting (Verify with the local IT Administrator)
  - Confirm the PASSWORD entered was correct
  - Verify the local Wi-Fi network is ON and available at this location
- Alternatively, verify local Wi-Fi network settings using a Mobile phone to connect to the same Wi-Fi network intended for the device.

## Device Firmware Updates

Each individual device on a property should be kept up to date to ensure property-wide device compatibility and operations. Additionally, keeping all firmware in each device at the latest revision will ensure the latest ENGAGE features and product updates are provided at the door.

Firmware device updates are performed manually at the door using the ENGAGE Mobile Application or devices may be set up to use the local Wi-Fi network for automated updates when the device supports Wi-Fi connectivity.

- **Manual Firmware Updates at the door:** (required for **Control**)
  - Available for all ENGAGE enabled devices.
  - Uses the ENGAGE Mobile Application and Bluetooth connectivity
  - Requires the Administrator to be near the device being updated
- **Automated Firmware Updates – overnight:** (**recommended**)
  - Available for all Wi-Fi enabled ENGAGE devices
  - Scheduled for an overnight update from the ENGAGE Web Application.
  - Performed overnight using the local Wi-Fi network connection.
- **Manual Firmware Updates at the door** (without local Wi-Fi connectivity):
  - Allows for devices to be updated when no local Wi-Fi network is available.
  - Allows devices to be update when no “Cell Data Signal” is available for the Mobile device.
  - Uses the Mobile Device Wi-Fi Hotspot feature to communicate the firmware update to the device

Each ENGAGE device will accept the firmware download and then the device must install the firmware into its memory so that the new firmware can be used.

→ **Note:** Installing the downloaded firmware will take a few minutes to complete. The device will not be operational as an access control device until the firmware installation is completed. The device will flash the LED RED and GREEN for a few minutes and then RESET to begin normal operation.

### Manual Firmware Updates at the door

Manual firmware updates are performed while nearby the device using the ENGAGE 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.

Manual firmware updates using Bluetooth communication is required for Control devices because they do not support Wi-Fi connectivity.

### Automated Firmware Updates overnight (Preferred)

This is the preferred method of firmware updates to help keep all devices at the latest revision.

Using the local Wi-Fi network firmware updates is faster than using the Bluetooth communication option and may be automated and scheduled using the ENGAGE 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.

- 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.
- Once completed the device will RESET and begin operation, using the newly download firmware.

All ENGAGE product families may have firmware updates performed at the door with local Wi-Fi connectivity except Control.

### Manual Firmware Update at Door with No Local Wi-Fi

All ENGAGE Wi-Fi network enabled devices may have firmware updates performed at the door using Wi-Fi connectivity even when there is no local Wi-Fi network signal available.

It is possible for devices to be installed and used in areas that have no Wi-Fi network available or when the local Wi-Fi network is still not yet installed at the property.



When a device does not have a Wi-Fi network connection available or the local Wi-Fi network is out of service, device firmware downloads may be performed by temporarily enabling a Wi-Fi network connection through the Administrator's Mobile device.

To perform Wi-Fi enabled Sync at the door using the ENGAGE Mobile device follow these steps.

1. Open the ENGAGE Mobile application and log into your ENGAGE account.
2. Select the In-Range device to receive the firmware update.
  - The device being updated will be in an area without Wi-Fi network connectivity or the device does not have its Wi-Fi enabled (ON).

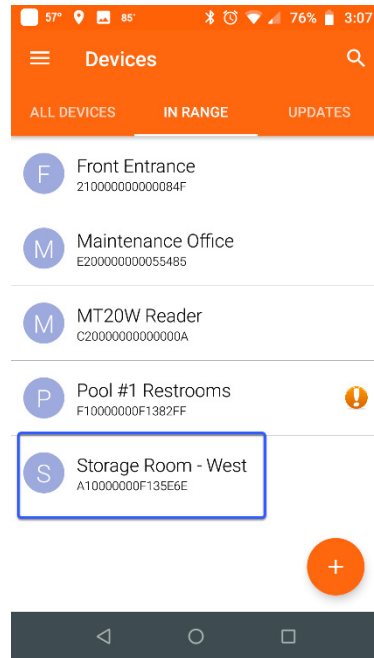


Fig. 12.107: Device

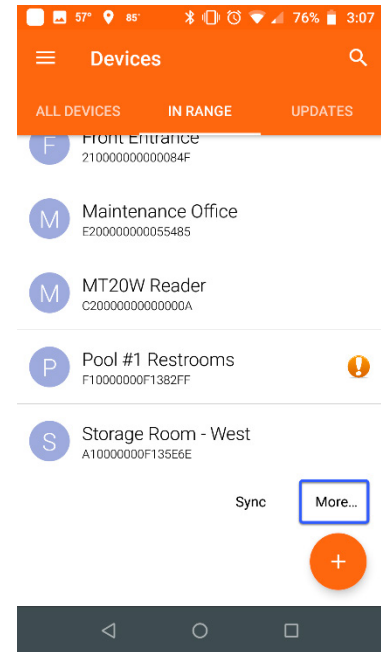


Fig. 12.108: More

3. Select More...
  - Wait a moment while the Mobile device connects with the lock.

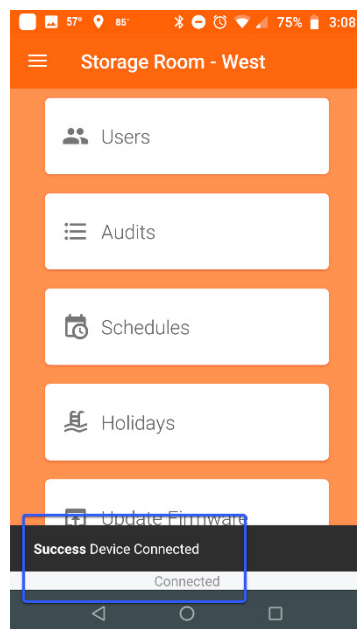


Fig. 12.109: Connected

then ...

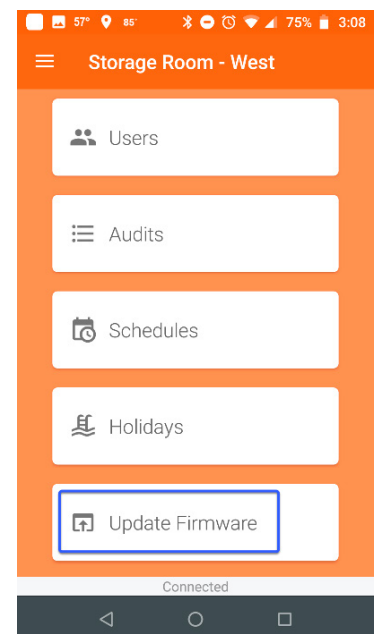


Fig. 12.110: Update Firmware

4. Select Update Firmware.

- The current firmware version is shown with the option to update firmware to a newer version – when available

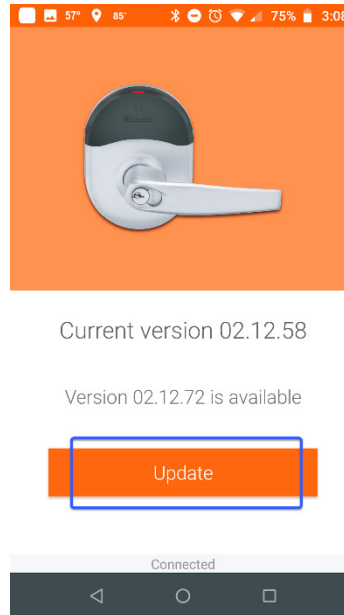


Fig. 12.111: Current Version

5. Select the Update button.

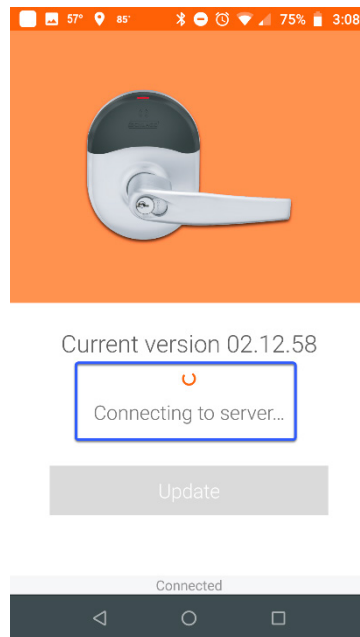


Fig. 12.112: Server Connecting

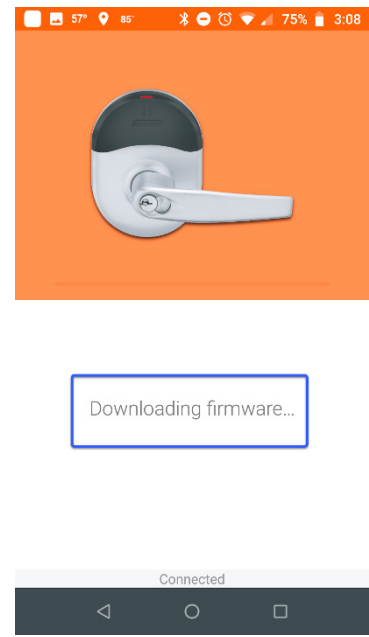


Fig. 12.113: Downloading

→ **Note:** While downloading a progress bar is shown. Firmware downloads can take a few minutes.

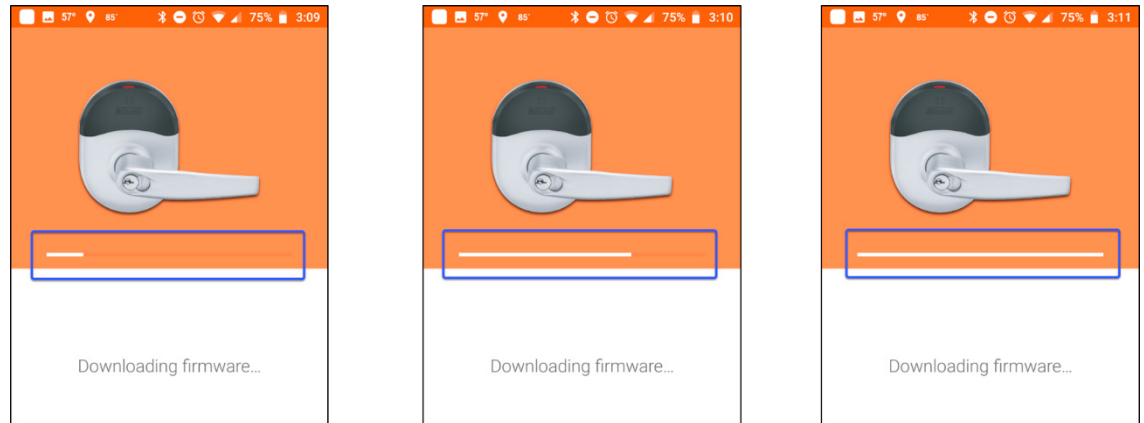


Fig. 12.114: Download Progress...

➔ **Note:** This download process will take a few minutes, be patient. After downloading, the device will take a few minutes to “Install the new firmware”. While installing the new firmware, the device will flash the LED RED and GREEN to show update status is progressing – be patient.

**WARNING:** The device will not operate as a locking device during the few minutes it takes for the firmware updates and installation process to complete.

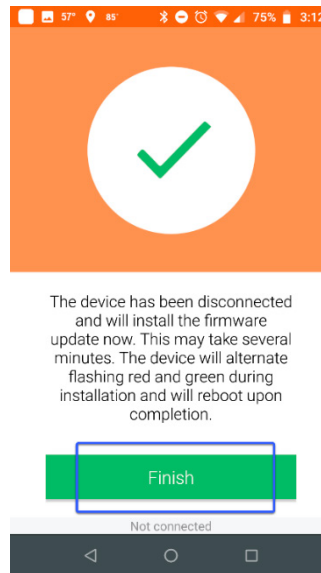


Fig. 12.115: Finish

#### 6. Select Finish.

➔ **Note:** When new firmware is downloaded to a device, the new firmware is not usable until the device installs the update into its internal memory. The device follows the successful firmware download with a firmware installation process that will take a few minutes. While updating the internal memory, the device LED will be blinking RED and GREEN for several minutes and the device will be Off-Line and not acting as an access control device. After LED stops flashing RED and GREEN, the devices' internal firmware update process is complete. The device will perform a RESET and begin normal operation.

### Automated Device Firmware Scheduled Updates

Automated firmware updates can be scheduled for an overnight update via the ENGAGE Web application and is available for the LE, NDE, CTE, and MT20W product families.

Use this method to automatically keep devices updated with the latest firmware revision and operational functionality.

**WARNING:** The LE, NDE, CTE, and MT20W product families must have their Wi-Fi network configured and a local Wi-Fi network available before overnight firmware updates are possible. Control Mobile Enabled Smart Locks do not support automated overnight firmware updates.

1. Go to the ENGAGE web application <https://portal.allegionengage.com/signin> and log into your account
2. Select Advanced menu, then the Firmware tab.
  - Compare the Current Firmware Version with the Latest Firmware Version for each device.

Device Name	Current Firmware Version	Latest Firmware Version
Back Office Door	01.07.58	01.07.67
Front Entrance	01.03.02	01.03.02
Maintenance Office	04.04.00	04.05.19
MT20W Reader	39.02.00	39.04.00000000
Pool #1	02.12.72	02.12.72
Pool #1 Restrooms	01.07.58	01.07.67
Storage Room - West	02.12.58	02.12.72

Fig. 12.116: Advanced &gt; Firmware

1. **Select** each device requiring a firmware update.
  - Remember, Control Mobile Enabled Smart Locks do not support the automated firmware updates and must be updated manually at the door with the ENGAGE Mobile application and a Mobile device.

Device Name	Current Firmware Version	Latest Firmware Version
<input checked="" type="checkbox"/> Back Office Door	01.07.58	01.07.67
<input type="checkbox"/> Front Entrance	01.03.02	01.03.02
<input type="checkbox"/> Maintenance Office	04.04.00	04.05.19
<input type="checkbox"/> MT20W Reader	39.04.00	39.04.00
<input type="checkbox"/> Pool #1	02.12.72	02.12.72
<input checked="" type="checkbox"/> Pool #1 Restrooms	01.07.58	01.07.67
<input checked="" type="checkbox"/> Storage Room - West	02.12.58	02.12.72

Fig. 12.117: Devices Selected

2. When finished, click **Update Selected Devices**.

- A 'firmware updates have been scheduled' message appears.

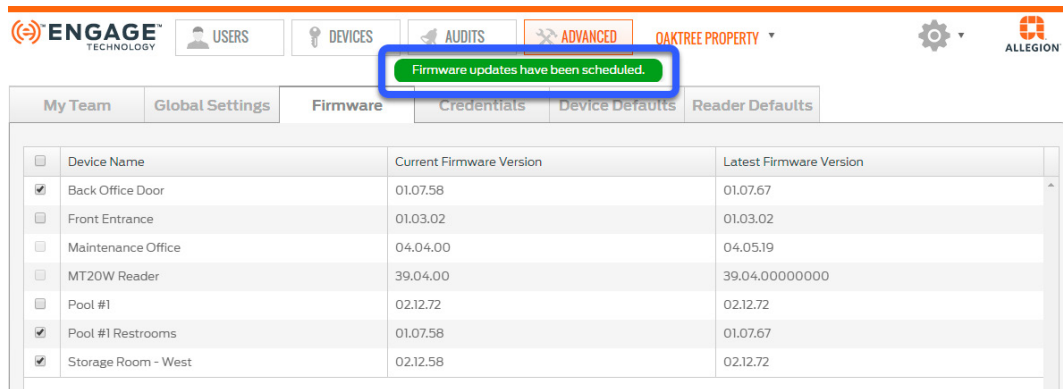


Fig. 12.118: Updates Scheduled

- The scheduled firmware updates will process overnight.
  - The day after the firmware updates were scheduled, review the current firmware version for each of the selected devices to ensure they have been updated and match the latest firmware version.

My Team	Global Settings	Firmware	Credentials	Device Defaults	Reader Defaults
Device Name	Current Firmware Version	Latest Firmware Version			
Back Office Door	01.07.67	01.07.67			
Front Entrance	01.03.02	01.03.02			
Maintenance Office	04.04.00	04.05.19			
MT20W Reader	39.04.00	39.04.00			
Pool #1	02.12.72	02.12.72			
Pool #1 Restrooms	01.07.67	01.07.67			
Storage Room - West	02.12.72	02.12.72			

Maintenance Office is a Control device therefore, does not have latest version.

Fig. 12.119: Firmware Updated

**CAUTION:** Nightly firmware updates are scheduled in the early morning hours during low Wi-Fi network activity to reduce user issues while the device is inoperative during the time it is being updated. Control Mobile Enabled Smart Locks **do not support** automated firmware updates.

- When a selected device did not update to the latest version, perform the following:
  - **Verify the Wi-Fi network communication and settings.**
    - Test Wi-Fi Connection using the ENGAGE Mobile Application
  - Ensure the **local Wi-Fi network was available and not offline** when the overnight updates were attempted.
    - Was the Wi-Fi network out of service?
  - After verifying the above items, **repeat steps 1-5.**

## Viewing Audit Information

Device and User Audits is information collected when any action is taken at a door.

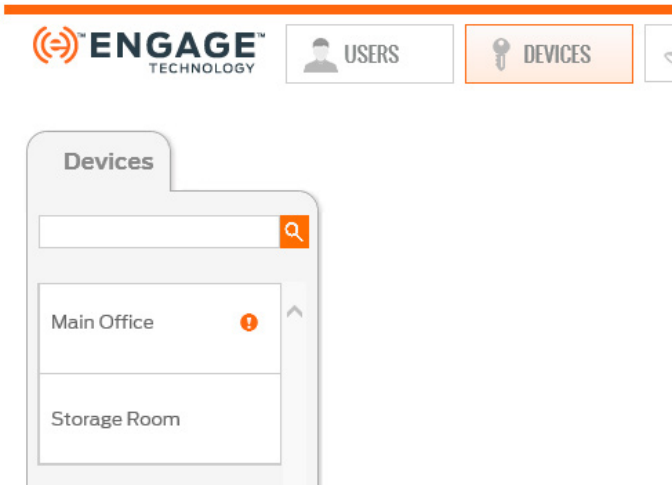
Viewing Audits can be invaluable for determining when users access certain areas, checking evidence of residence entry and for checking the device status and update history.

For Schlage Control Mobile Enabled Smart Locks, audits can only be retrieved locally at the door using the ENGAGE Mobile Application while all other ENGAGE devices may have Device and User audits gathered at the door, or remotely by taking advantage of these devices' nightly Wi-Fi network connection capability.

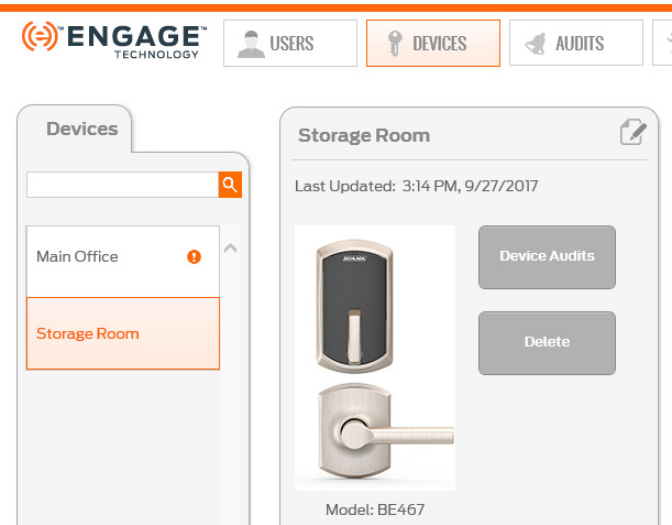
Audits may be reviewed by either the ENGAGE Web or Mobile Applications, however audit data may easily be filtered and exported for review and data analysis while using the ENGAGE Web Application.

Individual Device Audits Using the ENGAGE Web Application

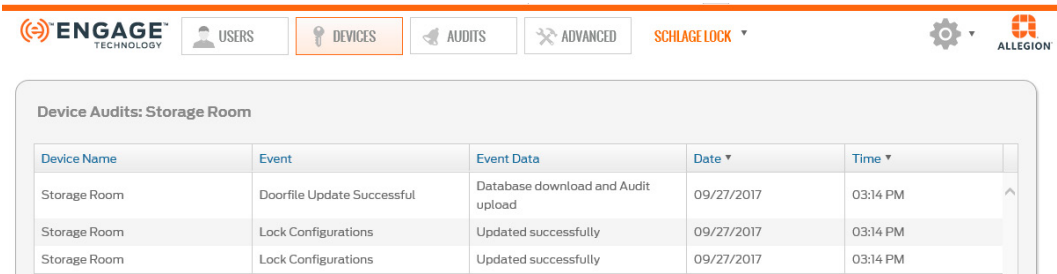
- 1. **Open** the ENGAGE Web Application.
- 2. **Select** the **DEVICES** menu and the **Devices** tab.



- 3. **Select** the desired lock from the list – we chose **Storage Room**.



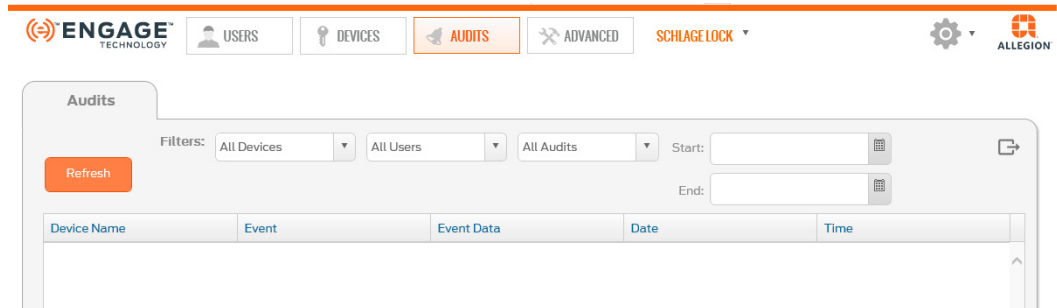
- 4. **Select Device Audits** button.




→ **Note:** **NOTE:** Sort the displayed data as necessary using the column headers.

### Property Wide Device Audits Using the ENGAGE Web Application


1. **Open** the ENGAGE Web Application.
2. **Select** the **AUDITS** menu and the **Audits** tab.



3. Use the available **Device**, **User** and **All Audits** sort and filter options.

4. **Select** the  button after each sort and filter action to view the updated fields and to view the latest Audits

→ **Note:** Audit data can be sorted or filtered by: Individual Users, Individual Devices, All Audits, With defined Start and End times

5. Use the EXPORT button at the top-right corner of screen to SAVE data into another file. 

→ **Note:** Data is saved into a .csv file for easy spreadsheet analysis. Save your audit file to disk for archive and analysis





# 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, enable the Master Credential feature with the ENGAGE Web Application, now.
  - Are all “Schedules” defined and properly entered into ENGAGE?
  - Then commission the MT20W as the first commissioned device.
- Determine property wide default 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 Sync 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 require Sync before the device knows which group it is assigned.
- Each User/Resident should NOT be assigned more than one credential.

Both HIGH and MAX reader sensitivity settings reduce device battery life

## ENGAGE Device Set-up

- Define the property wide Device 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.

## Control Mobile Enabled Smart locks

- Control devices do not support Wi-Fi connectivity.
- Every door access or device setting update **MUST** use the local Sync (Door File updates) process and the ENGAGE 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.

**⚠ 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.



### Schedules

- Schedules can **ONLY** be created or modified by the ENGAGE 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 Sync 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 Master Credential 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.

### 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.

#### Credentials

Credential 5034	Normal	
Credential 1	Normal	

- **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.

# Troubleshooting

## Activity and Diagnostics Audits

ENGAGE enabled devices provide diagnostic data anytime an action is taken at the device. Diagnostic data provided includes; Battery, Credential, debug-diagnostics, and door actions.

Device Audit data is gathered from the device anytime a Sync is performed. When using the nightly W-Fi enabled call-in, device data is gathered automatically.

Devices not using W-Fi network connection will require a local Sync at the door using the ENGAGE Mobile Application. Follow these steps:

- Open the ENGAGE Mobile Application.
- Select the **In Range** tab.
- Select the specific nearby device to gather **Diagnostic** data.
- Select **More**.
- Select **Audits**.
- Select the **Diagnostics** tab at the top.
- Scroll through the displayed information to view the available diagnostic audits.

**Audits** may be viewed with the ENGAGE Mobile or Web applications.

## Inviting Team Members

- If an email invitation never arrives in the team members email account:
  - Check the team members SPAM and TRASH folders for misplaced email.
  - Verify the entered email address is correctly entered in the ENGAGE account.
  - Verify your PASSWORD.

## Device Commissioning

- If the 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.)

## Construction Mode

- If a 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.

## MT20W

- When power is applied, the Schlage MT20W LED is RED for about 20 seconds, until the Schlage MT20W boots-up and begins operation.
- Boot-up is complete when the Schlage MT20W blinks red and beeps three times.
  - If the Schlage MT20W is not commissioned the LED remains solid RED.
- When using Wi-Fi connectivity:
  - The MT20W will attempt to connect to the local Wi-Fi network any time power is applied.
  - When connected and communicating the MT20W displays a solid Blue LED indicating it is ready for use.
  - The local Wi-Fi network must be locally available to the MT20W.
- When connecting via USB communication:
  - The ENGAGE Desktop PC Application must be installed and running.
  - The MT20W LED flashes fast BLUE for a few seconds followed by a solid Blue LED when the connection and communication is accomplished.

## 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.

## 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 be recorded with inaccurate times

### Perform a Schlage Control “Jump Start”

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

**⚠ CAUTION:**  
Replace the device AA batteries with Alkaline ONLY! Alkaline AA batteries are required for proper operation. Do Not use any other battery technology (Lithium, etc.)

## Setting Device Date and Time

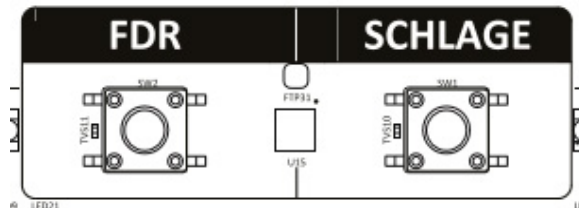
- Device date and time is automatically checked and set each time a Mobile device is connected and communicating with the ENGAGE device.
- Setting the date and time should only be necessary when the device power has been removed for an extended period. (Battery Replacements, Jump Start-Control)
- To connect to any device and set the current Date and Time, follow these steps:
  1. Open the ENGAGE Mobile Application.
  2. Select the **In Range** menu.
  3. Select the nearby 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
- View the Device Date and Time settings have been set into the device.

## 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" feature in the Mobile Application to verify Wi-Fi communication.

## 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.
- To pair a Schlage CTE and Credential Reader follow these steps:



1. Press and Release the Schlage Button one (1) time.
2. Press and Release the FDR button two (2) times.
3. The Credential Reader blinks AMBER three (3) times to indicate successful pairing.

# 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 NDE: Battery life is 1 - 2 years depending on use.
- Schlage LE: Battery life is 1 - 2 years depending on use.

 <b>NOTES</b>	<ul style="list-style-type: none"><li>• Advanced device reader sensitivity settings (High/Max) and Mobile Enabled device settings (Performance, Communication Range) will reduce battery life</li></ul>
---	---

### 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.
- 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.
- 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 No-Tour?

- 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.
- 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.

**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).

### 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).

### Why do ENGAGE Web Application Badge searches fail?

- 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.

### ENGAGE Mobile Access application Invitation Text not received

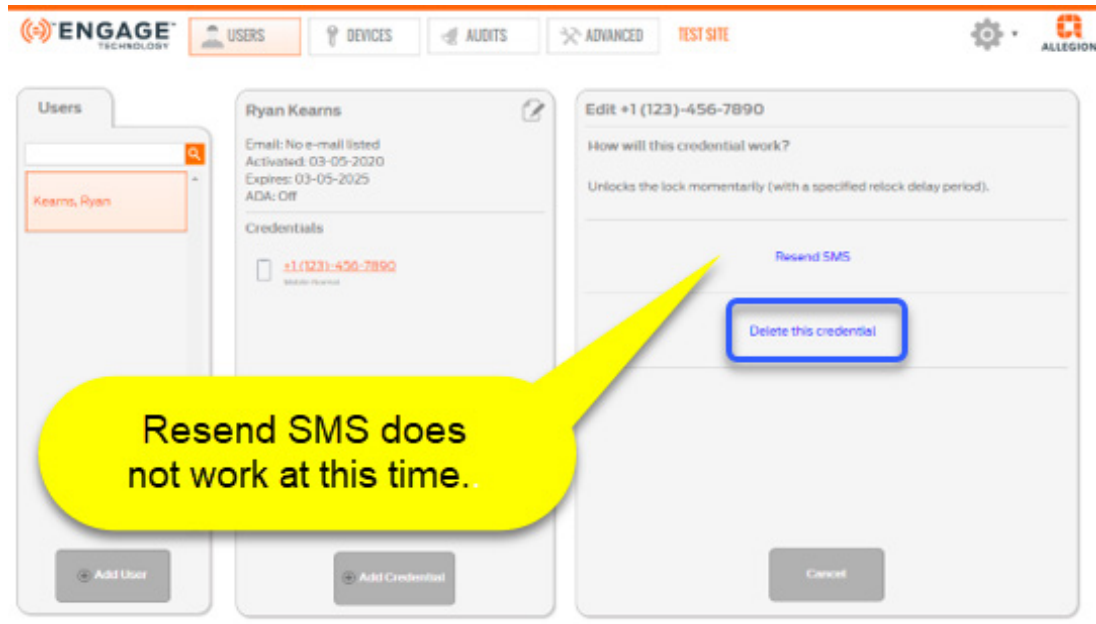
Check the following if user did not receive the invitation text message.

Verify the user's Mobile number was entered correctly.

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.

## Frequently Asked Questions



### Mobile credential user is unable to unlock assigned door.

Ensure the following tasks has been performed.

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.

### Customer Care & Technical Support

Customer Care & Technical Support is available via the following methods:

ENGAGE Support Page: <https://us.allegion.com/en/home/allegion-engage-program/resources.html>

ENGAGE Resources Library: <https://us.allegion.com/en/home/products/categories/electronic-locks/ENGAGE-web-Mobile-apps.html>


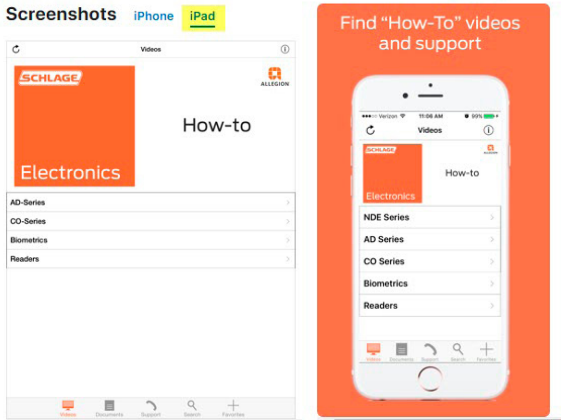
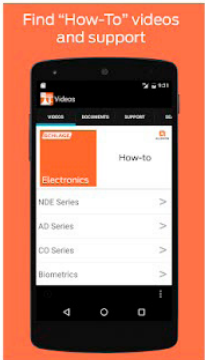
Email: [electronic\\_lock\\_techprodsupport@allegion.com](mailto:electronic_lock_techprodsupport@allegion.com)

Phone: For ENGAGE devices call 1.877.671.7011 then option 2, option 2. Hours of operation are Monday – Friday from 8 am to 8 pm EST, closed holidays.

## Appendix A: Capabilities by Property Role

#	Capability	Administrator	Manager	Operator
<b>Roles &amp; Application Access</b>				
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
<b>User Management</b>				
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	
<b>Device Management</b>				
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
<p>View 'how-to' videos via the Schlage YouTube channel. For best viewing results, use Chrome.</p> 	<p><a href="#">Schlage YouTube Channel</a></p>
<p>Screenshots <b>iPhone</b> iPad</p>  <p>View 'how-to' videos, product datasheets, and install sheets on your iPhone or iPad.</p>	<p><a href="#">iOS: Schlage Electronics How-To App</a></p>
<p>View 'how-to' videos, product datasheets, and install sheets on your Android.</p> 	<p><a href="#">Android: Schlage Electronics How-To App</a></p>

## Appendix C: ENGAGE 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 <b>does not</b> 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 <b>does not</b> 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](http://www.allegion.com)**.

*aptiQ* ■ **LCN** ■ **SCHLAGE** ■ **STEELCRAFT** ■ **VON DUPRIN**