About this document:

- This document provides functional descriptions and basic product information OVERVIEW for the ENGAGE™ System and family of products.
- Please refer to the appropriate device installation instruction and system setup requirements for detailed hardware door preparation and device installation instruction.
- This document describes the ENGAGE™ Managed system operation at the following major revision level(s)

<table>
<thead>
<tr>
<th>System Software</th>
<th>Device Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENGAGE™ = 6.1.1</td>
<td>Schlage MT20W = 39.00.00</td>
</tr>
<tr>
<td></td>
<td>Schlage Control™ = 03.06.07</td>
</tr>
<tr>
<td></td>
<td>Schlage NDE = 02.12.57</td>
</tr>
<tr>
<td>Mobile Application Software</td>
<td>Schlage LE = 01.07.57</td>
</tr>
<tr>
<td>Android = 3.1.144</td>
<td>Schlage CTE = 01.03.01</td>
</tr>
<tr>
<td>iOS = 2.1.128</td>
<td>Schlage MT11 / MT15 = 09.32.04</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REVISION</th>
<th>COMMENTS</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SES20171127A</td>
<td>Initial release @ ENGAGE 6.0</td>
<td>November 28, 2017</td>
</tr>
<tr>
<td>SES20171127B</td>
<td>Updates to ENGAGE 6.1</td>
<td>August 01, 2018</td>
</tr>
<tr>
<td>SES20171127C</td>
<td>Updates to ENGAGE 6.1.1 (Device Groups)</td>
<td>August 15, 2018</td>
</tr>
</tbody>
</table>
# Table of Contents

ENGAGE™ 6.1.1 Guide.................................................................................................................. 1

Table of Contents...................................................................................................................... 2

Introduction to ENGAGE™ Access Control ............................................................................ 6

The ENGAGE™ Enabled Devices .............................................................................................. 9

The ENGAGE™ Wi-Fi network requirements........................................................................... 11

The ENGAGE™ Mobile Devices ............................................................................................. 12

The ENGAGE™ Mobile Application Requirements................................................................. 12

The ENGAGE™ Web Application............................................................................................ 13

The ENGAGE™ Web Browser Requirements ......................................................................... 13

The ENGAGE™ Mobile Application ....................................................................................... 14

Property Management Options ............................................................................................... 15

User Credentials and Construction Credentials ................................................................. 16

Configuration Cards ................................................................................................................ 22

No-Tour Features ...................................................................................................................... 24

Initial Account Setup ................................................................................................................ 30

Creating an ENGAGE™ Account ............................................................................................ 30

Account Team Members .......................................................................................................... 35

Schedules Overview ................................................................................................................ 39

Creating Device and User Schedules .................................................................................... 40

Creating Holiday Schedules ................................................................................................. 43

Property Wide Default Device Settings ................................................................................. 45

Device Commissioning .......................................................................................................... 57

Creating Users ......................................................................................................................... 100

Enrolling Credentials ............................................................................................................ 103

Creating Device Groups ......................................................................................................... 115

Assigning Lock Access and User Schedules ......................................................................... 120

Sync – Updating a Door File .................................................................................................... 126
Sync – Overnight – Schlage NDE, LE, and CTE ................................................................. 129
ENGAGE™ Product Family Hardware Installation ........................................................... 140
  When working with Schlage® MT20W ........................................................................ 140
  When working with Schlage Control™ smart locks ..................................................... 141
  When working with Schlage® NDE wireless cylindrical locks ................................... 148
  When working with Schlage® LE wireless mortise locks .......................................... 156
  When working with Schlage® CTE single door controllers ...................................... 162
Daily System Operations ................................................................................................. 169
  Adding a User ............................................................................................................. 169
  Enrolling Credentials ................................................................................................. 171
  Assigning Credentials ................................................................................................. 183
  Adding New Devices .................................................................................................. 186
  No-Tour Credential Programming .............................................................................. 187
  Searching for Credential Owners ................................................................................ 189
  Resident Moves Out .................................................................................................... 190
  Deleting Existing Access ............................................................................................ 191
  Deleting a Credential .................................................................................................. 192
  Deleting Devices ......................................................................................................... 195
  Replacing Credentials ................................................................................................ 199
  Updating Device Firmware ........................................................................................ 204
  Scheduled Firmware Updates – Schlage NDE, LE, and CTE .................................... 218
  Retrieving Audit Data from Devices ........................................................................... 221
  Viewing Audit Information ......................................................................................... 225
  Master Credentials ..................................................................................................... 228
Things to Remember ...................................................................................................... 238
  Best Practices – System Set-up .................................................................................. 238
  Best Practices – Device Set-up ................................................................................... 238
  Schlage Control™ smart locks ................................................................................... 238
Schedules.................................................................................................................................................. 239
Master Credentials...................................................................................................................................... 239
Update ICONS.......................................................................................................................................... 239
Factory Default Reset................................................................................................................................ 240
Moving Devices Between ENGAGE™ Accounts...................................................................................... 240
Dual Technology Credentials (Schlage NDE, LE, and CTE ONLY)....................................................... 240
Troubleshooting......................................................................................................................................... 241
All devices – Diagnostic Audits ................................................................................................................ 241
Inviting Team Members............................................................................................................................. 241
Device Commissioning............................................................................................................................... 241
Construction Mode.................................................................................................................................... 241
Schlage MT20W (overview) ....................................................................................................................... 241
Schlage MT20W would not connect to the Wi-Fi Network................................................................. 242
Schlage Control™ - "Jump Start" Process.............................................................................................. 242
Set Device Date and Time .......................................................................................................................... 242
Device Firmware Updates Overnight were not performed................................................................. 243
Schlage CTE and Credential Reader stopped working........................................................................ 243
Frequently Asked Questions .................................................................................................................. 244
  1. How can I determine the local Wi-Fi network settings? ................................................................. 244
  2. Will ENGAGE™ work with 5.0GHz network routers?................................................................. 244
  3. What is the Wi-Fi network “Mandatory Data Rate”? ................................................................. 244
  4. What is the ENGAGE™ Mobile device Bluetooth communication range?.............................. 244
  5. What are the different ENGAGE™ Team Member Capabilities?.................................................. 244
  6. Do Property "Team Member" invitations Expire? ............................................................................. 244
  7. How do I know the Schlage MT20W is working? ........................................................................... 245
  8. What are the Battery Life expectations of ENGAGE™ devices? .................................................. 245
  9. What happens when a device battery gets low? .............................................................................. 245
 10. What is a Nuisance Delay? .............................................................................................................. 245
11. What is Critical Battery Mode? ................................................................. 246
12. Can I use Lithium batteries? ................................................................. 246
13. Why use a Software Alliance Member (SAM) Managed Account? .......... 246
14. Can I change a ENGAGE™ managed account to a SAM account? .......... 246
15. What concerns are there with No-Tour? ................................................ 246
16. What concerns are there with Schlage Control™ devices and Schedules? .... 246
17. Why do ENGAGE™ Web application credential searches fail? ................. 247

APPENDIX A – Property Role Assignment and Capabilities ................................ 248
    Administrator – Manager – Operator ....................................................... 248

APPENDIX B – ENGAGE™ Training Videos ............................................... 249
    Videos on YouTube ............................................................................... 249
    Videos on “Schlage Electronics How-To” mobile application ................. 249

APPENDIX C – ENGAGE™ Credentials ..................................................... 250
    ENGAGE™ Credential Functions ......................................................... 250
Introduction to ENGAGE™ Access Control

Overview

The ENGAGE™ cloud-based standalone security solution simplifies the ability to connect people, openings, and access management to deliver cost effective electronic access control and efficiency to any property.

The property administrator will have the option to use the ENGAGE™ Web application and its companion ENGAGE™ Mobile application to provide basic Access Control for their property or the property administrator may choose a Software Alliance Member (SAM) Access Control Platform for additional Access Control features.

With the ENGAGE™ cloud-based web and mobile applications, it’s easy to configure lock settings, manage users with basic access privileges, and view lock audits and alerts from almost anywhere.

IMPORTANT NOTE: Customers should consult with their Allegion sales consultant and/or a Software Alliance Member (SAM) before starting an ENGAGE™ account

Every property will be required to begin with an ENGAGE™ Account to enroll and initially configure system components no matter which Access Control solution is chosen.

You will begin by selecting “Create Account” from this ENGAGE™ welcome screen.
**ENGAGE™ Managed properties**

**ENGAGE™ Managed** property administrators will use both the **ENGAGE™ Web application** and the **ENGAGE™ Mobile applications** to manage their property.

These **ENGAGE™** applications are provided free of charge.

**Software Alliance Member Managed properties**

Property Administrators that choose to use a **Software Alliance Member** (SAM) Access Control Platform for additional features, must consult with an alliance member for details.

**System Management using Web browsers and Mobile devices**

Many **ENGAGE™** features and settings can be managed from either the **ENGAGE™ Web application** or with the **ENGAGE™ Mobile application**. It is recommended that customers use the **ENGAGE™ Web application** when possible for its ease of use, viewing on a larger screen, and for easier data inputs via a standard keyboard.

The **ENGAGE™ Web application** is supported by these popular web browsers:

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

The **ENGAGE™ Mobile application** is supported by these devices and Operating Systems:

- iOS
- iOS 10 or newer
- iPhone 6 or newer
- iPad Air, iPad Air 2, iPad Mini 2, and newer
- Android
- Lollipop 5.0 and newer
- Google Nexus 5X, Pixel or newer
- LG G6 or newer
- Moto Droid
- Samsung Galaxy Tab 2 or newer
- Samsung S6 or newer

Routine access right(s) and setting(s) updates in the devices installed on your property can be accomplished using any of the three device update methods.

1. **Immediate Updates at the door (Sync) using the ENGAGE™ Mobile application**

2. **Automatic Daily Updates (Sync) with optional local Wi-Fi network connection(s)**
   - a. Available with our Wi-Fi capable devices

3. **No-Tour access rights updates delivered to the door via smart credentials (read/write) when programmed on the MT20W enrollment reader**

![Image of locks and devices]

Send updates wirelessly at the lock with the ENGAGE mobile application on a Bluetooth® enabled smart phone or tablet. Or leverage the existing Wi-Fi network or built-in No-Tour capability to send periodic updates without visiting the lock.

- Update access rights
- Update lock/device settings
- Update firmware
- Perform diagnostics

![Immediate Updates, Automatic Daily Updates, No-Tour via Smart Credentials]

**NOTE:** Schlage Control™ smart locks do not include Wi-Fi network connectivity and are **not** compatible with automatic daily updates

Device sync updates will be required any time major system settings are enabled or changed, anytime user access rights change, when door settings or device groups are modified, or when new device firmware is available for download.
The ENGAGE™ Enabled Devices

The family of ENGAGE™ enabled products include the devices briefly described below.

➢ **Schlage® MT20W**: The ENGAGE™ technology smart credential enrollment and programmer

- Powered by a standard computer USB connection, or USB power block
- May be used anywhere there is a USB power and local Wi-Fi network access
- Communicates via local Wi-Fi network and Bluetooth® Low Energy (BLE) connection
- The MT20W credential enrollment reader connects to the local property Wi-Fi network for communication to the ENGAGE™ Web application or Software Alliance Member (SAM) server.
- The MT20W is used to enroll user credentials into the ENGAGE™ Managed Account and to program credentials for access updates using the No-Tour features.

➢ **Schlage Control™** smart deadbolt or interconnected lock:

- 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

➢ **Schlage® NDE** wireless cylindrical lock with ENGAGE™ technology:

- Cylindrical lever lock
- Mechanical key override
- 4 AA Batteries required (Alkaline only)
- Wireless communication: Bluetooth and Wi-Fi
- Always allows egress
- Storeroom function only
- Construction mode is based on MASTER and USER construction card enrollments
➢ **Schlage® LE** wireless mortise lock with ENGAGE™ technology:

- 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
- Always allows egress
- Storeroom, Apartment, Office, and Privacy functions available
- Construction mode is based on MASTER and USER construction card enrollments

➢ **Schlage® CTE** single door controller with multi-technology reader: For common areas and openings that require alternate locking devices.

- 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 an Schlage MT11-485 or MT15-485 credential reader – if desired
- Powered and relay outputs available for locking devices to include: E-strikes, E-trims, mag locks, Exit Devices, Auto-Operators, etc.
- The Schlage® CTE works exclusively with the Schlage MT11-485 or MT15-485 credential readers
- Construction mode is based on MASTER and USER construction card enrollments

<table>
<thead>
<tr>
<th>MT11</th>
<th>MT15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-technology – mullion</td>
<td>Multi-technology – single gang</td>
</tr>
</tbody>
</table>

**WARNING:** The ENGAGE™ Web application and the CTE do not support keypad functionality. Wall readers with keypads (MTK11-485 and MTK15-485) cannot be used with CTE.
The ENGAGE™ Wi-Fi network requirements

ENGAGE™ will use the local Wi-Fi network to enable many functions automatically for the property administrator, when the device(s) are Wi-Fi enabled.

The Schlage MT20W requires a local Wi-Fi network to enroll and program resident credentials while the Schlage NDE, LE, and CTE devices may be setup to utilize the local Wi-Fi network for daily updates and automated system maintenance. Remember, Schlage Control™ devices do not support Wi-Fi network connectivity.

The Schlage MT20W, NDE, LE, and CTE devices have the following requirements when working with Wi-Fi network settings:

NOTE: Consult with your local IT professional when working with Wi-Fi network connectivity. Alternatively, a mobile phone can be used to connect to the local Wi-Fi network to verify proper local Wi-Fi settings.

- **2.4Ghz (802.11 b/g) required.**
  - Additionally, the Schlage LE and CTE devices may use **2.4Ghz (802.11 b/g/n)**

- **Connect Data Rate:** 24Mbps or lower
  - IT professionals use this setting to force a required minimum data rate that is required before the device can connect to the Wi-Fi access point. Connect Data Rate setting is intended to improve Wi-Fi network performance and not allow weak or slow data rate devices to connect.
  - Each Wi-Fi network access point requires the Mandatory Connect Data Rate setting to be **24Mbps** (24 Mega-bits per second) or lower for Schlage NDE and MT20W connectivity.
    - The local IT professional can verify this setting if/when devices are not able to connect to the local Wi-Fi network.
  - The network router Connect Data Rate default setting usually is “Auto”

- **Connect to Internet** screens: The network connection should not require additional “Connect to Internet” pop-up or message acknowledgements

- Wi-Fi network security types supported:
  - **WPA2 (PEAP)** Wi-Fi SSID - Must be EXACT (case sensitive)
    - USERNAME
    - PASSWORD*
  - **WPA2** Wi-Fi SSID - Must be EXACT (case sensitive)
    - PASSWORD*
  - **WEP** Wi-Fi SSID - Must be EXACT (case sensitive)
    - PASSWORD*
  - **OPEN** Not recommended
    - No security
    - * PASSWORDs must be 64-character length
      - (max) and English alpha-numeric characters only
The ENGAGE™ Mobile Devices

The ENGAGE™ property administrators will need a commercially available mobile phone or tablet to perform many mobile ENGAGE™ functions with nearby devices. The latest “Flagship” mobile devices are always recommended for the best functionality and robust performance.

Mobile Devices compatible with ENGAGE™ can be either iOS or Android devices and both mobile phones and tablets are supported.

NOTE: Tablets must have an internet connection, either Wi-Fi or cellular service and Bluetooth (BLE) to be used as an ENGAGE™ mobile device.

Communication from a mobile device to an installed device is accomplished wirelessly using either low energy Bluetooth (BLE) communication or standard (2.4 GHz 802.11 b/g) Wi-Fi network depending on the device and function being performed.

NOTE: No cabling is ever required between the Mobile Device and the ENGAGE™ enabled products

The ENGAGE™ Mobile Application Requirements

- The ENGAGE™ Mobile application works best with the following software and hardware versions:
  - iOS
    - iPhone 6 or newer
    - iOS 10 or newer
    - iPad Air, iPad Air 2, iPad Mini 2, and newer
  - Android
    - Lollipop 5.0 and newer
    - Google Nexus 5X, Pixel or newer
    - LG G6 or newer
    - Moto Droid
    - Samsung Galaxy Tab 2 or newer
    - Samsung S6 or newer

NOTE: The latest “Flagship” mobile devices are always recommended for optimum system and mobile application performance.
The ENGAGE™ Web Application

The ENGAGE™ Web application is used to setup and manage a property with ENGAGE™ enabled devices. Management of the property is accomplished from virtually anywhere using a convenient web browser.

Use the ENGAGE™ Web application for property management data entry and general maintenance. The Web application is the easiest way to enter data and view your property information using a standard keyboard and a larger monitor screen.

Your ENGAGE™ account can be created by entering the URL below into your web browser and clicking “Create Account.” All that is required is a valid email address and a unique password.

After reviewing this document and planning your property requirements, go here to begin:

https://portal.allegionengage.com/

The ENGAGE™ Web Browser Requirements

- The ENGAGE™ Web application works best with the following web browsers:
  - Google Chrome 48.0 or newer
  - Microsoft Edge 12 or newer
  - Mozilla Firefox 49 or newer
  - Internet Explorer 11.0 or newer
  - Safari for Mac OS 10 or newer
The ENGAGE™ Mobile Application

The ENGAGE™ Mobile application must be used to commission ENGAGE™ devices into your account. The mobile application is a companion application to the ENGAGE™ Web application, or your SAM account. The mobile applications are available for free download on the familiar mobile device download sites for both iOS and Android devices. Search the app store for “Allegion ENGAGE”

- Get the ENGAGE™ mobile app from the iTunes App Store (iOS)
- Get the ENGAGE™ mobile app from the Google Play Store (Android)

You will use the ENGAGE™ Mobile application for operations to be accomplished while at the door, or nearby a device using Bluetooth (BLE) communication. Bluetooth communication is limited in range and the user should be as close as possible to the device for robust Bluetooth communications.

Operations normally performed at a nearby door include device commissioning, device setup and door file updates (Syncing), gathering device audit history, performing diagnostics, and can also include firmware updates to the device.

The chart below describes what functions are available and shared between the ENGAGE™ Web and Mobile applications.

<table>
<thead>
<tr>
<th>Function</th>
<th>ENGAGE™ Mobile</th>
<th>ENGAGE™ Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commission Locks and devices</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Commission MT20W</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Add Users</td>
<td>Yes, Better with Keyboard</td>
<td>Yes</td>
</tr>
<tr>
<td>Assign Credentials</td>
<td>Yes; use lock as reader; No-Tour is not available</td>
<td>Yes; No-Tour available</td>
</tr>
<tr>
<td>Grant User Access</td>
<td>Yes, must be at lock to update</td>
<td>Yes</td>
</tr>
<tr>
<td>Invite Team Member(s) to Manage Site</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Audits</td>
<td>Retrieve and View</td>
<td>View Only</td>
</tr>
<tr>
<td>Schedules</td>
<td>Assign Schedules</td>
<td>Create, Edit, and Assign Schedules</td>
</tr>
<tr>
<td>Global settings</td>
<td>No</td>
<td>Set and Edit</td>
</tr>
</tbody>
</table>
Property Management Options

Properties are managed using ENGAGE™ Web and Mobile applications described in this document, or properties may partner with our Software Alliance Members (SAM) for additional functionality.

Customers should consult with their Schlage sales representative and/or a Software Alliance Member (SAM) before starting their ENGAGE™ account

An **ENGAGE™ Managed** Account will provide the following options:

- A standalone 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

An **ENGAGE™ Software Alliance Member** (SAM) Account will provide the following options:

- A networked system managed with Software Alliances
- A system managed by a service provider
- Real-time device and system updates (where applicable)
- Expanded capacities for credential management and door openings
- Additional features – video capabilities, enhanced security and IoT connectivity

NOTE: Consult with a Software Alliance Members (SAM) to review and confirm their property management options.
User Credentials and Construction Credentials

There are two different credential functions defined for the credentials used with ENGAGE™. Credentials can be defined as User Credentials for normal access or as Construction Credentials for temporary access before the ENGAGE™ access control system is fully installed. The User and Construction credential types are described below:

Electronic credentials

Eliminate the time and costs associated with managing keys or re-keying locks by upgrading to electronic credentials. Provide a unique credential to authorized users that can be:
- Tracked for usage
- Added and removed remotely
- Assigned to be valid during specific days and times
- Deleted and replaced if lost or stolen – without having to re-key the lock

NOTE: 9691T is a dual Prox and Smart technology credential which may be most useful when using No-Tour, while also managing Proximity technology readers in common areas

User Credentials

User Credentials are available in card or fob physical formats. Both physical formats are available in multiple technologies: Proximity (read only), Smart (read/write) card Technologies, or Multi-Tech technology cards with both Smart and Proximity capability.

NOTE:
- A Proximity credentials provide a unique card serial number and facility code.
- Smart cards provide a unique card serial number and facility code, however smart cards can be written to and will carry additional access and update information when used for No-Tour.
- Smart credentials must be used for No-Tour applications.
- Schlage Control™ smart locks require smart card technology and are not compatible with Proximity credentials.
- 9651 - MIFARE Classic® Smart 1K byte and 9651T - MIFARE Classic Smart 1K byte thin key fobs are recommended. (highlighted above)
- Multi-tech technology credentials like the 9691T are most useful when both technologies are used for common areas and access control throughout the property.
Construction Credentials and Construction Mode

Construction Credentials are used for temporary access before the locking devices are Commissioned and programed with normal access rights by the property administrator.

Property administrators should be aware of some important facts for locking devices operating in Construction Mode.

- Construction Mode is enabled by default from the factory and after a device is successfully set back to Factory Default Reset (FDR)
- No audit information or credential use history is recorded in construction mode
- Construction credentials are a “Normal” credential function and will momentarily engage the thumb turn on Schlage Control™, or provide a momentary unlocking and relocking on Schlage NDE, LE, and CTE
- Each device in Construction Mode will relock after its Relock Delay period has expired
- Schlage Control™ devices allow Construction access based on the Facility Code (FC) of the initial credential presented
  - One construction credential presentation sets the Facility Code for all other Construction Credentials
- Schlage NDE, LE, and CTE devices allow construction access based on the card serial number.
  - Each User Construction credential must be enrolled separately before it can be used for construction access
- Factory Default Reset (FDR) is required to disable Construction Mode
- All previously valid Construction credentials will be denied access after FDR or Commissioning of a device is successfully accomplished
- Schlage Control™ devices require a 9651 - Schlage MIFARE Classic® Smart 8K bit Key fob credential to be used for Construction Mode access, all other devices may use any normally valid credential
- Credential serial number range and Facility Code (FC) must be assigned by the Res CardTrax™ Account CT8X4248 that is maintained internally by Allegion.
  - CardTrax account MUST be referenced on Construction Credential orders for Schlage Control™ smart locks
- Schlage NDE, LE, and CTE devices will allow any normally valid credential to be used for Construction Mode Access, Schlage Control™ devices require a 9651 - Schlage MIFARE Classic® Smart 8K bit key-fob credential to be used for Construction Mode access
Enabling Construction Mode (Schlage Control™)

When used with Schlage Control™, construction mode allows access for ALL credentials with the SAME Facility Code (FC) as the original card that was initially presented. One valid card presentation will set the Facility Code (FC) for all other Construction Mode User access.

Prerequisites:

- Schlage Control™ device should be fully installed with batteries connected and mechanically operational
- Schlage Control™ device must be new or recently set back to Factory Default Reset (FDR)

Actions:

- Present a credential with the desired Facility Code (FC) to be used for Construction User access
- The Schlage Control™ device will Beep once to acknowledge the credential presentation
- Present the original credential again
- Witness the Schlage Control™ device acknowledges the credential and enables the thumb turn for locking and unlocking

Results:

- All credentials with the same Facility Code (FC) will be allowed Construction Mode access.

Enabling Construction Mode (Schlage NDE or LE)

Schlage NDE and LE device Construction Mode enrollments are different than Schlage Control™. The Schlage NDE and LE devices will allow any normally valid credential to be used for Construction Mode access.

A valid credential is initially presented to the device to become the MASTER Construction credential, then the MASTER Construction credential is used to add additional USER Construction credentials.

Any number of USER credentials can be added for construction use; however, the MASTER credential is ONLY used to add new USER Construction credentials.

Each USER Construction credential is independently added before Construction access is provided.
Prerequisites:
- Schlage NDE or LE device should be fully installed with batteries connected and mechanically operational
- Schlage NDE or LE device must be new or recently set back to Factory Default Reset (FDR)

Actions:
- Turn and hold the inside lever
- Present a credential you want to use as a MASTER Construction Credential
- The device will blink 5 times for Successful MASTER Construction Credential enrollment
- Again, present the MASTER Credential
- The device LED will illuminate GREEN for 20 seconds waiting for a new User Construction credential to be presented
- Present another (new) credential to be enrolled as a User Construction credential, within 20 seconds
- The device will blink 5 times to indicate successful USER Construction credential enrollment
- Repeat the MASTER Construction credential presentation and User Construction credential enrollment process for each USER Construction credential that is needed
- NOTE: All USER Construction credentials enrolled will now be allowed Construction Mode access.

Results:
- All User Construction credentials added using the MASTER Construction credential will be allowed Construction Mode access.

WARNING: Be sure to store the MASTER Construction credential in a safe place. It will be required when additional User construction credentials are needed.
Enabling Construction Mode (Schlage CTE)

Schlage CTE device Construction Mode enrollments are different than Schlage Control™. The Schlage CTE and wall reader devices will allow any normally valid credential to be used for Construction Mode access.

Like Schlage NDE and LE a credential is initially presented to the reader to be enrolled as the MASTER Construction credential, then the MASTER Construction credential is used to add additional USER Construction credentials.

Any number of USER credentials can be added for construction use; however, the MASTER credential is ONLY used to add new USER Construction credentials.

Each USER Construction credential must be independently added to before Construction access is provided.

Prerequisites:
- The CTE and reader should be new from the factory or recently put back to Factory Default Reset (FDR)
- The CTE and reader should be fully installed
  - Proper power
  - Data lines properly connected
  - Reader is synced (paired) properly with the CTE
  - The opening locking device is properly installed and operational

Actions:
- Remove the CTE lid
- Press and hold the FDR button for 5 seconds and then release it
- The CTE MODE indicator LED is now illuminated ON for Construction Mode
- Within twenty seconds, present a credential you want to use as a MASTER Construction Credential to the wall mounted reader
- The CTE STATUS LED and the wall mounted reader LED will blink 5 times for successful MASTER Construction Credential enrollment
- Again, present the MASTER Credential
- The CTE STATUS LED and the wall mounted reader will illuminate GREEN for 20 seconds waiting for a new User Construction credential to be presented
- Present another (new) credential to become a User Construction credential, within 20 seconds
- The CTE STATUS LED and the wall mounted reader LED will blink 5 times to indicate successful USER Construction credential enrollment

- Repeat the MASTER Construction credential presentations and User Construction credential enrollment process for each additional USER Construction credential

- Properly install the CTE lid

Results:

- All User Construction credentials added using the MASTER Construction credential will be allowed Construction Mode access.

• WARNING: Be sure to store the MASTER Construction credential in a safe place. It will be required when additional User construction credentials are needed.
Configuration Cards

Configuration cards are special cards used for configuration and programming of Credential Readers. The Multi-Technology CTE MT11-485 and MT15-485 Wall Mounted Credential Readers will require Configuration Card programming to disable card technologies when desired.

Additionally, the MT20W, No-Tour Enrollment Reader will require a Configuration Card to perform Factory Default Reset (FDR).

When working with Schlage CTE Multi-Technology Readers (MT11-485, MT15-485)

To disable Proximity Credential technology, follow these steps:

- The MT11-485 or MT15-485 wall mounted Credential Readers must use a special Configuration Card to turn-off (disable) proximity card reads.

- The Configuration card to disable Proximity cards is CE-401-101

- Locate the correct Configuration Card

- To Disable Proximity Credentials - use the CE-401-101 Configuration Card, and follow these steps:

  1. Power cycle the Credential Reader
  2. Within the first 60 seconds from power up
  3. Present and hold the configuration card to the reader
  4. The reader will acknowledge the configuration card by beeping 3 times, the LED will flash red with each beep.
  5. When the beep and LED sequence is finished, the configuration update to ignore Proximity card presentations is complete.

- NOTE: Always re-sync Schlage CTE and Credential Reader after configuration card programming
  - To re-sync the Schlage CTE and reader
    - Press and release the Schlage button once
    - Then press and release the FDR button, twice.
  - The RS485 LEDs will be flashing when successfully sync’d

Results:

- The Credential Reader will no longer acknowledge any Proximity credential presentations
When working with the Schlage MT20W

- The Schlage MT20W must use a special Configuration Card for Factory Default Reset (FDR).

- The Configuration Card is provided with the Schlage MT20W, In-The-Box or a replacement card can be ordered separately. (CE-000-040).

- The Schlage MT20W should only need Factory Default Reset (FDR) when it is necessary to be moved to a new or different ENGAGE™ account.

To perform Factory Default Reset:

Prerequisites:

- Locate the CE-000-040 Configuration Card – In the Box

Actions:

- Power cycle the credential reader.
  - Wait a few seconds for the boot up process to complete.

- Within the first 60 seconds after power up.
  - Present and hold the configuration card to the reader.

Results:

- To indicate the successful completion of a Factory Default Reset (FDR), the Schlage MT20W will beep three times and the LED will be solid RED.
  - Be patient, the Schlage MT20W will reset and restart. This process will take a minute to complete before the solid RED LED is provided

NOTE:

1. FDR will not affect the current firmware of the Schlage MT20W.
2. FDR will de-commission and erase the Wi-Fi network settings of the Schlage MT20W.
3. FDR will not remove the Schlage MT20W from the ENGAGE™ property database.
No-Tour Features

Overview

The No-Tour feature allows the property administrator to program a 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 smart credential is presented for normal access.

The No-Tour feature is automatically enabled within the ENGAGE™ Web Application when a Schlage MT20W or Schlage Control™ device is commissioned into the ENGAGE™ Account.

ENGAGE™ 6.1 (and newer) WEB Application includes a door assignment counter that tracks and displays the current door assignments on each credential. 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 at one time.
- Each Individual door assignment information is stored in one of the 11 available credential sectors.
- A door assignment counter is displayed when assigning users to devices and includes new and prior programed settings.
- Multiple devices included in a defined ENGAGE™ “Group” will be stored in one (1) of the 11 available credential sectors.
- Access right changes are communicated at the door, when the programmed smart credential is presented to the lock.
- 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:
  - **Assigned** - Used, already assigned and the credential has been programmed
  - **Blocked** - Used, already assigned however access to this door is “DELETED”
  - **To be assigned** - Planned access assigned, however the credential is not yet programmed
  - **Free Space** - Unused, available for new access assignment
No-Tour Limitations

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

Please **BE ADVISED** of the following important No-Tour feature limitations:

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

  **WARNING:** The property administrator should sync all devices when removing or deleting user access, to ensure all doors the user had access to are updated. Ensuring all doors are up to date is most important when access is being deleted.

  **Be advised,** removed accesses using No-Tour requires the updated credential to be presented to the door. A door the user fails to visit using No-Tour programming after a credential replacement or an
access deletion, will still allow the old or lost credential access because the new lock access programming has not been performed.

- Credentials that have assigned door access deleted, will remain as “Blocked” assignments in the credential sector.
  
  NOTE: A blocked door will count in the maximum door programming limit of 11 doors per credential.

- When the User credential access expires per a defined User Schedule, the 11 credential sectors are freed-up and new access assignments can be programmed with a new expiration date.
  
  WARNING: Administrators must plan for their users to not require more than 11 unique door access or Group assignments when using No-Tour functionality.

- When door and Group assignments exceed 11, the administrator will not be able to use No-Tour programming. The property administrator will be required to manage access updates using the standard Sync process. All devices other than Schlage Control™, may enable nightly Wi-Fi updates to automate access updates.

**No-Tour Temporary Maintenance Access – Recommendations**

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

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

**NOTE:**

- User Schedules MUST first be saved in ENGAGE™ and then each device must be sync’d before the new schedule will be available at the door.

- User Activation / Expiration settings are programmed on the credential and will be immediately available when presented at the door.

Here is one example of a Maintenance Access setup:
- 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.

- Tour the property, perform nightly Wi-Fi updates, or commission new devices to save the new “Maintenance Shift” schedule into each device.

- Note: New or updated User Schedule will require syncing before the newly defined Maintenance Shift will be honored at the door.

![User Schedules](image)

**Maintenance Shift Schedule**

- When the sub-contractor needs maintenance access the property administrator will:
  - Program a credential with the contractor's name
  - Set 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 access or group assignments can be applied at one time using No-Tour.
Set expiration for today to limit access

- When the Maintenance Contractor access expires per its Expiration setting, the credential can be reused and reprogrammed with a new set of doors, a new expiration date, and a different USER name for credential reuse.
No-Tour Resident Moves-Out – Recommendations

When a resident moves-out, the property administrate 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 property administrator may choose to:
   a. Rename the old resident in the ENGAGE™ system with the new resident name.
   b. Hand the returned credential to the new resident.
   NOTE: The previous ENGAGE™ User Audit information will be maintained for history and any new accesses, resulting from this credential reuse, will be 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 on 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 then be available for use and reassignment as a new credential.
Initial Account Setup

There are two account types possible with ENGAGE™.

1. An ENGAGE™ Software Alliance Member account managed by one of our Software Alliance Members (SAM), or

2. An ENGAGE™ Managed account with the ENGAGE™ Web application

• NOTE: When choosing the account type for your property, consult with your local Allegion sales representative for further direction. An ENGAGE™ Software Alliance Member account managed by one of our Software Alliance Members (SAM) may provide additional system features not available with the free ENGAGE™ Web application.

Creating an ENGAGE™ Account

• Enter the URL https://portal.allegionengage.com/signin into your web browser.

![ENGAGE™ Sign In Form]

• Select Create Account

![ENGAGE™ Create Account Form]

• Enter the requested information
  - Email Address: must be unique and not used in any other ENGAGE Property
- **Password** and **Password confirmation**
- **First Name** and **Last Name**

- Select **I have read and accept the Terms and Conditions** “check box” to acknowledge
- Select **Sign Up**
- Acknowledge **Your account has been created** message

- Select **OK**

- To continue the process, sign on to your (property administrators) **email account** and OPEN the verification email sent to you from tickets@Allegionengage.uservoice.com

**Subject:** Verify Your Allegion ENGAGE Email

**From:** tickets@allegionengage.uservoice.com

**Verify Your Allegion ENGAGE Email**

Thank you for signing up. Please verify your email address by clicking the following link:

[Confirm my account](#)

If you have any issues with your account, please contact our technical support team at 877-671-7011.

Thanks,
The Allegion ENGAGE Team

**NOTES:**

- If no verification email arrives in your email
  - Check the SPAM and TRASH folders
  - Verify the original email address was entered correctly

- In addition to the Technical Services Support number provided in the message above (1-877-671-7011), you may also contact Technical Services Support at 1-800-847-1864 opt 3 for additional assistance.
• Click on the **Confirm my account** link in the email message (Above) to activate your account.

To continue the process:

• Log into your new ENGAGE™ Account using the new account Email and Password.

![ENgage Technology Sign In](image)

• Select **Sign In**

![ENgage Technology Create New Site](image)

• Select **Create New Site**
• Select the **Select Site Software** pull-down

  NOTE: The **ENGAGE** option is listed first, followed by alternate Software Alliance Members (SAM).

• In this case we will choose the **ENGAGE** Site Software.

  *Remember to consult with your Software Alliance Member (SAM) account manager before selecting any SAM Site Software*

• Enter the **Property (Site) Name**. We chose “YOUR PROPERTY”

• Select **Property (Site) Type** from the Pull-Down menu

  - **Education K-12**
  - **Education - Higher Education**
  - **Health Care**
  - **Commercial Office**
  - **Government/Public Building**
  - **Retail**
  - **Lodging/Hospitality**
  - **Food Service**
  - **Religious**
  - **Warehouse**
  - **Multi-Family residence**
  - **Other**

• Enter your local **Time Zone**

• Select the **Daylight Savings Time** (DST) setting (**ON/OFF**) based on your property’s Time Zone

  HINT: Default DST setting is **ON**. Setting DST to **OFF** will disable automatic device adjustments for DST

• Select **Save** to complete the initial account setup
Now that your account is setup and verified, you can now **Sign In** to your account and begin to manage your property.

**VERIFY SUCCESS:**

- Log into your new ENGAGE™ Web application account
- Enter **Email address** and **Password**
- Select **Sign In** to begin using your new **ENGAGE™ Managed account**

---

**NOTE:** If you selected a site software from a **Software Alliance Member (SAM)** Account, instead of the ENGAGE™ Managed account in the “Create New Site” screen shown above, only the following screen message will be displayed in the ENGAGE™ Web application:

> The devices in **YOUR PROPERTY** are being managed with software from one of our Alliance Partners.

Use the free ENGAGE™ mobile app to commission and configure devices in this site.

- Get the ENGAGE™ mobile app from the iTunes App Store (IOS)
- Get the ENGAGE™ mobile app from the Google Play Store (Android)
Account Team Members

Overview

Adding property Team Members will allow others to help the Administrator manage the property. Team members can be assigned Administrator, Manager or Operator roles to allow or limit specific capabilities. See Appendix A for a listing of ENGAGE™ features and capabilities available for each of the Team Member Roles.

Team Members assignments and changes can be managed in both ENGAGE™ Web and Mobile applications, however the ENGAGE™ Web application is preferred for ease of data entry.

Administrators:

- Administrators will have unrestricted access to create, modify and delete users, devices and to manage property and device settings.
- Administrators can invite other Administrators, Managers or Operators to the property.

Managers:

- Managers will have unrestricted access to create, modify and delete users, devices and manage property and device settings.
- Managers CANNOT invite new Administrators to the property.
- Managers can add new Operators to the property.

Operators:

- Operators will have the most restricted capability.
- Operators manage daily maintenance operations like syncing (Updating Door Files) and uploading Audits at the door into ENGAGE™.
- Operators may also perform some maintenance items like updating devices at the door with new firmware or new settings.
- Operators CANNOT invite other Administrators, Managers or Operators to the property.
Assigning Team Members

- Open the ENGAGE™ Web application
- Select the Advanced tab
- Select the My Team tab

Select Add Team Member button at the bottom of the screen and enter the details

First and Last Name
Email Address
Select the Team Members Role

HINT: You may hover over the symbol to see the Role definitions

Select Send Invitation
VERIFY SUCCESS

- The new Team Member is now listed in the My Team tab as Invited.

NOTE:

1. If a new Team member does not receive the Invitation email - check the SPAM / TRASH email folders and check that the email address was originally entered correctly
2. If the new team member does not open and verify their invite email before the expiration date listed in the screen above, the invitation is cancelled and property administrator must re-send the invite.
Verifying the Invitation Email Address (resend)

To verify the correct email address was entered and to re-send the invitation open the ENGAGE™ Web application to review the data entered.

- Select **Advanced** tab
- Select **My Team** tab
- Select the **Manage** button for the "Invited" Team Member

![Image of ENGAGE™ Web application]

- Verify the email address is correct for this Team Member

**Manage Invitees**

**Selected Invitee**

Account: someone@email.com  
Role: Manager  
Expiration Date: 2018-5-17

First Name: Team

Last Name: Member

- Select **Re-Send Invitation** to try again or **Delete Invitation** as desired
Schedules Overview

The administrator can define three types of Schedules with ENGAGE™. User Schedules, Door Schedules and Holiday Schedules. Each schedule type is described below:

Schedules are created within the ENGAGE™ Web application.

**BEST PRACTICE:** Property schedules should be defined before any device is commissioned into your account. This is the best practice because any schedules made or edited after a device is commissioned, will require device updates before the new or updated schedule is followed.

User Schedules

- User Schedules are defined to limit User access to specific times of day and days of the week.
  - Think of User Schedules as First Shift, Second Shift, etc.
- The default User Schedule assigned to every new user is 24/7 for access all the time.
- A maximum of 16 User Schedules can be defined for your property.

**WARNING:** When assigning User Schedules for the Schlage Control™ deadbolt locks, property administrators should be aware that Users exiting a room will not be able to relock a Schlage Control™ deadbolt lock when outside (after) their scheduled access time.

Device Schedules

- Device Schedules can be defined to schedule automatic lock/unlock operations at a door.
- A maximum of 16 Device Schedules is available for your property.
  - Think of Device Schedules as Open Hours, Lock up Time, etc.
  - Be advised, a device unlocking schedule and a device locking schedule will require two device schedule assignments to be defined.

**NOTE:** Schlage Control™ devices do not support Device Schedules.

Holiday Schedules

- Holiday Schedules can be used to specify the Start and Stop times of a holiday
- The desired State of the lock during the holiday is defined (Locked/Unlocked)
- User access during a Holiday Schedule can be also specified:
  - Restricted Access – PASS THROUGH credential function access ONLY
  - Locked – Valid credential presentation is required for access
  - Unlocked - No credential required, passage access is provided
- A maximum of 32 Holiday Schedules is available for your property.
  - Holidays can be defined to span multiple days when necessary

**NOTE:** Schlage Control™ devices do not support Holiday Schedule
Creating Device and User Schedules

The administrator can define up to 16 Device Schedules and 16 User Schedules for the property. Steps for entering both Device and User Schedules are described below.

- Log into the ENGAGE™ Web application
  - For Device Schedules, select DEVICE then SCHEDULES tab
  - For User Schedules, select USERS then SCHEDULES tab

- Select the Add New Event Schedule or the Add New User Schedule button at the top right of the screen

- Enter Schedule NAME, START TIME and END TIME
  
  Note: For Device Schedules, also enter the desired ACTION to be taken at the schedule Start and End times
Device Schedule:

User Schedule:

- Select the **Scheduled Days** of the week for the schedule to be active
- Select **Save**

**VERIFY SUCCESS**

- See the momentary **Device (or User) Schedule added successfully** message
  
  ![Schedule added successfully.]

- See the new schedules are now listed on the User and Device Schedules Screens.
Schedules
There is a maximum of 16 Device Events (8 scheduled pairs) provided by ENGAGE. If additional schedules or custom functionality is needed, please contact one of our Software Alliance Partners.

Office Hours
Exercise Room

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.

24/7 (default)
8-to-5 User Schedule
Maintenance Schedule

NEXT STEPS:

- The above process merely defines the User and Device Schedules to be used for the ENGAGE™ managed property.
- Each schedule will now be selectable for assignment to individual User(s) or Device(s) when performing those assignments.
  - See Assigning Lock Access and User Schedules for assignment of a User Schedules for a resident.
  - See Property Wide Default Device Settings and Adjusting individual Device Settings for assignment of Device Schedules to a door.
Creating Holiday Schedules

The administrator can define up to 32 Holidays for the property. Steps for entering Property Holidays are described below. A Holiday can be defined to span multiple days, as needed.

- Log into the ENGAGE™ Web application
- Select Devices and then Holiday tab

- Select Add New Holiday at the top right of the screen

- Enter Schedule NAME, START and END time

- Select Save
VERIFY SUCCESS

- See the momentary **Holiday added successfully.** message
- See the new “Memorial Day” Schedule listed on the Holiday Schedule Screen

NEXT STEPS:

- The above process merely defines the Holiday Schedules to be used for the ENGAGE™ managed property.
- Each schedule will now be selectable for assignment to individual Door(s) when performing those assignments.
  - See **Property Wide Default Device Settings**
  - See **Adjusting individual Device Settings** while assigning Door Schedules to an individual door.

WARNING: A new or edited Holiday Schedule must be synced with each assigned device using the ENGAGE™ Mobile application or via nightly call-in for Wi-Fi enabled devices, before the Holiday Schedule is active.
Property Wide Default Device Settings

When devices are commissioned into ENGAGE™, the Default device settings will be loaded in each device. Property administrators should think through their property needs and requirements before commissioning any devices. Each device that is commissioned will be programmed with the defined default settings as defined in ENGAGE™ Web application.

HINT: Property administrators who review each device type and confirm the associated default settings before commissioning will save time while setting up their property.

Device settings may be edited and updated at any time, however, setting up the device defaults before commissioning will provide for a better, less error prone installation and setup.

To view/edit Device Defaults

- Log into the ENGAGE™ Web application
- Select Advanced

- Then select Device Defaults tab

NOTE: The Schlage Control™ deadbolt default settings are presented initially. Select the Schlage CTE, LE, and NDE tabs on the left of the screen to view and set the Device Defaults for the other device types.

- Schlage Control™ smart locks Default Settings:
- **Beeper Enabled** - Slide to control the device beeper setting ON/OFF

- **Relock Delay** – Used to set the time the deadbolt thumb turn is engaged for locking and unlocking, after a valid credential is presented
  
  - Default Relock Delay is 3 seconds
  
  - Defines how long the deadbolt thumb turn will be engaged for locking and unlocking by the User

- Review and adjust any settings to define the DEFAULT settings to be used for all Schlage Control™ deadbolts on your property.

- Select **Save**
Schlage CTE Default Settings:

- **Relock Delay** – Used to modify the time the device is unlocked after a valid credential is presented
  - Default Relock Delay is 3 seconds
- **ADA Relock Delay** – Extended time for relocking of a device for residents with the ADA USER setting enabled.
  - Default ADA relock setting is 30 seconds
- **Propped Door Delay Enabled** – Slide control to turn ON/OFF
- **Propped Door Delay** – Record Propped Door Audit after a specified time
  - Default Propped Door Audit is 20 seconds
- **Anti-Tailgate** – Slide control to turn ON/OFF

- Review and adjust any settings to define the DEFAULT settings to be used for all Schlage Control™ deadbolts on your property.
- **Select Save**
LE Default Settings:

- **Beeper Enabled** – Slide to control the device beeper setting ON/OFF
- **Relock Delay** – Used to modify the time the device is unlocked after a valid credential is presented
  - Default Relock Delay is 3 seconds
- **ADA Relock Delay** – Extended time for relocking of a device for residents with the ADA USER setting enabled.
  - Default ADA relock setting is 30 seconds
- **Propped Door Delay** – Report and record Propped Door Audit after a specified time.
  - Default Propped Door Audit is 20 seconds
- **Power Fail Mode** – This setting defines what the lock should do when entering Critical Battery Mode.
  - Default Power Fail Mode is Lock the Door (Secure)
  - Passage (UNLOCKED) and AS IS (no change) are also options

NOTE: Use the scroll down bar on the right to reveal the additional Blink Interior LED Default Settings
LE Default Settings: (continued)

- **Blink Interior LED** – Slide to control the Blink Interior LED setting ON/OFF
  - Enables blinking of the Inside LED when door is secure (slow blinks)
- **Blink Internal LED Rapidly** – Slide to control the Blink Interior LED Rapidly setting ON/OFF
  - Enables fast inside LED blinks when door is in “Privacy Secure” mode
  - Initiated by the Inside Push Button (IPB) or deadbolt thumb turn

- Review and adjust any settings to define the DEFAULT settings to be used for all Schlage LE devices on your property.
- Select **Save**
Schlage NDE Default Settings:

- **Beeper Enabled** - Slide to control the device beeper setting ON/OFF
- **Relock Delay** – Used to modify the time the device is unlocked after a valid credential is presented
  - Default Relock Delay is 3 seconds
- **ADA Relock Delay** – Extended time for relocking of a device for residents with the ADA USER setting enabled.
  - Default ADA relock setting is 30 seconds
- **Propped Door Delay** - Record Propped Door Audit after a specified time
  - Default Propped Door Audit is 20 seconds
- **Power Fail Mode** – This setting defines what the lock should do when entering Critical Battery Mode.
  - Default Power Fail Mode is Lock the Door (Secure)
  - Passage (UNLOCKED) and AS-IS (no change) are also available options

- Review and adjust any settings to define the DEFAULT settings to be used for all Schlage NDE devices on your property.
- Select **Save**
Reader Default Settings:

Property administrators should think through their property needs and requirements before commissioning any devices. Each device that is commissioned will be programmed with the defined default settings as defined in ENGAGE™ Web application.

HINT: Property administrators who review each device type and confirm the associated default settings before commissioning will save time while setting up their property.

Default reader settings may be edited and updated at any time, however, setting up the device defaults before commissioning will provide for a better, less error prone installation and setup.

BEST PRACTICE:

1. Determine if your property will require both Proximity and Smart card credentials.
   - For best reader response and improved battery life, it is recommended to disable any credential technology that is not needed.
2. Normal Reader sensitivity is recommended for most properties.
   - Reader sensitivity may be set to HIGH or MAX when small format FOB credentials are in use
3. WARNING: Both HIGH and MAX reader sensitivity settings will reduce device battery life.

- Log into the ENGAGE™ Web application
- Select Advanced
- Then select Reader Defaults tab
• Review and adjust any settings to define the DEFAULT reader settings to be used for all devices on your property.

• Select Save
Adjusting individual Device Settings

When a device is commissioned, the defined Default Device Settings will be programmed into the device. Subsequently, a property administrator may wish to adjust specific device settings to be unique for a particular opening, situation, or feature.

To adjust individual device settings, follow these steps:

- Log into the ENGAGE™ Web application
- Select the Devices tab
- Select the device to update. In this case we chose the Copy Room

NOTE: Devices MUST be commissioned before they will be available, for additional device setting updates. See Device Commissioning to enroll a new device.

• Select the EDIT symbol to continue to the lock setting screen(s)
NOTE: Schlage Control™ has limited adjustments, while Schlage NDE/LE devices have additional adjustment options. See the separate Schlage Control™, Schlage NDE, and Schlage LE device settings screens below.
Schlage LE Lock Settings Tab

NOTE: The Blink Interior LED options are not available on locks with the Storeroom function setting. Locks commissioned as Privacy, Office and Apartment functions will have these options available.

Schlage NDE and LE Reader Settings Tab
• Make all necessary adjustments per your administrator and property needs
• Select **Save**

**VERIFY SUCCESS**
• See the momentary **Device updated.** message

---

**NEXT STEP(s):**

This process merely sets the programming intentions for each device. After assigning device settings, the administrator will be required to perform the following steps before the door settings will be honored.

• Sync all effected devices.
  • Schlage NDE, LE or CTE device syncing is available via overnight Wi-Fi network call-In
  • See [Sync - Updating a Door File](#)
  • See [Sync – Overnight – Schlage NDE, LE, and CTE](#)

**WARNING:** Device Settings are never programmed into any device when using the No-Tour update feature. Device sync is required when performing any device setting update.
Device Commissioning

Overview

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

IMPORTANT NOTES:

- All devices are commissioned using the ENGAGE™ Mobile application using Bluetooth communication. Device commissioning is never performed with the ENGAGE™ Web application.

- The device must be “Out-Of-The-Box” or recently Factory Default Reset (FDR) to be available for selection and commissioning.

- If a device has already been commissioned into another ENGAGE™ account, it MUST be deleted from the previous account and Factory Default Reset (FDR) before it can be reused and commissioned into a different account.

- Devices must be properly commissioned before they can be added to a Device Group.

BEST PRACTICE:

- Property administrators should define all Schedules, all Default Device Settings before commissioning locking devices.
  
  o All default Device Settings and defined Schedules are initially programmed into each locking device when it is commissioned. If a device setting, schedule is added or updated, a sync will be required for every device that is affected and was previously commissioned before an update was performed.
Schlage MT20W Commissioning

- Ensure the Schlage MT20W is powered and has completed its boot-up process.
  - The Schlage MT20W LED will be solid RED when ready.

- Log into the ENGAGE™ Mobile application to view the Devices Screen
  - One of the following screen shots will be presented.

NOTE: Android and iOS devices will have slightly different screens, however the functions are the same.

![iOS Device Menu](image1)

OR

![Android Device Menu](image2)

NOTE: No devices show as commissioned into the property account yet. Each device in the system MUST be commissioned before they will be available on the All Devices screen(s). The Schlage MT20W is our first device to be commissioned into our property.

- The next step is to select the nearby Schlage MT20W to be commissioned.
  - For iOS mobile devices
    - On the screen above, select the + sign in the upper right-hand corner
  - For Android mobile devices
    - On the screen above, select the + sign in the lower right-hand corner

- Select the device category that you want to commission. In this case select the MT20W device type in the “Select a device type” screen below, to continue.
• You will 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.

• In this case we chose **Schlage Reader** serial number **C20000000000010B** by tapping on that specific Schlage Reader in the screen shown below.

NOTE: New or recently Factory Default Reset Schlage MT20Ws will be displayed.
• Ensure the Schlage MT20W is in signal range of the local Wi-Fi network access point.

• Select Next
  • Confirm the Schlage MT20W Credential Reader selected for Commissioning.
    o The Blue LED should be flashing slowly to indicate it has been selected.

• Select YES
  • Next the property administrator will select the local Wi-Fi network for the device. There will be one of two options available.
1. When there are no saved Wi-Fi networks, a new network MUST be added.
2. When a *Saved Network* is available, the property administrator may select that Wi-Fi network for quick and accurate data entry.

*WARNING:* A Saved Network MUST be locally available at the location where the device is being installed and commissioned. Be sure a saved Wi-Fi network is present and locally available before selection.

- Initial the property administrator MUST select **Add a new network** to enter the Wi-Fi network Security Settings. See the section below when **Selecting a Saved Network**.
• Enter the **Wi-Fi SSID**.
  - This is the name of the local wireless local area network
  - This entry must be EXACT and is CASE SENSITIVE

• Select the **Wi-Fi Security** used by the local area wireless network
  - OPEN, WPA2, WPA2 (PEAP), or WEP

NOTE: Depending on the Wi-Fi network security chosen, you may need to enter different information. Those items highlighted in the screen below (not grayed out) will be required.

In this case we chose **Wi-Fi SSID 610baLWLAN** and the **WPA2 (PEAP)** network security protocol. Both a **Username** and **Password** are required.
• After entering all required information, Select **Next**

NOTE: The Wi-Fi network settings will now be programmed into the Schlage MT20W and the Schlage MT20W will connect to the local Wi-Fi network using the entered network settings. Wait a few moments until the Schlage 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 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.**

  HINT: 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.

- **Select the Press if Solid Blue (Connected) Blue bar to continue.**

  ![MT20W device screen with verification message]

- Acknowledge the “Setup Complete” message
- Select Exit

**VERIFY SUCCESS**

- 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.
• The Schlage MT20W LED will illuminate solid BLUE after power is applied and boot-up is completed indicating successful connection to the local Wi-Fi Network.

NOTES:
  o The Schlage MT20W solid BLUE “Connected” LED display indicates the Schlage MT20W is connected to the local wireless Wi-Fi network and operating properly.
  o The Schlage MT20W will flash BLUE quickly while trying to connect with the local Wi-Fi network.
  o When the local Wi-Fi network connection fails, the Schlage MT20W will display a solid RED LED.
  o When the local Wi-Fi network is not available (failed or down for maintenance), the Schlage MT20W will automatically retry to reconnect to the local Wi-Fi network every few minutes.

Selecting a Saved Network
• Instead of selecting “Add a new network”, the property administrator may select the appropriate (locally available) Wi-Fi SSID in the displayed list of Saved Networks. In this case only one Saved Network has been saved and made available for selection, **610baLWLAN**.
• **Select the Saved Network:** 610aLWLAN.

NOTE: The Schlage MT20W will reset and then try to connect to the local Wi-Fi network using the saved network settings. Be patient, wait a few moments while the Schlage MT20W tries to connect to the local Wi-Fi (fast Blue LED blinking) and then provides a solid Blue LED indicating it has successfully connected to the local Wi-Fi network.

• **Select the Press here on Solid Blue bar to continue**
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 correct or the local Wi-Fi network is not present.

- **Recheck or reenter the Wi-Fi network settings and Try Again.**

  HINT: You can also verify the local network security settings by using your mobile phone to enter the network settings and temporarily connect with your phone. When successful, the local Wi-Fi network connection requirements are verified and can be re-entered as a saved network.

- **Acknowledge the Setup Complete message and Select Exit**
Schlage Control™ smart lock Commissioning

- Log into the ENGAGE™ Mobile application while nearby the Schlage Control™ smart lock to be commissioned.
- Apply power to the Schlage Control™ smart lock (install batteries)

**IMPORTANT NOTES:**

1. The Schlage Control™ smart lock must be “Out-Of-The-Box” or recently Factory Default Reset (FDR) to be available for commissioning and selection for commissioning.
2. The Schlage Control™ smart lock must have the deadbolt RETRACTED during commissioning to allow for Bluetooth communications (Advertise)

- Log into the ENGAGE™ Mobile application to view the Devices Screen. Depending on your mobile device, one of the following screen shots will be presented.

  NOTE: Android and iOS devices will have slightly different screens, however the functions are the same.

  ![iOS Device Menu](image1)
  ![Android Device Menu](image2)

  **NOTE:** This display shows that no devices are commissioned into the property yet. Each device in the system MUST be commissioned before they will be shown on the All Devices screen(s).

- The next step is to select the nearby Schlage Control™ smart lock to be commissioned.
- For iOS mobile devices
  o On the screen above, select the + sign in the upper right-hand corner
- For Android mobile devices
  o On the screen above, select the + sign in the lower right-hand corner

- Select the device type that you want to commission. In this case select the Control Lock type in the “Select a device type” screen below, to continue.

- The next screen will be displayed only once per property, once for each property administrator, and once for each product type. This is your reminder to think about and use the predefined Sitewide Default Device Settings before setting up a bunch of devices.

- Answer the question: “Do you want to use the “currently defined” default Control Lock settings for this property?”

NOTE:
1. Property administrators can use the currently defined default settings for this device or elect to independently modify the settings “for this device” when necessary.
2. The property manager may modify individual device settings using the “Customize Settings” option also provided below.
• **Select** “Use Default Settings” to continue, using the previously defined Schlage Control™ smart lock default settings

• **Select** the specific Schlage Control™ smart lock to be commissioned from the list of new or recently Factory Default Reset (FDR) devices provided

**NOTE:**
1. All nearby Schlage Control™ smart locks with RETRACTED deadbolt and available for commissioning will be displayed.
2. Device serial number can be found on the sticker on the front of the Schlage Control™ smart lock or on the inside plate.
3. When multiple Schlage Control™ smart locks are presented, select the appropriate device by serial number, or just pick one and go to the next step to identify the selected device.
• Select the desired Schlage Control™ smart lock for commissioning. In this case we selected the **Schlage Lock** with serial number **E10000000001B846**

• Verify that the selected device LED is flashing RED.

• Select **YES** to continue.

• Enter the **Lock Name** for this Lock. In this case we entered “**Storage Room**”.
- Select **Next**

- View the Schlage Control™ device commissioned successfully **Check Mark** message

- Select **Finish** to complete the commission process or, select “**Add another Control device**” to continue enrolling additional Schlage Control™ devices.
VERIFY SUCCESS

- The newly commissioned Schlage Control™ device is now shown in the ENGAGE Mobile application “All Devices” screen and the “In Range” screen, when nearby the device.
Schlage NDE Commissioning

- Log into the ENGAGE™ Mobile application while near the Schlage NDE device to be commissioned.
- Apply power to the Schlage NDE device (install batteries)
  
  NOTE: The device must be “Out-Of-The-Box” or recently Factory Default Reset (FDR) to be available for commissioning and selection for commissioning

- Log into the ENGAGE™ Mobile application to view the Devices Screen. Depending on your mobile device, one of the following screen shots will be presented.

  NOTE: Android and iOS devices will have slightly different screens, however the functions are the same.

  ![iOS Device Menu](image) ![Android Device Menu](image)

  NOTE: This display shows that no devices are commissioned into the property yet. Your display may be different, this screen will display each device you have already commissioned into the property.

- The next step is to select the nearby Schlage NDE device to be commissioned.
  - For iOS mobile devices
    - On the screen above, select the + sign in the upper right-hand corner
  - For Android mobile devices
    - On the screen above, select the + sign in the lower right-hand corner
• Select the device type that you want to commission. In this case select the Schlage NDE Device Type in the “Select a device type” screen below, to continue.

![Select a device type](image)

• The next screen will be displayed only once per property, once for each property administrator, and once for each product type as a reminder to think about and use the predefined Sitewide Default Device Settings.

• Answer the question: “Do you want to use default Schlage NDE Lock settings for this site?”

**NOTE:**
1. Property administrators can use the currently defined default settings for this device or elect to independently modify the settings “for this device” when necessary.
2. The property manager may modify individual device settings using the “Customize Settings” option also provided below.
- **Select** “Use Default Settings” to continue, using the pre-defined Schlage NDE device default settings.

- **Turn and Release the inside Schlage NDE lever** to cause the Schlage NDE to “Advertise” its presence with its Bluetooth (BLE) radio

  **WARNING:** The Schlage NDE will “Advertise” for two (2) minutes to allow selection in this Commissioning step. If the Schlage NDE is not listed, turn the inside lever again and refresh the screen to try to connect again.
NOTE: If no device information is displayed:
1. Be sure the Schlage NDE battery cover is properly installed. Schlage NDE will not “Advertise” when the battery cover is not fully installed properly
2. Be sure the Schlage NDE is Out-Of-The-Box or recently Factory Default Reset
3. Be sure the mobile device is in Bluetooth communication (BLE) range of the Schlage NDE
4. You may need to select Cancel to return to the “Select a device type” selection screen and Try Again

- Select **Next**

- **Select** the specific Schlage NDE device to be commissioned from the list of new or recently Factory Default Reset (FDR) devices provided. In this case only one nearby Schlage NDE is available.

  NOTE: Only the Schlage NDE with a recent inside lever turn will be displayed

- Select the desired device for commissioning. **Schlage Lock 00000000A0000532**

- Verify that the selected Schlage NDE device LED is flashing RED.
- Select YES, after verifying the LED blinks
- Enter the Lock Name for this Schlage NDE. In this case we chose “Main Office”.

- Select NEXT

NOTE: The Schlage NDE requires the Door Position Sensor (magnet) calibration so that the Schlage NDE “Knows” when the door is physically CLOSED.
**WARNING:** The next step requires the door to be physically closed with the Door Position Sensor (DPS) magnet(s) properly installed into the door frame.

Note: Door Position calibration is accomplished and recorded by the Schlage NDE immediately after **Next** is selected in the screen above.

**WARNING:** If the door was not actually closed during this step, a false reading will be stored for the Door Position reading and the door position will not be reported accurately. Door Position magnet calibration may be repeated using the mobile application at any time after commissioning is completed.

- Ensure the Door is physically closed and then select **NEXT**
NOTE:
- The NEXT step in the commissioning process will ENABLE the Wi-Fi network connection capabilities of the Schlage NDE lock.
- Administrators may also elect to skip setup of the WI-FI network when a network is not available or not needed by selecting Skip in the screen above.
- The property administrator may ENABLE or edit a Wi-Fi network connection setting at any time using the mobile application.

- For now, let’s assume that the local Wi-Fi network has not been setup yet and there are no Wi-Fi network connections available. Select Skip

Note: See Enabling WI-Fi Network Connection Settings for setup requirements when a Wi-Fi network is available and the property administrator would like to take advantage of the Schlage NDE “Nightly Call in” feature.
• Select **Finish** to complete the commission process or, select **“Add another NDE device”** to continue enrolling NDE devices.

**VERIFY SUCCESS**

- The Schlage NDE lock is shown in the ENGAGE™ Mobile application Devices screen with its new name.
Schlage LE Commissioning

- Apply power to the Schlage LE wireless mortise lock (install batteries)

  NOTE: The Schlage LE must be “Out-Of-The-Box” or recently Factory Default Reset (FDR) to be available for commissioning and selection for commissioning

- Log into the ENGAGE™ Mobile application to view the Devices Screen. Depending on your mobile device, one of the following screen shots will be presented.

  NOTE: Android and iOS devices will have slightly different screens, however the functions are the same.

![iOS Device Menu](image1)

![Android Device Menu](image2)

  NOTE: This display shows that no devices are commissioned into the property. Your display may be different, with each device you have already commissioned into the property displayed here.

- The next step is to select the Schlage LE device to be commissioned.
  - For iOS mobile devices
    - On the screen above, select the + sign in the upper right-hand corner
  - For Android mobile devices
    - On the screen above, select the + sign in the lower right-hand corner

  SELECT the Schlage LE Device Type in the “Select a device type” screen below, to continue.
• As a property administrator reminder, the next screen will be displayed: only once per property, once for each property administrator, and once for each product type. This screen is intended to remind the property administrator to think about and use the predefined Sitewide Default Device Settings.

• Answer the question: “Do you want to use default Schlage LE Lock settings for this site?”

NOTE:
1. Property administrators should use the currently defined default settings for this device.
2. The property manager may also modify individual device settings using the “Customize Settings” option also provided below.

• Select “Use Default Settings” to continue, using the pre-defined Schlage LE device default settings.
• **Turn and Release the inside Schlage LE lever** to cause the Schlage LE to “Advertise” its presence with its Bluetooth (BLE) radio

  **WARNING:** The Schlage LE will “Advertise” for two minutes to allow selection in this Commissioning step. If the Schlage LE is not listed, turn the inside lever again and refresh the screen to try to connect again.
NOTE: If no device information is displayed:

- Be sure the Schlage LE battery cover is properly installed.
  - LE will not “Advertise” when the battery cover is not fully installed properly

- Be sure the Schlage LE is Out-Of-The-Box or recently Factory Default Reset
  - In FDR mode the Schlage LE will Beep with each inside lever turn and begin two (2) minutes of advertising for the commissioning process

- Be sure the mobile device has Bluetooth turned ON

- Is the Schlage LE in range for Bluetooth communication (BLE) with the Mobile device

- Select **Back** to return to the “Select a device type” selection screen and **Try Again**
- Select **Next**

As a property administrator reminder, the next screen will be displayed: only one time per property, one time for each property administrator, and one time for each product type. This screen is intended to remind the property administrator to think about and use the predefined **Sitewide Default Device Settings**.

- Answer the question: “**Do you want to use default LE Lock settings for this site?**”

NOTE:
1. Property administrators can use the currently defined default settings for this device.
2. The property manager may also modify individual device settings using the “Customize Settings” option also provided below.

   - **Select** “Use Default Settings” to continue, using the pre-defined Schlage LE device default settings.

   ![Image of app with options]

NOTE: View the specific Schlage LE device to be commissioned from the list of new or recently Factory Default Reset (FDR) devices
provided. In this case only one nearby Schlage LE is available. Only Schlage LE devices with recent inside lever turn (within two minutes) will be displayed

- **Select** the desired device for commissioning. In this case we chose, **Schlage Lock LE** serial number **F10000000F1232EF**

![Image of a device with an option to select Yes or No](image1)

- **Select** **Yes**, after verifying the Schlage LE lock LED is flashing

![Image of device with a prompt to give the device a name](image2)

- **Enter a Name** for the Device. In this case we chose **Storage**
• **Select** the desired **Lock function** from the list provided. In this case we chose **Storeroom**.

NOTE: Each possible Schlage LE lock function is available for selection. When selected the definition of the function is also provided for quick reference. See the additional screen shots below for the lock function descriptions.

**WARNING**: Each of the **Apartment**, **Office**, and **Privacy** Schlage LE lock functions will require the Inside Push Button (IPB) or deadbolt thumb turn to be available for proper operation. Also, the LEMS product (LE Mortise without deadbolt) is available with the Storeroom function ONLY.
The NEXT step in the commissioning process will ENABLE the Wi-Fi network connection capabilities of the Schlage LE lock. Administrators may also elect to skip setup of the WI-FI network when a Wi-Fi network is not available or not needed by selecting Skip in the screen above.

NOTE: The property administrator may ENABLE or edit a Wi-Fi network connection setting at any time using the mobile application.

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

NOTE: See Enabling Wi-Fi Network Connection Settings for setup requirements when a Wi-Fi network is available and the property administrator would like to take advantage of the Schlage LE “Nightly Call in” feature.
• Select **Finish**

**VERIFY SUCCESS**

• The Schlage LE lock is shown in the ENGAGE™ Mobile application “In Range” screen with its new name
Schlage CTE Commissioning

- Apply power (+12Vdc or +24Vdc) to the components and ensure credential reader and locking device are properly powered and connected.

NOTES:
1. The CTE and credential reader must be “Out-Of-The-Box” or recently Factory Default Reset (FDR) to be available for commissioning and selection for commissioning.
2. The credential reader must be properly connected and sync’d with the CTE
3. The CTE Mode LED will indicate FDR when in FDR mode and ready to commission.

- Log into the ENGAGE™ Mobile application to view the All Devices Screen.

NOTE: Android and iOS devices will have slightly different screens, however the functions are the same. Depending on your mobile device, one of the following screen shots will be presented.

NOTE: This display shows that no devices have been commissioned into the property yet. Your display may be different, and display each device you have already commissioned into the property displayed.

- The next step is to select the nearby Schlage LE device to be commissioned.
  - For iOS mobile devices
    - On the screen above, select the + sign in the upper right-hand corner
- For Android mobile devices
  - On the screen above, select the + sign in the lower right-hand corner

- **SELECT** the CTE Device Type in the “Select a device type” screen below, to continue.

As a property administrator reminder, the next screen will be displayed: only once per property, once for each property administrator, and once for each product type. This screen is intended to remind the property administrator to think about and use the predefined **Sitewide Default Device Settings**.

- Answer the question: “**Do you want to use default CTE settings for this site?**”

  **NOTE:**
  1. Property administrators should use the currently defined default settings for this device.
  2. The property manager may also modify individual device settings using the “Customize Settings” option also provided below.

- **Select** “Use Default Settings” to continue, using the pre-defined CTE device default settings.
• Follow the Pop up message instruction to enable Bluetooth “Advertising” for the desired CTE device. Press and release the Schlage button inside the CTE enclosure.

**WARNING:** The CTE will “Advertise” for two minutes to allow selection in the next Commissioning step. If the “Advertising” timeout occurs, repeat this step again — Press and release the Schlage button to try again.

• **Select Next**
• Select the CTE to be commissioned from the list

NOTE: If no device is displayed check for the following conditions
  o Be sure the CTE is Out-Of-The-Box or recently Factory Default Reset (FDR)
    - The FDR Mode LED must be ON
  o Be sure you are in wireless Bluetooth communication (BLE) range of the CTE
  o Be sure the CTE is “Advertising” via Bluetooth (BLE)
  o Select BACK to return to the Device Type selection screen and Try Again

• Answer the following question to verify the CTE being commissioned.
• Select Yes

then
- Enter a **Name** for the CTE (required). In this case we chose **Main Entrance**
- Select **Next**
- Now move through these screens to choose the locking device and any auxiliary equipment that this CTE will be required to control
Select the desired **Wi-Fi network connection** setup. In this case we chose **Skip**.

- Select **Skip** to use the CTE without a Wi-Fi connection or to setup the Wi-Fi network, later.
  - If you intend to take advantage of the CTE Wi-Fi nightly call-in network capabilities, see **Sync – Overnight – Schlage NDE, LE, and CTE**.
  - Wi-Fi settings can be updated after this initial setup is completed by connecting to the device and enabling the Wi-Fi settings.

- Select a displayed **Saved Wi-Fi Network**, if the Wi-Fi is locally available at the door opening. In this case there are two previously saved Wi-Fi networks available.

- Select **Add a new network**, initially or when no Saved Wi-Fi networks are not available locally at the door.
Select **Finish** to complete the CTE initial setup and return to the **Connect** screen.

**VERIFY SUCCESS**

- See the new CTE door **Main Entrance** is now listed and available.

**NOTE(S):**
- If you are a No-Tour property, it is recommended that unnecessary and unused proximity technology credential types be disabled.
• Disabling the proximity technology credentials will provide for improved battery life and quicker reader and access response. The device will not search for the unused credential technology (Proximity) each time a credential is presented. The device will no longer “look” for proximity cards when a credential is presented.

• To disable Proximity credentials on a CTE Credential Reader (MT11 or MT15), a “Configuration Card” part number CE-401-101 – Disable All Proximity Card Technologies - is required.
Creating Users

Overview

Creating Users 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 and is shown here.

NOTE: Default settings for User Activation/Expiration dates start “Today” and will automatically expire in 5 years.

- Open the ENGAGE™ Web application
- Select Users tab

- Select the Add User button at the bottom of the Users tab

- Enter User details.
  - First and Last Name (required). In this case we will enter New User
  - Email (optional)
• Enable **ADA** (American Disabilities Act) operation if the resident requires additional time to access doors.

**IMPORTANT NOTES:**
- ADA operation does not apply to Schlage Control™ devices.
  - HINT: When modified access timing is needed for a Schlage Control™ deadbolt, adjust the standard Relock Delay settings accordingly
- When the ADA setting is moved to ON, this ADA USER will be allowed modified access times at the Schlage NDE, LE, and CTE doors they are assigned.
- Each door has a default ADA Relock Time setting for ADA USERS. This ADA Relock time setting can be changed on a per door basis.
- Sync is required to update new or edited ADA Relock settings into a commissioned device
- Default ADA setting is 30 seconds

• Set the **Activation** and **Expiration** times for this user.

**NOTE:** Default Activation and Expiration settings provide for Activation to begin TODAY and Expiration to automatically to occur in five (5) years.

• Select **Save**

**VERIFY SUCCESS**

• See the **User added** momentary confirmation

• The new User (NEW USER) is now listed on the **Users** tab
NEXT STEPS:

- This process merely enrolls a User into ENGAGE™ to make them available for credential and Access Assignments, later.
- The administrator will still be required to Assign Credentials and Add New Access and User Schedules for this user
- Then Sync all devices or perform No-Tour credential programming to complete device programming
Enrolling Credentials

Overview

Enrolling credentials can be accomplished by three methods depending on the property administrator’s needs. Property administrators who use the No-Tour feature(s) must use Smart Card credentials and the MT20W Credential Reader for credential enrollments. Alternative credential enrollment options are available for property administrators that desire Proximity card use.

**BEST PRACTICE:** It is strongly advised that one credential is assigned to one user. Users should rarely need to have more than one credential assigned at one time.

1. **Smart** credential enrollments are provided using the ENGAGE™ Web application and the MT20W. This is the required credential enrollment method for No-Tour feature compatibility.
   
   a. Using the MT20W, credentials may be enrolled one at a time, or in bulk. Credentials are made available in the ENGAGE™ Web application **Select Existing Credentials** folder for assignment to a resident.

   **NOTE:** Administrators who use bulk enrollments, will need to physically control and manage the enrolled credentials so they are readily available when needed for User assignments. The Ink Stamp number on the credential will be displayed in ENGAGE™ Web application for easy reference.

2. **Proximity** credential enrollments are provided using ENGAGE™ Web application and an Schlage MT20 credential reader.

3. Or, credential enrollments can be made at a door using the ENGAGE™ Mobile application and a commissioned ENGAGE™ device as the credential enrollment reader. (Schlage NDE, LE, CTE or Schlage Control™)

   a. Since Schlage NDE, LE, and CTE devices will enroll multi-tech credentials, be sure to disable the card technology that is not needed in the device before enrolling a multi-tech (COMBO) credential. In this manner you are guaranteed to enroll the desired card technology and format. Note: Schlage Control™ devices will always enroll Smart credentials.

   b. This method of credential enrollment is NOT RECOMMENDED because the system does not provide the Ink Stamp reference and the credential cannot be searched for in the ENGAGE™ Web application (Badge Search)
Enrolling credentials individually (ENGAGE™ Web application)

- Log into the ENGAGE™ Web application
  - Ensure the MT20W is properly powered and commissioned. The LED will be solid BLUE when connected to the local Wi-Fi network and ready for use.

- Select USERS then USERS tab

- Select any User to assign a credential
  NOTE: You must add a new User if the user is not already entered. In this case we selected Existing User

- Select the Add Credential button (above)
- Select the Select Existing Credential tab (below)
• Present the new credential to the MT20W and wait a few seconds. The MT20W will turn GREEN and beep once when the card is accepted and enrolled in the **Select Existing Credential** tab. This process usually only takes a few seconds.

Note: In this case credential # 5998 was just added (see below)

• Select the **Refresh List** button (above) to view the newly updated credential list.

• Confirm the physical "Ink Stamp" on the credential matches the newly added credential.

• Select the newly added credential to highlight it for assignment to the user. In this case we choose credential #5998.
- Select the desired Credential Function using the Pull-Down menu (Default is Normal)

Note: The possible credential functions are shown below. Please see Appendix C for more credential function definition.

- Select Save to assign the credential to the selected User
VERIFIED SUCCESS

- See the **Credential Assigned** momentary confirmation

  Credential Assigned.

- See that the newly added credential (# 5998) is now listed under Credentials for the selected user.
Enrolling credentials in Bulk (Schlage MT20W only)

It is an easy process to enroll multiple credentials into ENGAGE™ Web application all at the same time (in bulk) and have them available for quick User assignments later.

- To begin, ensure the Schlage MT20W has been previously commissioned.
  
  **NOTE:**
  - There is no need for the ENGAGE™ Web application to be running or to have the Schlage MT20W connected to a computer.
  - USB power and a valid Wi-Fi network connection are all that is required.
  - Proper Wi-Fi communication is indicated by a solid BLUE LED on the MT20W.

- Plug your commissioned Schlage MT20W into any USB power source and verify proper Wi-Fi network connection.
  
  **NOTE:** Wait a few seconds after power application while the MT20W starts up (boots). When ready and connected to the local Wi-Fi network, the MT20W LED will be solid Blue indicating a good Wi-Fi connection.

- Present a new smart credential to the MT20W and wait a few seconds. The MT20W will turn GREEN and beep when the card is accepted. In this case we presented credential # 1335.

- Continue to present additional new cards (REPEAT) until all credentials have been successfully enrolled with a GREEN LED and beep. In this case we’ve added credentials #18740, #1965 and #5715.

  **NOTE:** Keep these enrolled credentials is a safe place so they are readily available when needed for credential function definition and assignment to a resident

**VERIFY SUCCESS**

- Log into the ENGAGE™ Web application

- Select the **USER** Menu and **Users** tab and then pick any predefined User from the list
• Select **Add Credential**

• View the newly added credentials are now available in the **Select Existing Credential** tab.

Note: All credentials enrolled will be listed and referenced by their “Ink Stamp” number. If an expected credential is not shown, you may want to select the **Refresh List** button to view credentials that have been added very recently.

• Select **Cancel** to quit viewing available credentials without assigning a credential to the selected User
Assigning Credentials at a door

It is also possible to enroll a credential using the ENGAGE™ Mobile application and an installed lock.

1. This credential assignment method allows the property administrator additional flexibility for quick credential enrollment and assignment; however, this method is NOT recommended because some functionality normally available in ENGAGE will not be available – for any credential enrolled using this assignment at the door method.

WARNING: Credentials assigned using the ENGAGE™ Mobile application and commissioned ENGAGE™ device method (here) will not have the typical credential # (ink stamp) listed as seen with Schlage MT20W enrolled credentials. Also, credentials enrolled with this method will not be searchable in the ENGAGE™ database because there is no credential ink stamp # available.

- Log into the ENGAGE™ Mobile application.
- Locate a nearby and already commissioned ENGAGE™ device to use as an enrollment reader.

Note: If using multi-tech credentials and devices with multi-tech credential capabilities (Schlage NDE, LE, or CTE) as your credential enrollment reader, property administrators should disable the card technology that is not wanted before attempting credential enrollments.

- Select the USERS menu then and the specific user to be assigned a new credential.

NOTE: In this case we chose NEW USER to be assigned a new credential.
• **Select** the user to be assigned a credential.

![User Information Screen]

- **First Name**: New
- **Last Name**: User

**USER INFORMATION**

![User Configuration Screen]

- **Activation**: 06/26/2018
- **Expiration**: 06/26/2023

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

- **ADA Enabled**: Off

**CREDENTIALS**

- Devices
- Users
- My Team
- Sites
- More

• **Select the **Credentials** Menu (shows no credentials assigned)**

![Credentials Screen]

- Devices
- Users
- My Team
- Sites
- More

• **Select the + sign to identify devices in-range to 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.**
• **Select** an "Available Enrollment Device" from the nearby device list. In this case we chose the **Storage**.

  NOTE: After selection the selected device LED will be flashing RED.

• Present the new credential to the nearby **Storage** device.
NOTE: When the device reads the credential, the ENGAGE™ Mobile application will display a credential "Value" with asterisks ********.

If no credential is presented, the process will "Time Out" after 20 seconds so the device can return to its normal use - securing an opening.

- Select **Save**

**VERIFY SUCCESS**

- See the **Credential Enrolled successfully** message

**Credential Enrolled Successfully!**

- Select **OK**

**VERIFY SUCCESS**

- Log into the ENGAGE™ Web application
- Select the **USER** Menu and **Users** tab and then pick the **NEW USER**
- View the current credentials assignments for **NEW USER** and credential assignment.
WARNING: Credentials assigned using the ENGAGE™ Mobile application and commissioned ENGAGE™ device method (described here) will not have the typical credential # (ink stamp) listed as seen with MT20W enrolled credentials. See the 1802 example below.

Also, credentials enrolled with this method will not be searchable in the ENGAGE™ database because there is no credential ink stamp # available.
Creating Device Groups

Overview

Device Groups are available for the property administrator to manage any number of doors with common user access. Openings assigned into a Group will be treated as a single assignment when programming the user credential and will require only one credential sector for access to all doors defined in the Group.

IMPORTANT NOTES:

- Devices must be commissioned before they are available for inclusion into a Device Group.
- Device Groups should be very static and not require updates frequently.
  - Any updates to a Device Group will require Sync of each affected device before the group update will be valid.
- Property administrators should define any Device Groups before making user access assignments for streamlined access assignment.
- A device may be included in ONLY one Device Group.
  - Device assignment into multiple Device Groups is not allowed.

▪ Open the ENGAGE™ Web application

▪ Select DEVICES tab and then the DEVICE GROUPS menu

▪ You will see this initial screen
- Select **Add New Group**

![Add New Device Group Window]

- **Enter a descriptive Group name.** A Device Group name is required. For this example, we will enter:
  - **Pool Access for Residents**

- **Enter a description** of the Group so that others can easily recognize the Group purpose. For this example, we will enter:
  - **Only the pool access and restroom doors for residents. Does not include pool storage or maintenance rooms.**

- Select **Save**
VERIFY SUCCESS

- See the momentary “Device Group added successfully” message and the Device Group is now listed with its description.

NOTE: A Device Group is successfully defined, however, there are no devices included in this group. The next step is to assign the property doors that you want in the newly defined Pool Access for Residents Device Group.

- Select the + sign to begin device selection(s) for this Device Group. The full list of all available devices will be provided.
NOTE: A device that is already assigned into another Device Group will not be available here for selection.

- Select the Unassigned Devices you would like to be included in this Device Group. In this case we will select **Pool 142** and **Pool 286**
  
  - Include a device: Select the device name and the > to move it into the “Assigned Devices” field.
  
  - Exclude a device: Select the device name and the < to move it back into the “Unassigned Devices” field.
  
  - Select all devices: Select the >> or << symbols to move all listed devices.

IMPORTANT NOTES:

- Initially, all commissioned and unassigned devices will be displayed in the “Unassigned Devices” field and will be available for selection.

- Devices already assigned to another Device Group will not be listed for selection here.

![Assign devices to group](image)

- Select **Save**

VERIFY SUCCESS

- See the momentary “**Device Group updated successfully**” message and the Pool Access for Residents Device Group is now listed it’s two assigned devices.
NEXT STEPS:

- A device Sync with the ENGAGE™ mobile application must be performed at each device that is added or deleted from a newly defined Device group.
  - Any User credentials programmed for this group will not allow access until a device Sync is successfully completed.
  - Any device (door) deleted from a Device Group will allow access until a device Sync is successfully completed to remove that door from the Device Group.

NOTE: NDE, LE and CTE devices that are connected to the local Wi-Fi network will be updated with newly defined Device Group settings during the next successful daily Wi-Fi update.

- This newly defined Device Group (with the two defined door assignments) will now be available when programming User access.
Assigning Lock Access and User Schedules

Overview

Assigning lock access rights 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 and is shown here

NOTE: Successful access assignments requires the User to be properly enrolled with a smart credential already assigned, the lock(s) commissioned in the account with all desired User Schedules defined. Additionally, any Door Groups should also be defined prior to assigning the first resident with access rights.

- Open the ENGAGE™ Web application.
- Select USERS tab.
- Select the User named “New User”.

**WARNING:** If the User has no Credentials Assigned, lock access assignments will not be possible. The User MUST have at least one smart credential assignment be assigned No-Tour access.
- Select the orange **Assign Access** button at the bottom of the screen (above) to begin assignment of doors/locks/openings for this Resident.

![Access](image)

**Access**

<table>
<thead>
<tr>
<th>Name</th>
<th>Expiration</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apt 502B</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Apt 8845</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Garage 141B</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Laundry 137</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Lobby 83</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Pool 142</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Pool 286</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Storage</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
<tr>
<td>Store Room</td>
<td>06/26/2023</td>
<td>24/7 (default)</td>
</tr>
</tbody>
</table>

**NOTE:** The individual “**Device**” selection screen is automatically selected by default. The “**Groups**” button is provided for when selecting predefined Device Groups.

- Check the “Box” by each defined individual lock where access is desired.
  - In this case we will choose Apt 5D2B, Garage 141B, Laundry 137, Lobby 83, and Storage.

  **NOTICE:** The **Credential Sector Usage** screen will fill up as access assignments are made. There is an 11-door assignment limitation per credential for No-Tour programming that cannot be exceeded.

- Select the **Schedule** pull-down to select defined User Schedules when default 24/7 access is not desired.

- Adjust the pre-defined **Expiration** access date now, if desired.

**Note:**

1. Expiration date is automatically entered as five years after the User is defined in the system. Property Administrators may adjust the Expiration date **on a per lock basis** at any time.

2. Credential programming is required before No-Tour updates will be honored at the door.
• **Select Save** to record your individual Resident access selections

You will be returned to the following screen

• **Select** the “**Groups**” button at the top of the screen to view and select any currently defined Device Group.

![Access Screen](image)

- Check the “Box” by each defined **Device Group** where access is desired.
  - In this case we will choose “Pool access for Residents”. Which has **Pool 286** and **Pool 142** pre-defined into the group.

**NOTICE:** The **Credential Sector Usage** screen will fill up as access assignments are made.

**NOTE:** A Device Group will only take up one sector even though each defined Device Group may contain any number of doors. There is an 11-door assignment limitation per credential for No-Tour programming that cannot be exceeded.

• **Select Save** to record your **Device Group** access selections
VERIFY SUCCESS

- View the momentary "Lock Access Updated" success message is presented.

- The new user now has assigned access to the five (5) individual door assignments and the two (2) door assignments from the assigned Device Group. See the new "Current Access" screen for the selected “New User” with seven (7) assigned doors.

![Image of Engage™ software interface showing a new user with assigned access rights.](image)

NEXT STEPS:

- This process merely assigns a User access rights to individual doors in ENGAGE™. The administrator will still be required to perform credential programming for No-Tour updates and/or sync before updates will be honored at the door.

- The property administrator must now obtain the identified smart credential and program the newly assigned access rights to it.
  - In this case we need smart credential # 22904 to proceed.

- Select **Update** in the Credentials screen above with the smart credential in hand.
- Follow the instruction provided on screen, then Select **Next**

- Select **Finish** in the screen above.
• Notice that the **Update** option is no longer presented in the **Credentials** screen.
  
  - This is your indication that the credential has the latest access assignments properly programmed.
Sync – Updating a Door File

Overview

Update devices with Sync using the ENGAGE™ Mobile application to communicate the latest ENGAGE™ system settings, and programmed access rights. Additionally, syncing a device will also capture and return the latest device Audits for review.

The administrator will know that the device has updates pending when the orange “Update ICON” is presented next to the device name. See below, the Copy Room and the Main Office both have pending updates, indicated by the orange exclamation point ICON.

**IMPORTANT NOTES:**

- Device Sync mobile updates at the door use the mobile device Wi-Fi (or data) network for an internet connection and communication with ENGAGE™.
- Mobile devices use Bluetooth (BLE) for communication to the nearby device(s).
- The Mobile device MUST stay in Bluetooth range until the update process is completed for reliable Bluetooth communication. Device Sync only takes a few seconds.
- Door Settings and Device or User Schedule updates MUST be accomplished using a Device Sync update or using nightly Wi-Fi call-in when available.
- No-Tour credential programming of a device will not update device settings or any type of schedules.

BEST PRACTICE: Turn OFF the lock local Wi-Fi network connection when coverage is spotty. Perform local Sync updates using your mobile device data connection for more reliable communication with ENGAGE™.

Performing Sync:
• Open the ENGAGE™ Mobile application and go to the **Devices** screen
• A list of all in-range devices will be displayed.

  **NOTE:** Those devices with updates pending will have the familiar ⬤ update pending indicator.

  ![Device List](image)

• **Select** the device to be updated. (Pool 142)
• Select Sync to begin the update process

NOTE: The selected device will begin flashing the RED LED when connected and during the sync communication.

VERIFY SUCCESS

• Notice the Success Sync Successful message at the bottom of the screen
• Test and check updated User Accesses are honored or denied appropriately
• Verify new lock operations and door settings (relock delay, accepted credential types, schedules, etc.) are honored

Using the ENGAGE™ Mobile application:

• Open the ENGAGE™ Mobile application.
• Select the Devices Menu
• Verify that the Update pending device ICON is removed for Pool 142 lock.
Sync – Overnight – Schlage NDE, LE, and CTE

Overview:

When the Schlage NDE, LE, and CTE device Wi-Fi network settings are entered properly and the device can connect with the local Wi-Fi network, the device will automatically sync and perform “Nightly Updates” to Update Door Files and to Get Audits.

Additionally, using the ENGAGE™ Web application, Schlage NDE, LE, and CTE devices may be scheduled for Firmware updates to be performed overnight. See Schlage NDE, LE, and CTE Scheduled Firmware Updates.

NOTE: Sync and firmware updates for Schlage Control™ devices must always be performed “At the Door” using the ENGAGE™ Mobile application. Schlage Control™ does not support Wi-Fi communication.

Enable nightly Wi-Fi updates (Sync)

To enable nightly sync (Door File and Get Audit updates) for an Schlage NDE, LE or CTE devices, all that is needed is to properly configure the device Wi-Fi network settings for the local Wi-Fi network.

- Open the ENGAGE™ Mobile application and select Devices to find the nearby Schlage NDE, LE, and CTE devices.
- Select a device to enable its Wi-Fi network connection

NOTE: We chose Storage, a Schlage LE device in this example

- Select the More... option
• Scroll down the screen to reveal the **Settings** menu at the bottom.

• Select **Settings**
• Select the **Wi-Fi** menu (under **GENERAL**)

![](image1)

• Slide the Wi-Fi button to enable and display the Wi-Fi setup menu

![](image2)

**NOTE:** The **Save Network** button is enabled by default. When this is enabled, each saved Wi-Fi network Security setting will be automatically stored by the mobile device and will be made available for menu selection (easier setup) of new Wi-Fi enabled devices.
To select a “Saved Network”, see Select a previously saved Wi-Fi network below.

- **Select** the Wi-Fi Security method to be used with your property
- **Enter** the required Wi-Fi configuration settings.
  - In this case we chose **WPA2(PEAP)** Wi-Fi Security and our **610baLWLAN** Wi-Fi SSID
  - Passwords and/or Usernames may be required, based on the Security method selected
- **Select** **Save** in the top right-hand corner of the Wi-Fi screen

**VERIFY SUCCESS**

- See that the new Wi-Fi SSID (**610baLWLAN**) is now listed on the Device, then **More** Screen.

• Select the **Wi-Fi menu**
NOTE: This example is for WPA2(PEAP) security. Username and Password will be unique for your Wi-Fi network security

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

- Select **Test Wi-Fi** to initiate the test

  NOTE: The device LED will be flashing AMBER while testing the Wi-Fi network connection
• Acknowledge the Success message

NOTES:
1. The selected device now has its Wi-Fi network connection verified and it will call in to Sync, every night to apply any assignment updates and to retrieve device audits.
2. This device can now be enabled for automated firmware updates and nightly call-in updates.
3. Device audits will now report Wi-Fi information like connection strength and connection issues for the property administrator.
4. Should the Wi-Fi test fail, you will see this message.

WARNING: If the Wi-Fi network connection fails, recheck your Wi-Fi network SSID and Security settings, then try again.

HINT: You can also check the local Wi-Fi network settings by using your mobile phone to connect to the Wi-Fi network while nearby the device.
• To select a previously saved Wi-Fi network

Wi-Fi network settings are automatically saved by the mobile device each time a unique Wi-Fi SSID is entered and saved. To select a saved Wi-Fi network, follow these steps:

WARNING:
- A saved Wi-Fi network may not be accessible at your current location and if not available, that saved network should not be selected. Be sure to select a saved Wi-Fi network that is local and available at the installed device location.
- Verify the saved connection using the available Test Wi-Fi Connection option(s).
- If not successful, verify the Wi-Fi settings using your mobile device and try again.

• Select Show Saved Network menu (below)

![Show Saved Network Menu](image)

NOTE: In this case the mobile device is showing two different Wi-Fi networks to choose from (below). Sfwifip and 610baLWLAN Wi-Fi networks have been previously saved and are available for automatic selection.

• Pick a saved (local) Wi-Fi network from the list provided. In this case we chose the 610baLWLAN Saved Network

WARNINGS:
1. Ensure you pick the saved Wi-Fi network that is local to the device being set up and in range for good communication.
2. A saved network may not be locally available at the installed device physical location.
3. Network settings can be saved from different Wi-Fi access points across your property.
4. Network names (SSID) may even vary within the same building. Your local IT administrator should be consulted.

NOTE: This example is for WPA2(PEAP) security. Username and Passwords will be unique for your Wi-Fi network security

- Select **Save** in the top right-hand corner of the screen
VERIFY SUCCESS

- See that the new Wi-Fi SSID (610baLWLAN) is now listed on the Devices Screen.
- Select the Wi-Fi menu

NOTE: This example is for WPA2(PEAP) security. Username and Passwords will be unique for your Wi-Fi network security

- Select Test Wi-Fi Connection menu
- Select **Test Wi-Fi** to initiate the test

  NOTE: The device LED will be flashing AMBER while testing the Wi-Fi network connection

- Acknowledge the **Success** message

  NOTE: The selected device now has its Wi-Fi network connection verified and it will call in every night to sync and apply any **Door File** updates and to **Get Audits**. Additionally, this device can be enabled for automated firmware updates as well.

- Should the Wi-Fi test fail, you will see this message.
WARNING: If the Wi-Fi network connection fails, recheck your Wi-Fi network SSID and Security settings, then try again.

HINT: You can also check the local Wi-Fi network settings by using your mobile phone to connect to the Wi-Fi network while nearby the device.
ENGAGE™ Product Family Hardware Installation

When working with Schlage® MT20W

Before you begin, review the product information provided in the box along with the product. A Schlage MT20W Enrollment Reader User Guide and the Factory Reset Default Configuration Card are provided.

Installation:

No hardware installation is required for Schlage MT20W, just plug the USB connector into your computer USB port or any USB power cube.

NOTE: The Schlage MT20W never communicates directly with the computer when connected via the USB cable connection. All communication is performed wirelessly via the local Wi-Fi network and the ENGAGE™ Web application. The Schlage MT20W merely uses the USB connection for power.

Initial Power up:

Whenever a new Schlage MT20W or a recently reset Schlage MT20W is powered up, it will go through a boot-up process. Wait a few seconds for the boot-up process to complete. The Schlage MT20W will beep, and the LED will be solid RED, waiting for the next step of commissioning.

Factory Default Reset (FDR):

To reset the Schlage MT20W you must use the CE-000-040 Configuration Card that was provided in the box.

The reset process is very simple, just present the Configuration Card within the 1st minute after power is applied and after the Schlage MT20W boot up process has completed.

IMPORTANT NOTES:

- To indicate the successful completion of a Factory Default Reset (FDR), the Schlage MT20W will beep three times and the LED will be solid RED.
- FDR will not affect the current firmware of the Schlage MT20W.
- FDR will de-commission and erase the Wi-Fi network settings of the Schlage MT20W.
When working with Schlage Control™ smart locks

Before you begin, review the installation instruction for the Schlage Control™ lock contained in the box along with the product. Schlage Control™ Deadbolt and Interconnected Lever Lock versions are available.

In addition, review the online Schlage Control™ deadbolt installation video available here and see Appendix B.
• NOTE: Out-of-the-box, the Schlage Control™ smart lock provides a label on the face of the lock with a bar code and the device serial number listed.

• Do not remove this label until the device is commissioned.

• You may want to record the lock serial number and the intended (or installed) location for use by the property administrator when commissioning and entering data into ENGAGE™.

Prepare for Installation

Gather your tools needed for lock installation. A Phillips screwdriver and a tape measure are all the tools you should need.

WARNING: DO NOT USE A POWER DRILL for installation. Hand tool use ONLY is recommended to prevent product damage.

Verify the door is properly prepared for the Schlage Control™ installation before attempting to install the deadbolt. You will need to verify the door thickness, the lock backset, proper hole
dimensions and for interconnected units (FE410), verify the bore to bore dimension of 4" or 5 ½".

NOTE: The Center Lines of the drilled holes and proper alignment is very important for proper deadbolt and/or latch retraction.

Installation

Install the Schlage Control™ smart lock as indicated in installation instruction. You will want to pay special attention to these items for best results.

Ensure

- The deadbolt is ALWAYS retracted during installation. If the deadbolt is not retracted during installation, the handing of the door and the electronic operation of the deadbolt will be reversed.

- The through door cable is routed from the exterior side OVER the top of the latch body and through the door.
2 Install the outside assembly.

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

- The CAM is in the correct position during installation. The CAM will be contacting the switch above when in the correct vertical position.

3 Install the inside assembly.

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

- 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, connector damage is possible.
• When working with INTERCONNECTED units (FE410) pay attention that the "Handing Plate" and "Handing Screw" are installed properly and the lever catch is in the correct orientation to allow proper lever installation (Handing)

Verify Installation success

• The thumb turn should move the deadbolt in and out of the closed door and frame, smoothly with no restrictions.

• The outside thumb turn should spin freely until a valid credential is presented.
• Interconnected Schlage Control™ devices will smoothly retract the deadbolt whenever the inside lever is used with no restrictions.

• Upon Power-up the Schlage Control™ device will boot up and flash the GREEN LED and beep three times indicating it is ready for Commissioning or Construction Mode operation.

CONSTRUCTION Mode

Things to know

• The first valid credential presented to the Schlage Control™ smart lock will automatically set the "Facility Code" for all Construction cards to be used at the door. Any credential with the SAME Facility Code will be granted access.

  NOTE: Construction Mode for other products (Schlage NDE, LE, and CTE) will use a Master Construction Credential and a separate Access Construction Credential enrollment process.

• Construction mode is available Out-Of-The-box or after a successful Factory Default Reset (FDR)

• Construction mode operation provides NORMAL Credential function. Valid credentials will allow the user to momentarily rotate the thumb turn to retract or extend the deadbolt.

• Construction mode can be canceled by Commissioning the lock or by performing a Factory Default Reset (FDR).
  
  o All previously valid Construction Credentials will no longer function at the door after Commissioning or Factory Default Reset.

  o CAUTION: The Schlage Control™ lock will accept the first card presented after FDR and use the Facility Code of that card to again allow Construction Access, if the device is not immediately commissioned and programmed.

  NOTE: No User Audits are stored in Construction Mode because the lock does not track time or credential numbers, yet

Creating a Normal Construction Credential

After successful hardware installation, present a valid credential to the lock to set the Facility Code for all construction credentials to be used at the door. The lock will beep to acknowledge the credential enrollment.

Verify Construction Mode operation by presenting the original credential and any other credential with the same Facility Code to gain momentarily engage the thumb turn for locking and unlocking access to the door.
Factory Default Reset (FDR)

Things to Know

- FDR will return the Schlage Control™ smart lock to its original Settings as shipped from the factory.
- FDR will remove any non-default device settings, delete any construction or user credentials and again allow commissioning or construction mode.
- FDR does not have any effect on the firmware currently on the lock.
- FDR will NOT remove the lock from your ENGAGE™ account. To re-enroll a Schlage Control™ into another, ENGAGE™ account, you must first delete the lock from the original ENGAGE™ account.

Performing a FDR

- Remove the battery cover and one battery for at least ten (10) seconds.
- With the deadbolt retracted, re-install the battery to apply power to the lock.
- Wait a few seconds for the lock to boot up after power is applied. During boot up the lock will provide one long GREEN Flash, five short GREEN flashes and indicates successful Boot up completion with three short GREEN blinks and beeps.
- Within 10 seconds of completing the boot up process, toggle the inside thumb turn (tail piece) two times to complete the FDR process. The lock will acknowledge successful FDR completion with one long GREEN flash and beep.

VERIFY SUCCESS

- The lock will now "Advertise" via Bluetooth and can been seen in the In Range screen when commissioning with an ENGAGE™ Mobile application.
- The Schlage Control™ device can now be re-programmed into Construction Mode.
When working with Schlage® NDE wireless cylindrical locks

Before you begin, review the installation instructions for the Schlage NDE lock contained in the box along with the product.

In addition, review the online Schlage NDE installation video available here and see Appendix B.

Prepare for Installation

Gather your tools needed for lock installation. A Phillips screwdriver, pin wrench, a tape measure and a T-15 Torx screwdriver (optional) are all the tools you should need.

**WARNING:** **DO NOT USE A POWER DRILL** for lock installation. Hand tool use ONLY is recommended to prevent product damage.

Verify the door is properly prepared for the Schlage NDE installation before attempting to install.

**NOTE:** The Schlage NDE and the mechanical ND locksets use the SAME door preparation template.
Verify these **critical items** before attempting to install the Schlage NDE.

- Through door hole **backset** = 2 3/4 or 2 3/8 inches
- Through door hole **diameter** = 2 1/8 inches
- The two 5/16 inch through door bolt holes are drilled and located properly
- Latch Bore hole = 1.0 inch and the hole is centered in the door

**WARNING**: The **Center Line** of the **Latch Bore** Hole and **Center Line** of the though **Door Bore** MUST be accurate for proper latch retraction.

**Installation**

- Install the Schlage NDE as indicated in the installation instruction.
- You may want to record the lock serial number and the intended (or installed) location for use by the property administrator when commissioning and entering data into **ENGAGE™**.
Pay special attention to these items for best results:

- Cable routings are done properly with no pinching and both cable connections are properly seated in the proper channels. See the picture below:

WARNING: Pay extra attention to the cable routing when the Door Thickness Adjustment setting is changed from the default setting 1 ¾”
- The installed latch and chassis is properly aligned and fully engaged

**WARNING:**
- The latch prongs MUST fully engage the top and bottom chassis slides.
  - See the properly assembled, blue chassis slide and orange latch prongs above
- The installed latch MUST be centered in the chassis and door
• The Door Position Sensor magnet tray or T-strike magnet must be installed properly.

WARNING:

○ You MUST use the strike and magnets provided in the box for the Door Position Sensing to be effective.

○ T-strikes are needed ONLY for Schlage LE devices with a deadbolt latch. (LEMD)

NOTE: When the T-Strike and standard Door Position Sensor (DPS) is used, additional door prep will be required to install the magnetic switch and wiring.

VERIFY SUCCESS:

• Once the Schlage NDE is properly installed, the inside lever should smoothly retract the latch with no restrictions and hold the door securely in the door frame.

• Upon Power-up the lock will perform a Power-On-Self-Test (POST). A few seconds after power is applied the Schlage NDE will indicate successful POST

• Three GREEN flashes and 3 beeps are provided to indicate - ready for Commissioning or Construction Mode operation.
CONSTRUCTION Mode

Things to know

- Construction Mode is provided like the Schlage LE and CTE products. Schlage NDE requires a MASTER Construction Credential that is used to add additional Access Constructions Credentials to each installed Schlage NDE.

- Construction mode is available Out-Of-The-Box or after a successful Factory Default Reset (FDR)

  NOTE: Master Construction Credentials for Schlage NDE do not provide access through the door. Schlage NDE Master Construction Credentials can only add other construction credentials to the lock that will gain access.

- Construction mode operation provides NORMAL Credential function, and the Schlage NDE will always automatically relock after momentary access is granted.

- Construction Mode must be canceled by performing Factory Default Reset (FDR). After an FDR, all previously valid Construction Credentials will no longer be valid.

  NOTE: No User Audits are stored in Construction Mode because the Schlage NDE does not track time or credential numbers, when in construction mode.

  WARNING: If the Master Construction Credential is lost or destroyed no additional construction credentials can be added. The Schlage NDE will require FDR and all construction credentials will need to be re-enrolled into the Schlage NDE using a new Master Construction Credential.

Create a Master Construction Credential

- Start with a new Schlage NDE or one just after a Factory Default Reset has been successfully performed. Turn and HOLD the inside lever (Request to Exit) then present a new credential to become the property Master Construction Credential.

- The Schlage NDE will acknowledge the credential presentation with 5 GREEN flashes and enroll the credential as the Master Credential.

VERIFY SUCCESS

- Present the newly added Master Construction Credential to the lock. The Schlage NDE LED will light GREEN for 20 seconds waiting for another credential to be presented for enrollment as a Construction Access Credential.
Create a **Construction Access Credential**

- To enroll a construction credentials that will allow access, present the previously enrolled Master Construction Credential. While the Schlage NDE LED is solid GREEN, present the credential intended to become a Construction Access Credential.
- The lock will beep after successfully enrolling the presented credential.
- Repeat the Master Credential presentation followed by a new Construction Access Credential process for each Construction Access Credential that will be needed.

**VERIFY SUCCESS**

- Present the newly added Construction Access Credential(s) and verify momentary access is granted.

**Factory Default Reset (FDR)**

**Things to Know**

- FDR will return the Schlage NDE to its original settings as shipped from the factory.
- FDR will remove any non-default device settings, delete any construction or user credentials, and, allow construction mode to be entered again.
- FDR does not have any effect on the firmware currently on the Schlage NDE.

**NOTE:** FDR will NOT remove the Schlage NDE from your ENGAGE™ account. To re-enroll a Schlage NDE into another ENGAGE™ account, you must first delete the Schlage NDE from the original ENGAGE™ account.

**Perform a FDR**

- Remove the Schlage NDE battery cover and Press and HOLD the FDR button for 5 seconds. The Schlage NDE will beep and blink two (2) times.

- Then turn the inside lever three (3) times within 20 seconds.
  - The Schlage NDE will blink RED and beep on each lever turn and then provide two GREEN flashes and beeps to indicate success.
VERIFY SUCCESS

- The Schlage NDE will now "Advertise" via Bluetooth communication and can been seen in the CONNECT screen as available for commissioning with an ENGAGE™ Mobile application.

  NOTE: Bluetooth communication requires the battery cover to also be properly installed.

- A new Master Construction Credential can be created.
When working with Schlage® LE wireless mortise locks

Before you begin, review the installation instructions for the Schlage LE lock contained in the box along with the product. In addition, review the online Schlage LE installation video here and see Appendix B.

- You may want to record the Schlage LE serial number and the intended (or installed) location for use by the property administrator when commissioning and entering data into ENGAGE™

Prepare for installation

- Gather your tools needed for installation. Phillips screw drivers (#1, #2), needle nose pliers and a tape measure are all the tools you should need.

  **WARNING:** **DO NOT USE A POWER DRILL** for lock installation. Hand tool use ONLY is recommended to prevent product damage.

- Verify the door is properly prepared for the Schlage LE installation before attempting to install the lock. You will need to verify the Door thickness, the Mortise pocket size and mounting hole locations specified in the installation instruction.

  **WARNING:** The mortise pocket is deeper due to additional wire clearance requirements. It is RECOMMENDED that you dry fit the Mortise chassis into the pocket to verify final fit and wire clearance.

- LE locks with a deadbolt (LEMD) MUST have additional door prep for a Door-Position-Sensor (DPS) to add a magnet and route its wires into the mortise pocket. Special attention is needed here to ensure proper Door Position Sensor magnet and wire installation.
Installation

Install the Schlage LE as indicated in installation instruction. You will want to pay special attention to these items for best results.

ENSURE

- The Mortise 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.

- The Spring Cage Arrow direction is mounted properly with the arrows pointing in the lever down direction.
• The latch is in the correct direction with the latch bevel towards the door opening.

• The RX module switch and Handing Screw is on the SECURE side of the mortise chassis (inside).
Verify Installation success

- Once the Schlage LE is properly installed, the inside lever will move the latch in and out of the door and frame, smoothly without resistance.

- If the Schlage LE is a deadbolt version (LEMD) the thumb turn and deadbolt also move in and out of the door and frame, smoothly without restrictions.

- The door closes properly and the lever handing is correctly installed.

- Upon power-up the lock will perform a Power-On-Self-Test (POST). A few seconds after power is applied, the Schlage LE will indicate successful POST with five GREEN flashes and beeps indicating it is ready for Commissioning or Construction Mode operation.

Operation in CONSTRUCTION Mode
Things to know

- Construction Mode is provided like the Schlage NDE and CTE products. Schlage LE requires a MASTER Construction Credential that is used to add additional Access Constructions Credentials to each installed Schlage LE.

- Construction mode feature is available out of the box or after a successful Factory Default Reset. (FDR)

- Construction mode operation provides NORMAL Credential function and the lock will always automatically relock after momentary access is granted.

- Master Construction Credentials do not provide Access through the door. Master Construction Credentials can only add other construction credentials intended to gain momentary access.

- Construction Mode can be canceled by performing Factory Default Reset (FDR). After an FDR, all previously valid Construction Credentials will no longer be valid.

  NOTE: No User Audits are stored in Construction Mode because the lock does not track time or credential numbers, yet.

- If the Master Credential is lost or destroyed no additional construction credentials can be added to the lock. The lock will require FDR and all construction credentials will need to be re-enrolled into the lock.

Create a Master Construction Credential

- Start with a new Schlage LE or one just after a Factory Default Reset (FDR) has been successfully performed. Turn and hold the inside lever Request-to-Exit (RTE) and present a new credential to become the property Master Construction Credential.

- The Schlage LE will acknowledge the credential presentation with 5 GREEN flashes and enroll the credential as the Master Construction Credential.

VERIFY SUCCESS

- Present the newly added Master Construction Credential to the lock

- The lock LED will light GREEN for 20 seconds waiting for a credential to be presented for enrollment as a Construction Access Credential in the lock.

- The next credential presented will be enrolled as a Construction Access Credential and be allowed momentary access to the lock when presented again.

Create Construction Access Credentials

- To enroll a construction credentials that will allow access, present the previously enrolled Master Construction credential. While the Schlage LE LED is solid GREEN, present the credential intended to become a Construction Access Credential.

- The lock will beep after successfully enrolling the presented credential.
• Repeat the Master Credential presentation followed by additional Construction Access Credentials for as many Construction Access Credentials as needed.

VERIFY SUCCESS

• Present the newly added Construction Credential(s) and verify access is granted

Factory Default Reset (FDR)

Things to Know

• FDR will return the Schlage LE to its original Settings as shipped from the factory.
• LE will beep when in FDR mode any time the inside lever is turned
• Factory Default Reset (FDR) will remove any non-default device settings, delete any construction or user credentials and allow for construction mode to be entered again.
• FDR does not have any effect on the firmware currently on the lock

NOTE: FDR will not remove the lock from your ENGAGE™ account.
To re-enroll a lock into another, ENGAGE™ account, you must first delete the lock from the original ENGAGE™ account

Perform a FDR

• Remove the Schlage LE battery cover and Press and HOLD the FDR button for 5 seconds. The Schlage LE will beep and blink two (2) times.

Verify Success

• Turning the inside lever will cause the Schlage LE to beep.
• Use the ENGAGE™ Mobile application and see the Schlage LE is now available for Commissioning
• The Schlage LE will now "Advertise" and be available in the ENGAGE™ Mobile for Commissioning
  NOTE: “Advertisement” Bluetooth communication requires the Schlage LE battery cover to be properly installed.
• A new Master Construction Credential can now be created
When working with Schlage® CTE single door controllers

Before you begin, review the installation instructions for the CTE Controller contained in the box along with the product. Also review all accessory details for the Power Supply, Credential Reader and locking device installation instruction to be sure of their interconnection and mounting requirements.

- You may want to record the CTE serial number and the intended (or installed) location for use by the property administrator when commissioning and entering data into ENGAGE™

Prepare for installation

- Gather your tools and accessories needed for the CTE, Credential Reader and Locking Device system installation. Additional items may be needed depending on the Power Supply and accessories chosen.

**WARNING:** DO NOT USE A POWER DRILL for any Schlage CTE Controller or accessory installation. Hand tool use ONLY is recommended to prevent product damage.

Schlage CTE Printed Circuit Board – labels, connections and indicators

Prepare for Installation

Install the Schlage CTE and accessories as indicated in their respective installation instruction. You will want to pay special attention to these installation planning concerns and items for best operational results.

- The Schlage CTE installation is intended for indoor use ONLY with a temperature range of -35C to +66C (-31F to +151F)
- For best security, mount the Schlage CTE in a location that is not accessible by the public.
• Determine the location and interconnection wiring requirements for each component before beginning (Schlage CTE enclosure, Credential Reader, Locking Device, etc.)

• For best Wi-Fi network and Bluetooth (BLE) wireless communication:
  o The Schlage CTE should not be mounted near larger metal objects or inside other metal enclosures or cabinets.
  o The Schlage CTE should be mounted within Bluetooth (BLE) communication range of the door opening. (Within 15 feet).

  NOTE: This is only important when the property is (or will be) also using Mobile Bluetooth enabled credentials.

• 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 wring the door hardware to either NO or NC, and selecting a failsafe or fail secure locking device.

Installation: CTE

The Schlage CTE is provided in an enclosure that allows the installer multiple options when mounting in its permanent location. Be advised, the Schlage CTE is not plenum rated.

The installer should refer to the Schlage 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 Schlage CTE, mounting anchors should be used.

The Schlage 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 very far into 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 electrostatic save manner.
Installation: Power Supply

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.

Installation: Credential Reader

The Schlage CTE will support one RS-485 Credential Reader. Either the MT11-485 mullion reader or the MT15-485 single gang reader are compatible. Refer to the credential reader installation instruction when installing.

IMPORTANT NOTES:

- Schlage CTE will not control the Credential Reader beeper.
- A Configuration Card (CE-401-133) is required to disable the credential reader beeper.
- The Reader needs to be paired with the Schlage CTE.
- Paring should happen automatically during the initial Power-ON process. If the Credential Reader does not respond, and presents a solid RED LED, it is not paired with the Schlage CTE.

NOTE: To pair a Schlage CTE and Credential Reader follow these steps

- Press and Release the Schlage Button one (1) time, then
- Press and Release the FDR button two (2) times
- The Credential Reader will blink AMBER three (3) times to indicate success

Installation: Locking Devices

Schlage CTE can support 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 INSTALLATION SUCCESS:

Test Relay Outputs:

The Schlage CTE has built in TEST options to test its installation quickly. Each of the three output relays DRY relays and three POWERED outputs can be manually actuated using a push-button on the CTE PCB. The installer may Press and Hold any of the TEST switches to manually test the LOCK RELAY, ALARM RELAY or AUX RELAY.
Both the DRY and the POWERED outputs of the relays will be exercised when the TEST buttons are pressed.

NOTE: Each output is overcurrent protected. The FAULT LED (see arrow) will be illuminated RED any time an overcurrent condition is detected at any of the relay outputs.

- **PRESS and Hold** each output relay TEST push button to verify the output is operating the locking device(s) and or accessories as intended.

**Test Credential Reader:**

A correctly wired the reader (Schlage MT11-485 or MT15-485) and the Schlage CTE STATUS LED blink whenever a credential is presented.

Test the READER and Schlage CTE RS485 connection, by following this button press sequence:

- Press and Release the **SCHALGE** button
- Quickly press the **FDR** button two (2) times
- When wired correctly the Schlage CTE and reader will respond with:
  - Three (3) LED AMBER blinks and three Beeps
  - The RS485 LEDs will be flashing

**Operation in CONSTRUCTION Mode:**

Things to know

- Construction Mode is provided like the Schlage NDE and LE products. Schlage CTE requires a MASTER Construction Credential that is used to add additional Access Constructions Credentials to each installed CTE.

- Construction mode feature is available out of the box or after a successful Factory Default Reset. (FDR)

- Construction mode operation provides NORMAL Credential function and the Schlage CTE will always automatically relock after momentary access is granted.
• Master Construction Credentials do not provide Access through the door. Master Construction Credentials can only add other Access Construction Credentials intended to gain momentary access.

• Construction Mode can be canceled by performing Factory Default Reset (FDR). After an FDR, all previously valid Construction Credentials will no longer be valid.

NOTE: No User Audits are stored in Construction Mode because the lock does not track time or credential numbers, yet.

• If the Master Credential is lost or destroyed no additional construction credentials can be added to the CTE. The Schlage CTE will require FDR and all construction credentials will need to be re-enrolled into the lock.

Create a Master Construction Credential:

• Start with a new Schlage CTE or one just after a Factory Default Reset (FDR) has been successfully performed.

• Remove the lid, and PRESS and HOLD the SCHLAGE button for 5 seconds

• Verify the Schlage CTE Mode indicator switches ON for Construction Mode.

NOTE: You will have 20 seconds to present a credential to the reader to become the Master Construction Credential before a timeout occurs

• Present a new credential to the reader to become the Master Construction credential.

NOTE: The Schlage CTE will acknowledge the credential presentation with 5 GREEN flashes of the Schlage CTE MODE LED and enroll the credential as the Master Construction Credential.

VERIFY SUCCESS

• Present the newly created Master Construction Credential to the Schlage CTE.
• The Schlage CTE STATUS LED and the Credential Reader LED will light GREEN for 20 seconds waiting for a credential to be presented for enrollment as a Construction Access Credential in the Schlage CTE.

NOTE: The next credential presented will be enrolled as a Construction Access Credential and be allowed momentary (normal) access to the Schlage CTE when presented again.

Create Construction Access Credentials

To enroll a construction credential that will allow Construction Mode Access, follow these steps:

• Present the previously enrolled Master Construction credential to the Schlage CTE reader.
  - The READER LED and CTE STATUS LED will illuminate GREEN waiting for the next credential presentation
• While the READER LED and the CTE STATUS LED solid GREEN, present a new credential intended to become a Construction Access Credential.
• The Schlage CTE will flash the Credential reader LED GREEN and CTE STATUS LED five (5) times to indicate successful Construction Access Credential enrollment.
• Repeat the Master Credential presentation to the reader followed by additional Construction Access Credentials for as many Construction Access Credentials as needed.

VERIFY SUCCESS

• Present the newly added Construction Credential(s) and verify momentary access is granted
**Factory Default Reset (FDR)**

**Things to Know**

- FDR will return the Schlage CTE to its original Settings as shipped from the factory.
- Factory Default Reset (FDR) will remove any non-default device settings, delete any construction or user credentials and allow for construction mode to be entered again.
- FDR does not have any effect on the firmware currently on the Schlage CTE or in the Credential reader.

**NOTE:** FDR will not remove the Schlage CTE from your ENGAGE™ account. To re-enroll a Schlage CTE into another ENGAGE™ account, you must first delete the Schlage CTE from the original ENGAGE™ account and perform a Factory Default Reset (FDR).

- The Schlage CTE MODE indicator will illuminate when the Schlage CTE is in Factory Default.

Perform a FDR:

- Remove the lid
- **PRESS and HOLD** the **FDR** button for **5 seconds** – then **RELEASE** it

- Press the **SCHLAGE** button three (3) times, there will be a beep with each button press.
  - The Schlage CTE STATUS and Credential Reader LED will blink **GREEN** for one second. This is indicating that the FDR process has been successfully completed.
- The CTE MODE indicator will illuminate when the CTE is in Factory Default as shown above.
- Replace the Schlage CTE lid.
Daily System Operations
Adding a User

Overview

Adding new users 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 and is shown here.

- Log into the ENGAGE™ Web application and Select USERS

![ENGAGE Technology Interface](image)

- Select the Add User button at the bottom of the screen

- Enter the Users’ information

![Add New User Interface](image)

- **First** and **Last Name** (required). In this case we entered John Doe.
- **Email Address** (optional)
- **Activation** and **Expiration dates** (required)
- Select **SAVE**

**VERIFY SUCCESS:**

- See the momentary “User Added” success message.

- See the new User (John Doe) is now listed in Users Tab.

**NEXT STEPS:**

After defining a New User, the new User will require the following steps to also be completed:

- At least one Credential Assignment (See Assigning Credentials)
- Access and Schedule Assignments for the property (See Assigning Lock Access and User Schedules)
- User Credential programming for No-Tour device updates. (See No-Tour Credential Programming)
- And, perform sync or No-Tour updates with each lock that the User has been granted Access. (See Sync – Updating a Door File)
Enrolling Credentials

Overview

Enrolling credentials is the process of entering the credential into ENGAGE™ for assigning to a resident. There are three methods of Credential Enrollment possible depending on the administrator preference.

Credential enrollment is a first step of granting a resident access to a door. After successfully enrolling credentials, the administrator must ensure all devices are commissioned and ready for access programming and previously enrolled credentials have been assigned to each User.

1. No-Tour credential enrollments are accomplished using the ENGAGE™ Web application and the commissioned MT20W credential reader. This method of enrollment is recommended:
   - The credential to be entered into ENGAGE™ for No-Tour functionality.
   - The credential to be assigned to the selected, existing User.
   - Access rights for the user are programmed into the credential, for No-Tour credential programming functionality.

2. No-Tour credential enrollments may also be accomplished using just the commissioned MT20W. This method of enrollment allows:
   - Credentials to be enrolled quickly – in bulk – for assignment – later
   - Credentials enrolled in this manner will be available in ENGAGE™ Web application under “Select Existing Credential” tab

3. Credential enrollments may be accomplished with the ENGAGE™ Mobile application and an installed device at the door. This method of enrollment allows:
   - Immediate credential enrollments and access assignment for a selected user while at a door.
   - Credentials are enrolled at any commissioned device; access updates can be made using the ENGAGE™ Mobile application.

   **IMPORTANT WARNING:**
   Credentials enrolled via this method will not be searchable by the Ink Stamp # (or Badge ID) in the ENGAGE™ Web application.
Enrolling credentials using ENGAGE™ Web application - RECOMMENDED

- Apply power to your commissioned MT20W
- Wait a few seconds until the MT20W boots up and connects with the local Wi-Fi Network. The LED will be solid BLUE indicating it is ready and connected to the local Wi-Fi network.

- Log into the ENGAGE™ Web application and Select USERS then USERS tab.
- Select any User to enroll credentials.
  
  NOTE: You must add a User if a user is not available for selection. See Adding a User if a User is not available.

- Select Add Credential

- Select the Select Existing Credential tab
• Obtain a new credential from your box of credentials (stock) to be enrolled.

   NOTE: In this case we chose credential # 2078

• Present the new credential to the MT20W and wait a few seconds.

   NOTE: The MT20W will turn GREEN and beep one (1) time when the card is accepted.

• Repeat card presentation(s) and enrollment process for each credential you want to make available in the “Select Existing Credentials” tab.

VERIFY SUCCESS

• Select the "Refresh List" button to view the newly added credential's ink stamp number(s).
- Confirm the physical “Ink Stamp” on your credential matches the new credential in the list.

**NEXT STEPS:**

Credential enrollment merely makes the credential available in ENGAGE™ Web application for assignment to a resident. To complete the process, the administrator may need to also:

- Assign the credential to an existing User (See Assigning Credentials)
- Provide Access and Schedule Assignments for the property (See Assigning Lock Access and User Schedules)
- Perform User Credential programming for No-Tour device updates. (See No-Tour Credential Programming)
- And, perform device syncing with each device the User has been granted Access. (See Updating a Door File)
Enrolling credentials into stock list (Schlage MT20W only)

It is possible to quickly enroll credentials into ENGAGE™ using just the Schlage MT20W. This method of credential enrollment will allow bulk enrollments into stock that can be selected and assigned to individual Users, later.

NOTE: Administrators will need to keep track of and manage the physical credentials that are enrolled to ensure they are available when needed for programming.

• To begin plug your Schlage MT20W into a power source and verify proper Wi-Fi network connection.

NOTE: The Schlage MT20W will take a few seconds to boot up and connect to the local Wi-Fi network. The LED will be solid Blue when the Wi-Fi connection is made and the MT20W is ready for use.

• Present a new credential to the Schlage MT20W and wait a few seconds.

NOTE: The Schlage MT20W will turn GREEN and beep once when the credential is enrolled into the Select Existing Credentials tab found in the ENGAGE™ Web application

• (REPEAT) Continue to present new credentials until all credentials have been successfully presented and enrolled

NOTE: We chose credentials 1171, 1802, 2886 and 5998 for enrollments in this example.

VERIFY SUCCESS

• Log into the ENGAGE™ Web application.

• Select any user, and Add Credential to view the available credentials in the “Select Existing Credential” tab.

  - All credentials previously enrolled will be listed.
NOTE: If the credential you want is not listed, you may need to select the "Refresh List" button to view a newly added credential.

NEXT STEPS:

Credentials enrolled with this method are merely enrolled into ENGAGE™ for assignment later. Administrators will still need to follow these steps to complete the process.

- Assign the credential to an existing User (See Assigning Credentials)
- Provide Access and Schedule Assignments for the property (See Assigning Lock Access and User Schedules)
- Perform User Credential programming for No-Tour device updates. (See No-Tour Credential Programming)
- And, perform device syncing with each device the User has been granted Access. (See Updating a Door File)
Enrolling Credentials at a Door

It is possible to assign a credentials to a specific user, using the ENGAGE™ Mobile application and an already enrolled ENGAGE™ device.

**IMPORTANT WARNING:** Credentials enrolled at the door, using a local device instead of the MT20W will have one limitation.

The enrolled credential will not be searchable in the ENGAGE™ Web application when using the Badge ID Search Utility.

- Log into the ENGAGE™ Mobile application while physically near an already commissioned ENGAGE™ device.
- Select the **USERS Menu** then the specific user to be assigned a new credential.
  
  **NOTE:** You must add a new user if the user is not already entered. See Adding a User if needed.

- Select an existing User to receive the new credential.
  
  **NOTE:** In this case we chose **John Doe** from the list

- Select the **Credentials** menu
• View the existing credentials assigned to this User. In this case, John Doe has no credential assignments.

• Select "+", to continue.

NOTE: A list of nearby commissioned devices will be displayed.
• Select the "Available Enrollment Device" you want to use as the enrollment reader from the nearby device list provided. In this case we chose the **Storage**.

  **NOTE:** After selection of the Storage lock, the LED will be flashing RED for the next 20 seconds. The Storage door is waiting for a credential to be presented.

• Present the new credential to the nearby device (Storage) with a flashing RED LED.

  **NOTE:** When the device reads the credential, the ENGAGE™ Mobile application will display a credential "Value" with asterisks ******** displayed.
NOTE: If no credential is presented, the process will “Time Out” after 20 seconds so the device can return to normal operation - securing an opening.

Should a Timeout occur, Select OK in the popup message and try again.

- Tap on the Function menu setting if the default “Normal” assignment is not wanted. You may set any credential function as needed.
Contact Technical Support @ 1-877-671-7011 Option 2, Option 2 for ENGAGE™ and supported devices
– Hours of Operation 8 AM to 8 PM EST –

Page 181 of 250

- Select Done, then
- Select Save
- Acknowledge the “Credential Updated Successfully” message

Credential Updated
Successfully!

OK

- Select OK
- Select Save to complete the credential enrollment.
- Acknowledge the Credential Enrolled successfully message.

Credential Enrolled Successfully!

Ok

- Select OK

VERIFY SUCCESS

- The new credential is now listed for John Doe with the desired (Toggle) credential function
NEXT STEPS:

This enrollment process merely selects the credential function and assigns the credential to the existing User. To complete the process, the administrator may need to also perform these steps:

- Provide new Access and Schedule Assignments for the property. (See Assigning Lock Access and User Schedules)
- Perform device Sync with each device the User has been granted Access. (See Updating a Door File)

Remember, the enrolled credential will not be searchable in the ENGAGE™ Web application when using the Badge ID Search Utility
Assigning Credentials

Overview

Assignment of a credential will connect a credential to a user to identify the user in ENGAGE™ Audits and in the ENGAGE™ devices for granting access

HINT: To successfully assign a credential and grant access, you must have commissioned locks, added Users into ENGAGE™ and created any property Schedules.

WARNING: New credential assignments will require all devices that the User has assigned access to be programmed before the credential will be honored. Device programming can be immediate with the No-Tour process or provided via syncing (Door File Updates) at the door or overnight Wi-Fi connection when available.

- Open the ENGAGE™ Web application.
- Select USERS tab and a user to be assigned a credential. In this case we chose New User. Notice this user has no credentials assigned now.

  NOTE: You must add a new user if the user is not already entered. See Adding a User if needed.

- Select Add Credential
• Select the Credential to be used from the "Existing Credential" List. In this case credential # 1965 has been selected.

Note: If no credential is available, you must enroll a Credential now.

• Select Credential Function from the Pull-Down menu. (Normal is default)

WARNING: When working with Schlage Control™ devices, a Toggle credential function will act as a Normal credential function

• Select SAVE

VERIFY SUCCESS

• The selected credential (# 1965) is now listed under Credentials for the selected User
NEXT STEPS:

This process merely assigns a credential to the User. Property administrator will need to ensure the effected property doors are programmed before the credential access will be honored at the door. Administrators will need to follow these steps to complete the device programming process.

- Provide Access and Schedule Assignments for the new credential (See Assigning Lock Access and User Schedules)
- Perform User Credential programming for No-Tour device updates. (See No-Tour Credential Programming)
- And, perform device syncing with each device the User has been granted Access. (See Updating a Door File)

NOTE: ENGAGE™ will display device **Update ICONs** indicating the Devices and credentials that need programmed.
Adding New Devices

To add a new device into the ENGAGE™ database, you must use the ENGAGE™ Mobile application, commissioning process.

See Device Commissioning for information on how to add the a new ENGAGE™ compatible device into your account.
No-Tour Credential Programming

Overview:

The Schlage MT20W must be used to initially enroll Smart credentials and to read and write information to the credentials and to enable No-Tour functionality. No-Tour functionality access rights and programming information is written to the credential and then the programming information is transferred to the ENGAGE™ devices when the credential is presented to the device at the door.

ENGAGE™ will read the smart credential serial number of a credential presented to the Schlage MT20W, apply the required updates from the ENGAGE™ database and program updates onto the credential.

The credential is then prepared to update the door programming when presented to the device by the resident.

To begin:

- Make all access and user schedule assignments and updates for the resident in ENGAGE™ as necessary.

- Ensure the Schlage MT20W is powered up and within the local Wi-Fi network communication range.
  - The Schlage MT20W will take a few seconds to boot-up and connect to the local Wi-Fi network.
  - The Schlage MT20W LED will be solid Blue when the Wi-Fi connection is made and the Schlage MT20W is ready for use.

  NOTE: There is no requirement for the property manager to open the ENGAGE™ Web application during No-Tour credential programming. Access updates that are already defined in ENGAGE™ will be programmed onto the smart credential, automatically

- Place the residents’ smart credential to be programmed with new Access Rights on the Schlage MT20W.
  - The Schlage MT20W will turn solid GREEN to begin the programming process, followed by one beep. This is your indication that the credential serial number has been read by the Schlage MT20W to start the process

- Leave the credential on the Schlage MT20W until it provides its programming success message indicating that the credential programming process is completed.
- The PROGRAMMING SUCCESS message is three (3) GREEN LED blinks and beeps.

- If the PROGRAMMING SUCCESS message is NOT provided, see the No-Tour Credential Programming Failure section below:

  - Wait for the Schlage MT20W to provide the programming success message.

VERIFY SUCCESS

- Open the ENGAGE™ Web application

- Verify the ENGAGE™ orange Update ICONs are no longer displayed next to the resident’s credential listing.

  - This is your indication that the credential is programmed with the latest updates.

- Complete the No-Tour programming process by physically presenting the newly programmed credential to all effected locks.
Searching for Credential Owners

Overview:

A "Found" credential that was enrolled using the Schlage MT20W can be identified by entering the badge ID (or ink stamp) in the Badge ID search feature.

When a credential is not in the database a "Badge ID not Found" message is displayed.

![Badge ID Not Found]

The search for badge ID 22905 was unsuccessful. Credentials enrolled through the lock will not have a Badge ID, so these will not be part of the Badge ID search.

OK

WARNING: If the credential as initially enrolled using an installed device, instead of the Schlage MT20W, it will not be searchable in the ENGAGE™ database and will not be found here.

- Open the ENGAGE™ Web application
- Select Advanced
- Select Credentials
- Enter the Badge ID (22904) into the "Badge ID Search" field and select the Search ICON

![Credential Search]

VERIFY SUCCESS

- The credential owner and badge ID is displayed. New User with badge 22904
- If no credential is found, check that the Badge ID was entered correctly and try again
Resident Moves Out

When a resident moves out, it is important to recover the residents’ credentials and plan for the credential(s) next use. Here are two situations to consider:

1. Resident Moves out and returns their smart No-Tour credentials with a new resident in line. The new resident will require the SAME access rights. In this case the property administrator may choose to:
   - Just rename the User in the ENGAGE™ database to “The New Resident”
   - Re-issue the credential to the new resident.
   Or,
   - Use the ENGAGE™ “Replace” feature

2. Resident Moves out and does not return their smart No-Tour credential. In this case the property administrator must proactively manage their property to block/remove access programming from the credential and to guarantee security at every door the resident previously had access.
   - The credential should be deleted in the ENGAGE™ database
     - This will remove all previously programmed door accesses for that credential
     - This will generate the update ICONs in the ENGAGE™ database needed to indicate which doors will require Sync updates
   - Sync all doors with updates required

   **WARNING:** The property administrator must Sync doors with previous access to remove the unreturned credential from the lock database and to deny future accesses
Deleting Existing Access

When the resident’s credential is not available you must **Delete Credential** from the ENGAGE™ database and then Sync with each door that the credential had access.

- Open the ENGAGE™ Web application
- Select the User to have access deleted on the Users tab
- Select **Assign Access** button
- Remove the "Check Marks" for each of the locks from the list to delete their access rights
- Select **SAVE**

**VERIFY SUCCESS**

- The access rights for the deleted doors are no longer displayed in the "Current Access" list

**WARNING:** The doors with newly deleted access assignments, MUST be updated before the deleted Access Rights will be honored (denied). Sync with each device is required

**NOTE:** ENGAGE™ will display the "Update" ICON indicating the selected doors need programmed. The update ICON will remain presented until an Audit is returned that confirms that the door has been updated.
Deleting a Credential

- Open the ENGAGE™ Web application.
- Select the USERS and the specific User to have a credential deleted on the Users tab.

- Select the credential to be deleted from the Credentials listed to continue.

- Select Delete This Credential.
- Type the word **DELETE** into the Confirm: Field
- Select **Delete**

**VERIFY SUCCESS**

- The Credential is no longer listed under Credentials
WARNING: Deleting a credential requires all devices that previously had access with that credential, to Sync or No-Tour programming, before the deleted credential will be denied access at the door.

NOTE: ENGAGE™ Web application will display the exclamation point "Update" ICON to indicate which doors with deleted access rights that require programming.
Deleting Devices

Overview

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

- Open the ENGAGE™ Web application.
- Select the **DEVICES** tab.
- Select the specific device to be deleted from the property device list.
  
  **NOTE:** We chose the **Conference Room** door for deletion.

- Select the **Delete** button
• Confirm the process by typing **DELETE** into the Confirm box.

• Select the **“Delete”** button to continue.

**VERIFY SUCCESS**

• See the momentary “Device deleted” success message.

  ![Device deleted](image)

• The **Conference Room** device is no longer listed in the **Devices** screen.
Using the ENGAGE™ Mobile application for device deletions

- Open the ENGAGE™ Mobile application
- View the **Devices** tab.
- Find the device to be deleted in the list.

**NOTE:** In this case we will chose the **Apt B845** device for deletion.

- Swipe (leftward) on the device name to enable (or uncover) the **DELETE** button.
• Select **DELETE**.

**VERIFY SUCCESS**

• The **Apt B845** is no longer listed in the **Devices** screen
Replacing Credentials

Overview

Replacing a credential swaps one credential for another that carries the same access assignments as the original credential and blocks/deletes all access from the original (lost or destroyed) credential. This feature is most useful when credentials are damaged/broken or when the original credential is lost.

IMPORTANT WARNING: An old or lost credential will still be valid at previously programmed doors until the lock is presented with the replacement No-Tour credential or until a device Sync is performed automatically over-night or done at the door.

- Open the ENGAGE™ Web application.
- Select USERS tab and the effected User in the User tab.

- Select the BLUE credential currently assigned to the Existing User (Credential 1171).

NOTE: In this case credential # 1171 is going to be removed from the system and replaced with a credential that is available in stock (previously enrolled)
• Select **Replace this credential** to bring up a list of available replacement credentials.

![Diagram of credential interface](image)

**NOTE:** If no credentials are available for replacement, you must enroll a credential now. See Enroll Credentials.

• Select a new **Replacement** credential from stock list. In this case we chose credential # 1802.

**WARNING:** Physically verify the ink stamp on the physical credential matches with the assigned credential from the stock list before Confirming the Replacement.
• Select **Confirm**

**VERIFY SUCCESS**

• View the momentary "Credential Replaced Successfully" message.

[Credential Replaced Successfully]

• The new Credential (1802) is now listed under the user Credentials and the old "Replaced" credential (1171) is removed from the list.

• Notice the ICON by the credential is indicating the credential now needs programming with the Schlage MT20W.

• Select **Update** in the Credentials screen above with the Schlage MT20W powered up and communicating with ENGAGE™ and with the smart credential in hand.
- Follow the instruction provided on screen, then Select **Next**

- Select **Finish**
• Notice: the ICON by the credential is now removed, indicating the credential was programmed successfully and has no additional programming required.

NOTES:
- ENGAGE™ will also display Update ICONs indicating the affected locks that require Sync with new access programming.
- Schlage NDE, LE, and CTE devices may be updated nightly via automated Wi-Fi network connections.
- Schlage Control™ smart locks may be updated via No-Tour or by the ENGAGE™ Mobile application using the “Sync” feature.
Updating Device Firmware

Overview

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

Individual device firmware updates are available for Schlage Control™, Schlage NDE, LE, CTE and the MT20W using the ENGAGE™ Mobile application. Alternatively, Schlage NDE, LE, and CTE devices may be scheduled for overnight firmware updates when the local Wi-Fi network is properly enabled and available.

WARNING: If you are using a Software Alliance Member (SAM) account, be sure to consult your SAM before updating firmware on your devices. Ensure your SAM software version is compatible with the latest ENGAGE™ device firmware.

IMPORTANT NOTES:

- Schlage Control™ device firmware must always be updated at the door using the ENGAGE™ Mobile application and Firmware Updates at the nearby door.

- For Schlage NDE, LE, 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.

- Schlage NDE, LE, and CTE nightly Wi-Fi updates require Wi-Fi network availability over night for the scheduled firmware updates to be successful.

- Schlage NDE, LE, and CTE firmware nightly Wi-Fi updates are scheduled by ENGAGE™ in the early morning hours during low Wi-Fi network activity and to reduce user issue opportunities while the device is inoperative for the few minutes it is being updated.

- Firmware updates will take some time to complete. The devices will flash the “Amber” LED while the firmware file is being sent to the device. Then the device will parse the file into its memory while flashing the LED RED and GREEN. This process will take several minutes to complete – be patient.
Device Firmware Updates - at the door using Bluetooth (BLE) communication

Firmware updates are available for all devices using the ENGAGE™ Mobile application. Schlage Control™ devices require nearby Bluetooth (BLE) communication with the mobile device for firmware updates, while the all other ENGAGE devices may also use a local Wi-Fi network connection for faster firmware updates and scheduled firmware updates using Wi-Fi.

This example is updating a Schlage Control™ device which requires Bluetooth (BLE) for updates. All other devices may also be updated via local Bluetooth (BLE) communication, when necessary.

- 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.

- Select the local device to be updated with the latest firmware. In this case we chose a Schlage Control™ device, Apt 5D2B
• Select More

NOTE: The device will begin flashing the RED LED when connected and communicating.

• Select Update Firmware in the connected device menu.
NOTE: When a firmware update is available, this message is presented.

- Select **Update** in the connected device menu.

WARNING: This is a local Bluetooth (BLE) firmware update method. The mobile device MUST stay within communication range while downloading firmware. This will take a few minutes – be patient.
The following screen will be displayed when the firmware update is successful.

NOTE: The recently updated device will load the new firmware into its memory and REBOOT itself. This process will take a few minutes – be patient.
Device Firmware Updates – at the door using local Wi-Fi network communication

ENGAGE devices with local Wi-Fi connectivity may have firmware updates performed at the door. This method is preferred over the previous described Bluetooth (BLE) method because it will use the local Wi-Fi network for faster communication and does not require the property administrator (mobile device) to remain at the door during the firmware update process.

For this example, we will update a Schlage LE device using a local Wi-Fi network connection.

- 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.

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

- Select **Update Firmware** in the connected device menu.
NOTE: Confirm the requested firmware update in the screen above. If the firmware version on the device is current a “Firmware is up to date” message is provided.

- Select Update

NOTE: installing the firmware will take a few minutes, be patient
NOTE: This message is provided as an indication that the firmware has been downloaded from the server to the device.

- Select Finish

NOTE: The device will blink the LED RED and GREEN while installing the new firmware update. During this time, the device will be inoperative. Once the firmware installation is complete, the device will reboot and begin normal operation. This process will take a few minutes, be patient.
Device firmware updates – at the door with no local Wi-Fi network available

When the device *does not* have the Wi-Fi network connection available or the local Wi-Fi network is not enabled. The firmware download will be performed by temporarily enabling a Wi-Fi connection through the property administrator’s mobile device.

In this case the **Storage** device Wi-Fi has been turned **OFF** in **Settings** (not enabled)

- 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.

  ![Device List Screen](image)

- Select the local device to be updated with the latest firmware. In this case we chose **Storage**

  **NOTE:** This is an Schlage LE device with its Wi-Fi network connection disabled (OFF)
• Select More

then

• Select **Update Firmware** in the connected device menu.
NOTE: Confirm the requested firmware update in the screen above. If the firmware version on the device is current a “Firmware is up to date” message is provided.

- Select Update

NOTE: Follow the displayed instruction to enable the ENGAGE™ device and the mobile device Wi-Fi connection

NOTE: The system will know the device name, the Wi-Fi PASSWORD will be stored in the mobile device “Clipboard”.

Contact Technical Support @ 1-877-671-7011 Option 2, Option 2 for ENGAGE™ and supported devices
- Hours of Operation 8 AM to 8 PM EST – 5ES20171127C
Page 215 of 250
• The steps to be performed on the mobile device are:

1. **Leave** the ENGAGE™ mobile application – temporarily
2. **Open** the Settings menu on your mobile device
3. **Select** the Wi-Fi network settings menu
4. **Connect** with the Wi-Fi with the same name as the device you are connected to.
   - In this case we must choose **Storage**
5. **Paste** the PASSWORD into the Wi-Fi settings field, using the standard mobile device “Clipboard” paste utility
6. **Select Join** the network
7. Verify the mobile device connects with the selected device by viewing its Wi-Fi connect information.

• **Return** to the previous ENGAGE™ mobile application screen
• **Select** Next
Complete the device Firmware updates after download

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

The device will follow the successful firmware download with an additional firmware installation process indicated by the device blinking the LED RED and GREEN for a few minutes – be patient.

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

IMPORTANT NOTE: After a firmware update using this method is successfully accomplished, the device is ready for normal operation. However, ENGAGE™ will not know that the firmware update process has been accomplished and will report the previous firmware revision until the next device Sync reports the new successful firmware update to ENGAGE™.

WARNING:

- The firmware internal memory installation will take a few minutes to complete. Be patient.
- While the device internal firmware installation is in process the device will be flashing RED and GREEN LED.
- During the device internal firmware update process the device will not act as a lock. Access attempts will be ignored.
- Wait for the RED and GREEN LED flashing to stop before using the lock for normal access again. Be patient this will take a few minutes
- A device Sync will be required to report this update to ENGAGE™

VERIFY SUCCESS

- Open the ENGAGE™ Mobile application.
- Connect to the nearby device with new firmware
- Select the device, the More
- Select the Update Firmware menu
- See that the device has the latest firmware
Scheduled Firmware Updates – Schlage NDE, LE, and CTE

Firmware update scheduling is available for Schlage NDE, LE, CTE, and MT20W devices using the ENGAGE™ Web application. Administrators will use this feature to automatically keep their devices updated with the latest firmware revision and operational functionality. To schedule automatic firmware updates for your Schlage NDE, LE, CTE, and MT20W devices, follow these steps.

WARNING: Schlage NDE, LE, CTE, and MT20W must have their Wi-Fi network configurations set and working with the local Wi-Fi network before automated firmware updates are possible.

- Open the ENGAGE™ Web application
- Select Advanced tab
- Select the Firmware tab
- Compare the "Current Firmware Version" on each device and the "Latest Firmware Version" that is available

- When a firmware update is available, check each device(s) that require a firmware update

NOTE: In this case the Garage 141B, Laundry 137, Lobby 83, Pool 142 and Pool 286 firmware is not at the latest revisions. Also note that the Store Room has outdated
firmware as well, but that device is a Schlage Control™ device and cannot be selected for scheduled firmware updates.

- Select the "Update Selected Devices" button at the bottom of the screen to complete the schedule event

VERIFY SUCCESS

- See the momentary Firmware updates have been scheduled message

- Wait until the next day to review the device firmware status to confirm the process was completed.

VERIFY SUCCESS using the ENGAGE™ Web application

- Open the ENGAGE™ Web application
- Select the ADVANCED and Firmware tabs to review the device firmware status.
- The Current Firmware Version listed should now be the Latest Firmware Version available for any device that was scheduled for an overnight firmware update

WARNING: If a selected device still has an old firmware version installed
- Check the local Wi-Fi network availability overnight - it may have been down
- Verify Wi-Fi network communication and settings in the device are correct.
- Reschedule the device firmware update to try again
Retrieving Audit Data from Devices

Overview

Device and User Audits are information collected by the devices whenever any action is taken. For Schlage Control™, audits can only be retrieved locally at the door using the ENGAGE™ Mobile application, while Schlage NDE, LE, and CTE device audits may also be gathered nightly via a Wi-Fi network connection.

Using the ENGAGE™ Mobile application

- Log into the ENGAGE™ Mobile application while nearby the device for Audit gathering.
- View the In Range Screen.

- Select the device for audit gathering for the nearby listing. In this case we chose Storage.
• **Select More**

![Select More](image)

then

• **Select Audits**

![Select Audits](image)
NOTE: Device Activity is the default Audit Screen. Additionally, the property administrator may select the Diagnostics tab for system Audits. Also retrieved Audits are always available via the ENGAGE Web Application as well.

- The retrieved Audits are now available for viewing on either the ENGAGE™ Web application or the ENGAGE™ Mobile application.

- If you receive this message after selecting “Get Audits”, there are no new Audits available, all existing device audits have already been retrieved.
Using Nightly Wi-Fi Updates

Schlage NDE, LE, and CTE devices may be enabled to call in to ENGAGE™ every night when the Wi-Fi network communication settings are properly setup.

New or updated access rights, schedule addition or changes and any Audits will be gathered during the nightly Wi-Fi network call in.

NOTE: No actions other than ensuring proper Wi-Fi network settings are initially installed and working are required by the property administrator to automatically receive nightly device audits from Schlage NDE, LE, and CTE devices.

Use the device’s Test Wi-Fi feature to verify network settings and proper communication.

See Sync – Overnight – Schlage NDE, LE, and CTE for more detail

WARNING: Nightly Wi-Fi network updates (Call-In) is not available with Schlage Control™ smart locks.
Viewing Audit Information

Overview

Device and User Audits are information collected by the lock when any action is taken. Viewing Audits can be invaluable for determining when users access certain areas, crime detection and prevention, checking evidence of residence entry or attendance, collaborating verbal accounts, and so forth.

For Schlage Control™ devices, audits can only be retrieved locally at the door using the ENGAGE™ Mobile application. Schlage NDE, LE, and CTE device audits may have Audits gathered at the door, or remotely by taking advantage of these devices’ Wi-Fi network connection capability.

Audits may be reviewed by either of the ENGAGE™ Web or Mobile applications. Audit data may be filtered and exported for easier review and data analysis while using the ENGAGE™ Web application.

Using the ENGAGE™ Web Application

- Open the ENGAGE™ Web application

Displaying Audits for an individual device

- Select the DEVICES and the Devices tab

- Select desired lock from the list – we chose Storage Room
• Select Device Audits.

NOTE: Sort the displayed data as necessary using the column headers

**Displaying Audits for Property Wide Audits**

• Open the ENGAGE™ Web application.
• Select AUDITS.
• Use the available Sort and filter options, as desired. 
  
  NOTE: Data can be sorted or filtered numerous ways. 
  - By Device or User 
  - By Audit Type 

- START and END times 

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

  o Data will be saved into a .csv file for easy spreadsheet analysis 
  o Save your audit file to disk for archive and analysis 

  NOTE: You may need to select the Refresh button for the latest information to be displayed
Master Credentials

Overview

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

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.

IMPORTANT NOTES:

- Master Credentials are generally used for Property Maintenance and local Fire Department and emergency access to all openings on the property.
- A Master Credential will allow PASS THROUGH credential function access to every ENGAGE™ managed opening on the Property.
- The Master Credential feature is **DISABLED by default**.
- When using Master Credentials, the feature should be enabled before commissioning.
- Any device commissioned before the Master Credential feature is enabled will require a syncing (Door File update) to enable the feature, at the door.
- No-Tour cannot enable the Master Credential function at the door – The ENGAGE™ database setting must be enabled first and then each lock must be Sync’d before a Master Credential feature will be enabled.
- No-Tour programming can **ADD** a Master Credentials. However, to **DELETE** a Master Credential the credential must be deleted in the ENGAGE™ database and every lock must be sync’d.
- Any valid User credential type can be assigned as a Master Credential.
- Multiple Master Credentials can be generated for the same property.
- Lost Master Credentials, require every originally programmed device to be re-programmed to remove the lost Master Credential.
- 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 syncing process (Door File updates) across the whole property.
- **DELETED** Master Credentials are permanently **DELETED** and can never be used again in the same ENGAGE™ account – ever. **BEST PRACTICE** - Destroy Deleted Master Credentials.
- **BEST PRACTICE**: Provide a special name for the user assigned the Master Credential for easy traceability within device and user audits. (i.e. Master User-1)
Enable Master Credential Generation

- Open the ENGAGE™ Web application
- Select the ADVANCED tab and Global Settings

- Slide the Master Credentials button to ON to enable the generation of Master Credentials

VERIFY SUCCESS

- View the momentary Master Credentials setting updated. message
- View the Master Credentials setting has moved to ON

**NEXT STEPS:**

- This process merely enables Master Credentials to be generated within the ENGAGE™ Web application. The administrator should now:
  - Add a User to become the Master Credential holder
  - Assign a credential to the User, to become the Master Credential
  - Assign a credential as MASTER
  - Update each lock on the property via No-Tour or syncing (Door File updates).

**WARNING:** All devices must be synced (Door file updated) if they were commissioned before enabling the Master Credential. BEST PRACTICE is to make this setting before commissioning and devices
Assign a Credential as MASTER

- Open the ENGAGE™ Web application.
- Select the **Users** tab and the User intended to receive a MASTER CREDENTIAL.

**NOTE:** As BEST PRACTICE we have given the User a name that identifies them as a Master Credential holder in Device Audits. In this case we will pick the current User, **Master Credential-1** with credential #5715 already assigned.

- **Select** the currently assigned credential that is to become a MASTER CREDENTIAL. In this case we have only one credential to choose, #5715.

**NOTE:** If the option in the next screen, *make this credential a Master Credential* is not presented, you must go back and enable the Master Credential Feature first. See **Enable Master Credential Generation**
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.

- Select **Make this credential a Master Credential**
- **Acknowledge** this WARNING message.

- Select **OK**
VERIFY SUCCESS

View the User’s assigned credential and see the Master Credential ICON by the credential indicating it is programmed as a MASTER CREDENTIAL with the PASS-THROUGH function assignment on every lock.

NOTE: This process merely assigns the credential as a Master Credential and schedules it to be programmed into every lock on the property.

• Select Update in the Credentials screen above with the MT20W powered up and communicating with ENGAGE™ and with the smart credential in hand.

• Follow the instruction provided on screen, then Select Next
• Select **Finish**

**NEXT STEPS:**

• Every Device will now have the **Device Update ICONs** displayed to inform the operator that door updates are needed.

• The Master Credential itself and all devices will be required to be updated before these changes will be honored.

• The administrator must ensure all doors on the property are updated with No-Tour or sync’d (Door Files updated) to add the new Master credential.

  **WARNING:** The administrator should provide device sync for the entire property when a Master Credential is being added. No-Tour updates can replace Master Credentials; however, device updates can be easily missed (skipped) when using the manual No-Tour process.
View and Delete MasterCredentials

- Open the ENGAGE™ Web application.
- Select the ADVANCED and then select the Credentials tab.

To View Master Credentials:

- Select View All Master Credentials. All Users with Master Credential assignments are displayed.
To Delete Master credentials:

- Select **Delete Master Credentials**.

- Select the checkbox for each Master Credential to be deleted.
  - Select **Delete**.
  - Select **OK** to accept the Delete the Master Credential WARNING message.
VERIFY SUCCESS

- Verify that the selected Master Credential has been removed.

NOTE: The deleted Master Credential # 1171 is no longer displayed.

NEXT STEPS:

- This process merely removes the Master Credential from the ENGAGE™ database and schedules the changes needed for the property. All devices in the ENGAGE™ Web application will now show the Device Update ICONs.

- All devices will be required to be updated before the deleted Master Credential change will be honored at the door.

WARNING: The administrator should provide sync (Door File updated) the entire property when a Master Credential is being deleted. No-Tour updates can remove and replace Master Credentials; however, devices can be easily missed when using No-Tour.
Things to Remember

Best Practices – System Set-up

- Each User/Resident should not be assigned more than one credential.

- Determine what your property wants to use for the default User Expiration date. ENGAGE™ will default all User Expiration Dates to five (5) years after enrollment automatically.

- Property administrators who review and confirm **default settings** before commissioning the first device, will save time setting up their property and not require device Sync updates for device settings after commissioning.

- Property device schedules should be defined before any device is commissioned. Any 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 will require Sync of devices, before any group update will be valid at 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 door’s locking device will require Sync so that it knows what group it is assigned.

Best Practices – Device Set-up

- For best reader response and improved battery life, it is recommended to disable any credential technology on multi-technology readers that will not be 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 when small format FOB credentials are in use. **WARNING**: Both HIGH and MAX reader sensitivity settings will reduce device battery life

Schlage Control™ smart locks

- Schlage Control™ smart lock setting updates always require local Sync (Door File updates) using the ENGAGE™ Mobile application for access updates. No-Tour updates will not provide device setting changes.

- The automated nightly Wi-Fi device syncing (Door File updates) is available with Schlage NDE, LE, and CTE only, Schlage Control™ devices do not support Wi-Fi connectivity.

- Schlage Control™ devices only support User Schedules - No Holiday Schedules, No Door Schedules.
o Schlage Control™ devices require an “Audit” request at the nearby device using the ENGAGE™ Mobile application to gather audits.

o Device Audits are also automatically gathered immediately following a Device Sync Update.

o Construction Mode uses ONLY the Facility Code of the first card presented which immediately allows ALL OTHER credentials with the SAME Facility Code to have access. Other products (Schlage NDE, LE, and CTE) require a Master Construction Credential and individually added Access Construction Credentials for temporary construction access.

Schedules

• Schedules can ONLY be created or modified by the ENGAGE™ Web application.
• Best practice is to define and confirm ALL schedules needed in your property before commissioning any device. Otherwise every installed and commissioned device may require reprogramming when a new schedule is made or updated.
• 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). All devices get the same set of User Schedules defined by ENGAGE™.

  NOTE: Therefore, a schedule change requires the administrator to program each door when new schedules are added or changed
• Temporary access for maintenance should use User (Time-of-day) Schedules and User Activation/Expiration settings to manage temporary access.
• A device sync (door file update) is needed to communicate new device settings and schedule device access and firmware updates in a device.
• Schedule START/STOP times and Days-Of-The-Week settings cannot be programmed to a device with No-Tour.

  NOTE: No-Tour programming will allow for User Schedule Activation and Expiration setting updates.

Master Credentials

• When Master Credentials are defined or deleted ALL devices MUST be updated via device syncing (Door File updated) to enroll or remove the Master Credential.

Update ICONS

• Device Update ICONS ⬤ within the ENGAGE™ Web AND Mobile application(s) are your indication of work performed and work remaining to be accomplished.
• **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 table]

NOTE: The credential update ICON will remain until the credential is successfully programmed with the desired changes.

• **Device Update ICONs** are provided next to the device name, any time the device has changes or updates pending and the device need to be programmed.

NOTE: The device update ICON will remain until Audit information is returned to let ENGAGE™ "KNOW" the update at the door has been accomplished.

  - Once an update is acknowledged in an Audit, ENGAGE™ will remove the Update ICONS.

**Factory Default Reset**

• Factory Default Reset is used to recover a device that was previously commissioned in another property or in Construction mode, so that it may be commissioned again.

• Factory Default Reset will NOT remove the device from the ENGAGE™ database, it merely returns the device to its out-of-the-box configuration.

**Moving Devices Between ENGAGE™ Accounts**

• To use a commissioned device in a new account, the original ENGAGE™ device enrollment MUST be deleted from the original ENGAGE™ account before it can be commissioned into a new (different) account.

**Dual Technology Credentials (Schlage NDE, LE, and CTE ONLY)**

• When using dual technology credentials AND No-Tour, all “No-Tour” multi-tech devices can be configured to disable PROXIMITY credentials. Disabling the unnecessary proximity credentials will save battery life by not “looking” for unnecessary credentials and improves the user experience when presenting credentials for access (faster response).

• To disable Proximity Credentials, see Device Settings for Schlage NDE and LE devices.

• The Wall mounted reader used with Schlage CTE will require a Configuration Card to disable Proximity Credentials.
Troubleshooting
All devices – Diagnostic Audits

Schlage NDE, LE, and CTE devices will provide diagnostic data when requested by the ENGAGE™ Mobile application. Diagnostic data that is provided includes, Battery Health, Wi-Fi connection success, hardware module checks and more. NOTE: You must be nearby the device for Bluetooth communication.

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

NOTE: You can view Audits for the device using the ENGAGE™ Web application, select the DEVICES tab, select the device name and then select Device Audits.

Inviting Team Members
- Email invitation never arrives
  - Check SPAM and TRASH folders for misplaced email
  - Verify the entered email address is correct
  - Verify your PASSWORD

Device Commissioning
- Device never shows up in the In Range mobile 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?
  - Schlage Control™: Is the deadbolt retracted?

Construction Mode
- Device will not allow Construction Mode
  - Devices MUST be “out-of-the-box” or recently Factory Default Reset (FDR)
  - Perform a device Factory Default Reset (FDR), and try again

Schlage MT20W (overview)
- A commissioned Schlage MT20W will try to connect to the local Wi-Fi network any time power is applied.
- When connected and communicating the Schlage MT20W will display a solid Blue LED indicating it is ready for use.
• When power is applied, the Schlage MT20W LED will be 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 will remain solid RED.
  - If the Schlage MT20W is commissioned it will connect to the Wi-Fi network after booting up is finished.
• When connecting to Wi-Fi the MT20W LED will flash fast BLUE for a few seconds followed by a solid Blue LED when the connection is accomplished.

Schlage MT20W would not connect to the Wi-Fi Network
• Verify with a Mobile device if the Wi-Fi network (Access Point) is present and available by using a mobile device (phone) to connect to the SAME Wi-Fi the device is using. This will:
  - Verify proper SSID and Password settings, if applicable
• Perform FDR and Commission again,
  - NOTE: Requires Configuration card CE-000-040 for Schlage MT20W FDR

Schlage Control™ - "Jump Start" Process
• Schlage Control™ devices will allow an external +9Vdc battery to be applied for access when the internal AA batteries are depleted. This device has NO mechanical key access so the Jump Start is the only method for access when the batteries are completely depleted.
• Devices with depleted batteries replaced should CONNECT with the ENGAGE™ Mobile application to ensure the Date and Time is accurately maintained and audit information is correct.

To Perform a Schlage Control™ “Jump Start”
• Touch and HOLD a new alkaline 9-Volt battery to the Schlage Control™ contacts just below the thumb turn
  - Battery connection orientation is not important as the lock accepts either polarity
• Wait until the lock starts up and provides 1 RED LED flash and then 3 GREEN LED flashes and 3 beeps. The lock startup will take a few seconds
• While still HOLDING the external battery in place, present a valid credential for access
• The lock will unlock as normal with the normal Relock Delay
  - Remove the external battery while the device is unlocked and turn the Thumb Turn to gain access
  - NOTE: The battery is removed after gaining access because the Thumb Turn will physically hit the external battery when turned
• Replace the device AA batteries
  - NOTE: Alkaline AA batteries are required for proper operation

Set Device Date and Time
• Device date and time is automatically checked and set (if needed) each time a mobile device is connected and communicating with the ENGAGE™ device. Setting the date and time should only be necessary if/when the device power has been removed for an extended period.
  - Open the ENGAGE™ Mobile application
- Select the **In Range** menu
- Select the nearby device
- NOTE: When connected the device LED will be flashing RED
- The Mobile Device Date and Time settings will automatically be set into the device

**Device Firmware Updates Overnight were not performed**

- Verify local Wi-Fi network was operational overnight. Was there an outage?
- Verify the device Wi-Fi network settings, SSID, user name and password

**Schlage 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 will not be able to communicate with the Schlage CTE.

  NOTE: To pair a Schlage CTE and Credential Reader follow these steps

  - Press and Release the **Schlage** Button one (1) time, then
  - Press and Release the **FDR** button two (2) times
  - The Credential Reader will blink AMBER three (3) times to indicate successful pairing.
Frequently Asked Questions

1. How can I determine the local Wi-Fi network settings?
   - Consult with the local property IT responsible person
   - Use a Mobile Phone to try to connect and verify the local Wi-Fi network

2. Will ENGAGE™ work with 5.0GHz network routers?
   - ENGAGE™ requires 2.4 GHz 802.11 b/g Wi-Fi and is not compatible with 5.0 GHz routers.

3. 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 will support standard Wi-Fi data rates and will always connect with the local Wi-Fi as necessary.

4. 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 50 feet, for a Line-Of-Sight connection.
   - For all ENGAGE™ Mobile application Bluetooth communications, the administrator should be as close as possible to the device – a few feet.
   - Bluetooth communication through walls and doors will significantly reduce communication range.
   - You will know you are within programming range when the ENGAGE™ Mobile application successfully connects with the nearby device AND the device LED is blinking.
   - BEST PRACTICE is to be as close as possible to the device when trying to connect with the ENGAGE™ Mobile application.

5. What are the different ENGAGE™ Team Member Capabilities?
   - See the table in Appendix A

6. Do Property "Team Member" invitations Expire?
   - When invitations are not confirmed by email, they will expire in less than a week
   - Resend of invitations is possible for expired invitations, any time
   - Invitations and Team Members can be deleted at any time
7. How do I know the Schlage MT20W is working?
   ▪ When ready and communicating on a Wi-Fi network, the Schlage MT20W LED will be solid BLUE
   ▪ If not Commissioned the LED will be solid RED after booting up
   ▪ The Schlage MT20W will Boot Up upon power application
     - On Power up, the RED LED will flash and beep
     - The BLUE LED will begin flashing for a few seconds
     - This is indicating Wi-Fi communications during connection to the local Wi-Fi
     - The BLUE LED will turn solid BLUE when ready for enrollments/programming

8. 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

9. What happens when a device battery gets low?
   ▪ All battery enabled devices will provide local feedback to the user at the door when the batteries are low. Low Battery status will cause the lock to provide a “Nuisance Delay” LED display before allowing access. This delay is about 3 seconds with flashing RED LED followed by the normal Access Granted Green LED.
   ▪ Nuisance Delay will be provided for low battery for up to 500 operations or about two weeks of normal use.
   ▪ Devices will enter “Critical Battery” mode after the “Nuisance delay” warning is ignored for a significant time.
   ▪ Devices in critical battery mode will not operate normally or allow access without a mechanical key or using the Jump Start feature on Schlage Control™ devices.
   ▪ Schlage NDE and LE devices will have 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.

10. What is a Nuisance Delay?
    ▪ A Nuisance Delay, is a delayed access at a door with a battery-operated device. The Nuisance delay happens any time a valid credential is presented to a device with Low Batteries.
    ▪ Nuisance Delay is provided when the device batteries are nearing depletion. The delayed access is intended for the user to report back to the Site Administrator that the device needs attention.
    ▪ Nuisance Delay will be provided for up to 2 weeks of normal operation before “Critical” battery level is reached or approximately 500 normal access attempts.
    ▪ Battery operated devices will begin providing the Nuisance Delay when the batteries are at the following voltage levels or lower:
      - Schlage Control™ = +4.60Vdc
      - Schlage NDE and LE = +4.40Vdc
    ▪ When the Nuisance Delay is ignored long enough, the device will transition into “Critical” battery mode and stop normal operation.
11. **What is Critical Battery Mode?**
   - Critical Battery mode is provided when the device batteries are completely depleted.
   - Devices in Critical Battery Mode will have a solid RED LED under the battery cover. This is intended to signal that the device needs attention for as long as possible.
     - Schlage Control™: Outside LED will be solid RED to indicate Critical battery.
     - Schlage NDE: LED under Battery Cover will be solid RED to indicate Critical battery.
     - Schlage LE: Outside LED will be solid RED to indicate Critical battery.
   - No normal lock operations are possible in Critical Battery Mode.
   - Jump Start for Schlage Control™ or keyed access will be required for battery replacements when a device is in “Critical Battery” mode.

12. **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.

13. **Why use a Software Alliance Member (SAM) Managed Account?**
   - Software Alliance Member (SAM) Partners may provide additional product and system functionality with features not available with ENGAGE™.
   - If using a Software Alliance Member (SAM) to manage Access Control, please consult with them before registering for a Partner Managed Account in the ENGAGE™ Web application.

14. **Can I change a ENGAGE™ managed account to a SAM account?**
   - YES - Switching devices from an ENGAGE™ Managed account to a Software Alliance Member (SAM) Managed account would require:
     - All devices to be deleted from the original ENGAGE™ Managed account.
     - All devices must be Factory Default Reset (FDR).
     - All devices will require commissioning into the new SAM account.

15. **What concerns are there with No-Tour?**
   - No-Tour credentials are limited by the number of devices (doors) that can be programmed onto a credential. 11 doors maximum.
   - For temporary access (Maintenance) property 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.
   - Properties planning the use of No-Tour should enroll and commission the MT20W before any other devices are commissioned, as BEST PRACTICE.
     - Commissioning of a MT20W tells ENGAGE™ that the property will be a No-Tour property and to enable the feature in all newly commissioned devices.
- **WARNING:** Any device commissioned prior to the MT20W, will be required to have be sync’d (door file updated) *again* before the No-Tour feature can be used.
- Devices enrolled before the MT20W will not be No-Tour capable until they are sync’d (Door File updated).
  - A credential can ONLY carry up to a maximum of 11 door assignments for No-Tour programming.
  - The total number of door assignments possible on a credential cannot exceed 11 doors total.
  - 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
  - BEST PRACTICE: Disable all Proximity Credentials on Schlage NDE, LE, and CTE devices when using No-Tour, for improved battery life and credential read performance

16. **What concerns are there with Schlage Control™ devices and Schedules?**
   - WARNING: When Assigning User Schedules on Schlage Control™ devices, be advised, that users exiting a room (outside their programmed schedule) with a Schlage Control™ deadbolt installed will not be able to relock the deadbolt after exiting because the lock will deny their credential as outside their scheduled access time(s).

17. **Why do ENGAGE™ Web application credential searches fail?**
   - The search for a badge (or credential) requires that the badge be initially enrolled using the MT20W enrollment reader
   - Credentials enrolled through a lock (at a door) or using the MT20 credential reader (Prox only) will not have a Badge ID and will not be found using the ENGAGE™ Web application Badge Search utility
## APPENDIX A – Property Role Assignment and Capabilities

Administrator – Manager – Operator

<table>
<thead>
<tr>
<th><strong>ENGAGE™ Feature and Role Assignment</strong></th>
<th>Administrator</th>
<th>Manager</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Roles per property account</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access Multiple property accounts</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Default role for new accounts</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile application Access</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web application Access</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Manage property information</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite users as Administrators</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite users as Manager</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite users as Operator</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Manage Invited users as Administrator</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Invited users as Manager</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Invited users as Operator</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Assign users as Administrator</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign users as Manager</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign users as Operator</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Delete Property Administrators</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Property Managers</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Property Operators</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Commission Devices</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Manage Devices</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Delete Devices</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage People</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Connect to Devices</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sync - Update Door Files</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Update Firmware</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Update from Server</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Run Diagnostics</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Get Audits</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View Wi-Fi Settings</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Change Wi-Fi settings</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View Audits / Alerts</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B – ENGAGE™ Training Videos

Videos on YouTube

Training Videos for ENGAGE™ can be accessed on the following YouTube channel:

There are many videos for review when necessary or just when you are curious about an operation or feature.

Videos on “Schlage Electronics How-To” mobile application

Allegion has many videos available for your mobile device to help with all the ENGAGE™ features and options available.

Download the Schlage “Schlage Electronics How-To” for either iOS or Android mobile devices from their familiar download sites (App Store and Google Play) to have them readily available when needed.

- Get the ENGAGE™ mobile app from the iTunes App Store (iOS)
- Get the ENGAGE™ mobile app from the Google Play Store (Android)

Search for “Schlage Electronics how-to” to download the mobile application

NOTE: You can provide Allegion feedback, email documents and request support from within the Schlage How-To-Electronics application.
APPENDIX C – ENGAGE™ Credentials

ENGAGE™ Credential Functions

- **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 lock.
    - Schlage Control™ does not support Toggle credentials. If a Toggle credential is programmed into a Schlage Control™, the lock will engage the thumb turn for the defined relock delay period.

- **Freeze**
  - Freezes the lock in its current state (locked or unlocked).
  - Lock remains frozen until a Freeze credential is presented again.
  - The Freeze credential used to “unfreeze” a lock can be the same credential or a different Freeze credential

- **One Time Use**
  - Allows only one attempt with Normal Access granted
  - Schlage Control™ does not support One Time Use credentials and will deny access anytime a One Time Use credential presented

- **Pass Through**
  - Unlocks a lock momentarily
  - Gains access to a lock in Freeze and Lock Down states
  - Gains access during scheduled Holiday lockouts
  - Will attempt 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 will 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