About this document:

- This document provides a basic product information OVERVIEW and functional descriptions 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 instructions.
- 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™ = 6.1.3</td>
<td>Schlage MT20W = 39.02.00</td>
</tr>
<tr>
<td></td>
<td>Schlage Control™= 03.06.07</td>
</tr>
<tr>
<td></td>
<td>Schlage NDE = 02.12.58</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile Application Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Android = 3.3.12</td>
<td>Schlage LE = 01.07.58</td>
</tr>
<tr>
<td>iOS = 2.3.2</td>
<td>Schlage CTE = 01.03.02</td>
</tr>
<tr>
<td></td>
<td>Schlage MT11 / MT15 = 20.04.00</td>
</tr>
<tr>
<td>REVISION</td>
<td>DATE</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>SES20171127A</td>
<td>11/28/2017</td>
</tr>
<tr>
<td>SES20171127B</td>
<td>08/01/2018</td>
</tr>
<tr>
<td>SES20171127C</td>
<td>08/15/2018</td>
</tr>
<tr>
<td>SES20171127D</td>
<td>12/07/2018</td>
</tr>
</tbody>
</table>
Table of Contents

Introduction to ENGAGE™ Access Control ................................................................. 7
  ENGAGE™ Managed properties ............................................................................. 8
  Software Alliance Member Managed properties .................................................. 8
  System Management using Web browsers and Mobile devices ............................. 8
The ENGAGE™ Enabled Devices ............................................................................. 10
The ENGAGE™ WiFi Network Requirements ......................................................... 12
The ENGAGE™ Mobile Devices ............................................................................. 13
The ENGAGE™ Mobile Application Requirements ................................................. 13
The ENGAGE™ Web Application .......................................................................... 14
The ENGAGE™ Web Browser Requirements ........................................................ 14
The ENGAGE™ Mobile Application ..................................................................... 15
Property Management Options .............................................................................. 16
User Credentials and Construction Credentials ..................................................... 17
  User Credentials ................................................................................................. 17
  Construction Credentials and Construction Mode ................................................. 18
Configuration Cards ............................................................................................... 23
  When working with Schlage CTE Multi-Technology Readers (MT11-485, MT15-485) ... 23
  When working with the Schlage MT20W ............................................................ 24
No Tour Features .................................................................................................... 25
  No Tour Limitations ............................................................................................ 26
  No Tour Temporary Maintenance Access – Recommendations ......................... 27
  No Tour Resident Moves Out – Recommendations ............................................ 30
Initial Account Setup .............................................................................................. 31
Creating an ENGAGE™ Account .......................................................................... 31
Account Team Members ......................................................................................... 36
  Assigning Team Members ................................................................................. 37
  VERIFY SUCCESS ............................................................................................... 38
  Verifying the Invitation Email Address (resend) ................................................. 38
Schedules Overview ............................................................................................... 40
  User Schedules ................................................................................................. 40
  Device Schedules .............................................................................................. 40
  Holiday Schedules ............................................................................................ 40
Creating Device and User Schedules ........................................................................ 41
Creating Holiday Schedules .................................................................................. 41
Creating Device and User Schedules ........................................................................ 41
Property Wide Default Device Settings ................................................................. 46
  Adjusting individual Device Settings ................................................................. 54
Searching for Credential Owners .................................................................................. 201
Resident Moves Out ........................................................................................................ 202
Deleting Existing Access ................................................................................................. 203
Deleting a Credential ....................................................................................................... 204
Deleting Devices ............................................................................................................... 206
  Using the ENGAGE™ Web Application ....................................................................... 206
  Using the ENGAGE™ Mobile Application for device deletions ................................. 208
Replacing Credentials .................................................................................................... 210
Updating Device Firmware ............................................................................................. 215
  Device Firmware Updates - at the door using Bluetooth (BLE) communication .......... 216
  Device Firmware Updates – at the door using local WiFi network communication ...... 220
  Device firmware updates – at the door with no local WiFi network available .......... 224
Perform the following steps on the mobile device: ......................................................... 227
Completing the device Firmware updates after download .............................................. 228
Scheduled Firmware Updates – Schlage NDE, LE, and CTE ....................................... 230
Retrieving Audit Data from Devices ................................................................................ 233
  Using the ENGAGE Mobile Application .................................................................... 233
  Using Nightly WiFi Updates ......................................................................................... 236
Viewing Audit Information .............................................................................................. 237
  Using the ENGAGE™ Web Application ................................................................... 237
Master Credentials .......................................................................................................... 240
  Enable Master Credential Generation ........................................................................ 241
  Assign a Credential as MASTER ................................................................................. 242
  View and Delete Master Credentials ........................................................................... 246
Things to Remember ........................................................................................................ 249
Best Practices – System Set-up ....................................................................................... 249
Best Practices – Device Set-up ......................................................................................... 249
Schlage Control™ Smart locks ......................................................................................... 249
Schedules .......................................................................................................................... 250
Master Credentials .......................................................................................................... 250
Update ICONS ................................................................................................................ 250
Factory Default Reset ....................................................................................................... 252
Moving Devices Between ENGAGE™ Accounts ............................................................. 252
Dual Technology Credentials (Schlage NDE, LE, and CTE ONLY) ............................... 252
Troubleshooting ............................................................................................................... 253
All Devices – Diagnostic Audits ..................................................................................... 253
Inviting Team Members ................................................................................................. 253
Device Commissioning ............................................................ 253
Construction Mode ................................................................. 253
Schlage MT20W ................................................................. 254
Schlage MT20W would not connect to the WiFi Network .................................................. 254
Schlage Control™ - "Jump Start" Process ........................................ 254
   To Perform a Schlage Control™ “Jump Start” .................................. 254
Set Device Date and Time ........................................................ 255
Device Firmware Updates Overnight Not Performed ......................................................... 255
Schlage CTE and Credential Reader Stopped Working ...................................................... 255
Frequently Asked Questions ........................................................................... 256
1. How can I determine the local WiFi network settings? .................................................. 256
2. Does ENGAGE™ work with 5.0GHz network routers? .................................................. 256
3. What is the WiFi network “Mandatory Data Rate”? ....................................................... 256
4. What is the ENGAGE™ Mobile device Bluetooth communication range? ..................... 256
5. What are the different ENGAGE™ Team Member Capabilities? .................................... 256
6. Do Property "Team Member" invitations Expire? .............................................................. 257
7. How do I know the Schlage MT20W is working? .......................................................... 257
8. What are the Battery Life expectations of ENGAGE™ devices? ....................................... 257
9. What happens when a device battery gets low? ............................................................... 257
10. What is a Nuisance Delay? .................................................................................. 257
11. What is Critical Battery Mode? ........................................................................... 258
12. Can I use Lithium batteries? ................................................................................... 258
13. Why use a Software Alliance Member (SAM) Managed Account? ............................. 258
14. Can I change an ENGAGE™ managed account to a SAM account? ............................ 258
15. What concerns are there with No Tour? ................................................................... 259
16. What concerns are there with Schlage Control™ devices and Schedules? ....................... 259
17. Why do ENGAGE™ Web Application credential searches fail? .................................... 259
APPENDIX A – Property Role Assignment and Capabilities ............................................... 260
   Administrator – Manager – Operator Roles .................................................................. 260
APPENDIX B – ENGAGE™ Training Videos ................................................................... 261
   Videos on YouTube ................................................................................................. 261
   Videos on “Schlage Electronics How-To” mobile application ........................................ 261
APPENDIX C – ENGAGE™ Credentials ....................................................................... 262
   ENGAGE™ Credential Functions ............................................................................. 262
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 has the option to use the ENGAGE™ Web Application and its companion, the 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 is required to begin with an ENGAGE™ Account to enroll and initially configure system components no matter which Access Control solution is chosen.

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

**ENGAGE™ Managed** Property Administrators use both the **ENGAGE™ Web Application** and the **ENGAGE™ Mobile Application** 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 WiFi network connection(s)
   - Available with our WiFi capable devices
3. No Tour access rights updates delivered to the door via Smart credentials (read/write) when programmed on the MT20W enrollment reader

**Update 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 WiFi 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**

Send updates at the lock, anytime, with the ENGAGE mobile app. Available on Schlage Control™, LE, NDE and CTE.

**Automatic Daily Updates**

Connect locks to the WiFi network for automatic daily updates. Available on Schlage NDE, LE and CTE.

**No Tour via Smart Credentials**

Eliminate the need to visit the locks by using smart credentials to deliver updates to access rights. Available on Schlage Control™, LE, NDE and CTE.

**NOTE:** Schlage Control™ Smart devices do not include WiFi network connectivity and are NOT compatible with automatic daily updates.

Device sync updates are required anytime major system settings are enabled or changed, user access rights change, when door settings 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 WiFi network access
  • Communicates via local WiFi network and Bluetooth® Low Energy (BLE) connection
  • The MT20W credential enrollment reader connects to the local property WiFi 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 WiFi
  • 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 WiFi
- 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 WiFi
- 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.

**WARNING:** The ENGAGE™ Web Application and the CTE do not support keypad functionality. Wall readers with keypads (MTK11-485 and MTK15-485) cannot to be used with CTE.
The ENGAGE™ WiFi Network Requirements

ENGAGE™ uses the local WiFi network to enable many functions automatically for the Property Administrator when the device(s) are WiFi enabled.

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

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

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

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

- **Connect Data Rate:** 24Mbps or lower
  - IT professionals use this setting to force a minimum data rate that is required before the device can connect to the WiFi access point. Connect Data Rate setting is intended to improve WiFi network performance and not allow weak or slow data rate devices to connect.
  - Each WiFi network access point requires the Mandatory Connect Data Rate setting to be **24 Mbps** (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 WiFi network.
  - The network router Connect Data Rate default setting usually is “Auto” and may need to be adjusted.

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

- WiFi network security types supported:
  - **WPA2 (PEAP)**
    - WiFi SSID - Must be EXACT (case sensitive)
    - USERNAME
    - PASSWORD*
  - **WPA2**
    - WiFi SSID - Must be EXACT (case sensitive)
    - PASSWORD*
- **WEP**
  - WiFi 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 need a commercially available mobile phone or tablet to perform many mobile ENGAGE™ functions on 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 WiFi 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 Bluetooth (BLE) communication or standard (2.4 GHz 802.11 b/g) WiFi 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)

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 may 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>ENGAGETM Mobile</th>
<th>ENGAGETM 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.

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

An **ENGAGE™ Managed** Account provides these 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 provides these 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 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:

![User Credentials Diagram]

**NOTE:** The 9691T is a dual Proximity 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.

**NOTES:**

1. A Proximity credential provides a unique card serial number and facility code.
2. Smart cards provide a unique card serial number and facility code, however Smart cards can be written to and carry additional access and update information when used for No Tour.
3. Smart credentials must be used for No Tour applications.
4. Schlage Control™ Smart locks require Smart card technology and are not compatible with Proximity credentials.
5. 9651 - MIFARE Classic® Smart 1K byte and 9651T - MIFARE Classic Smart 1K byte thin key fobs are recommended. (highlighted above).
6. Multi-tech technology credentials like the 9691T are most useful when both technologies are used for common areas and access control throughout the property.

**13.56 MHz Smart Credentials**

<table>
<thead>
<tr>
<th>Model Number</th>
<th>9451</th>
<th>8420</th>
<th>9551</th>
<th>8520</th>
<th>8620</th>
<th>9651</th>
<th>9651T</th>
<th>9691T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Type</td>
<td>Clamshell</td>
<td>Clamshell</td>
<td>ISO-Glossy White</td>
<td>ISO-Glossy White</td>
<td>Keyfob</td>
<td>Keyfob</td>
<td>Thin Keyfob</td>
<td>Thin Keyfob</td>
</tr>
<tr>
<td>Memory Capacity: Application Sectors</td>
<td>8k bit / 1K byte: 16 sectors</td>
<td>2K byte</td>
<td>8k bit / 1K byte: 16 sectors</td>
<td>2K byte</td>
<td>2K byte</td>
<td>8k bit / 1K byte: 16 sectors</td>
<td>8k bit / 1K byte: 16 sectors</td>
<td>8k bit / 1K byte: 16 sectors</td>
</tr>
</tbody>
</table>
Construction Credentials and Construction Mode

Construction Credentials are used for temporary access before the locking devices are commissioned and programmed 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 momentarily engage the thumb turn on Schlage Control™, or provide a momentary unlocking and relocking on Schlage NDE, LE, and CTE devices.
- Each device in Construction Mode relocks 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 are 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 ResCardTrax™ Account CT8X4248 that is maintained internally by Allegion.
  - The CardTrax account MUST be referenced on Construction Credential orders for Schlage Control™ Smart locks.
- Schlage NDE, LE, and CTE devices 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 sets 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 beeps 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) are 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 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 blinks 5 times for Successful MASTER Construction Credential enrollment.
- Present the MASTER Credential again.
- The device LED illuminates 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 blinks 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 are now allowed Construction Mode access.

**Results:**

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

**WARNING:** Be sure to store the MASTER Construction credential in a safe place. It is 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 allows 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 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, 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 blinks 5 times for successful MASTER Construction Credential enrollment.
- Present the MASTER Credential again.
- The CTE STATUS LED and the wall mounted reader illuminates 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 blinks 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 are allowed Construction Mode access.
**WARNING**: Store the MASTER Construction credential in a safe place. It is 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 require Configuration Card programming to disable card technologies when desired. The MT20W, No Tour Enrollment Reader requires 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, present and hold the Configuration Card to the reader
  3. The reader acknowledges the Configuration Card by beeping 3 times, the LED flashes red with each beep.
  4. When the beep and LED sequence finishes, the configuration update to ignore Proximity card presentations is complete.

**NOTE:** Always re-sync Schlage CTE and Credential Reader after Configuration Card programming.

5. To re-sync the Schlage CTE and Reader:
   a. Press and release the Schlage button once.
   b. Press and release the FDR button, twice.
5. The RS485 LEDs flash when successfully sync’d.

Results:

- The Credential Reader no longer acknowledges 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 a **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 beeps three times and the LED is solid RED.
  - Be patient, the Schlage MT20W reset and restart. This process takes a minute to complete before the solid RED LED is displayed.

**NOTES:**

1. FDR does not affect the current firmware of the Schlage MT20W.
2. FDR does de-commission and erase the WiFi network settings of the Schlage MT20W.
3. FDR does 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.

The 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 screenshot below:

Important No Tour facts:

- No Tour Smart Credentials 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 programmed settings.
- Multiple devices included in a defined ENGAGE™ “Group” are 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 device.
- User Scheduled access assignments are commonly used to control individual door access that is limited to a day or days, time of day, or a specific maintenance schedule.
- While programming access, the status of each credential sector is displayed as:
  - **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 Property Administrators to save time and effort during daily operations, however the Property Administrator MUST be aware that proper door updates are dependent on the user visiting each door assigned with new or deleted access updates.

**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 does 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 at the door. A door the user fails to visit using No Tour programming after a credential replacement or an access deletion, still allows the old or lost credential access because the new lock access programming has not yet been performed.

- Credentials that have assigned door access deleted, remain as "Blocked" assignments in the credential sector.

**NOTE:** A blocked door is counted in the maximum door programming limit of 11 doors per credential.
• When the User credential access expires per a defined User 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 not to require more than 11 unique door access assignments when using No Tour functionality.

• When door assignments exceed 11, the Property Administrator is not able to use No Tour programming. The Property Administrator is required to manage access updates using the standard Sync process. All devices other than Schlage Control™ may enable nightly WiFi 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 is needed, and then use a pre-defined maintenance User Schedule to specify the specific “Time-Of-Day” access is to be allowed.

**NOTES:**

1. User Schedules MUST first be saved in ENGAGE™ and then each device must be sync’d before the new schedule is available at the door.
2. User Activation / Expiration settings are programmed on the credential and are 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 WiFi updates, or commission new devices to save the new “Maintenance Shift” schedule into each device.
• A new or updated User Schedule requires syncing before the newly defined Maintenance Shift is honored at the door.
Maintenance Shift Schedule

- When the sub-contractor needs maintenance access, the Property Administrator:
  o Programs a credential with the contractor’s name.
  o Sets Expiration for one (or more) days of access (as needed).
  o Selects the scheduled “Maintenance Shift” to limit the daily hours of access to be provided for only those doors assigned.

**NOTE:** A maximum of 11 doors can be assigned at one time using No Tour.
Set Expiration for Today to Limit Access

- When a 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 Administrator may follow one of these methods for credential reuse:

1. If a new resident is moving in at the same time an old resident is moving out, and their access rights are to be the SAME, the 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 is maintained for history and any new accesses resulting from this credential reuse, are reported with the new residents’ name.

2. If a credential is just being returned (not re-issued), follow these steps to take control of the returned credential, properly manage the ENGAGE™ property database, and to make the credential available for reuse and reprogramming:
   a. Change the name on the credential to “Unassigned” (or other).
   b. Set the User Expiration date to “Today”.
   c. Remove (delete) all access assignments currently assigned to the credential.
   d. Successfully program the credential with the Schlage MT20W.

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

There are two account types possible with ENGAGE™:

- An ENGAGE™ Software Alliance Member account managed by one of our Software Alliance Members (SAM), or
- 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](https://portal.allegionengage.com/signin) into your web browser.

- Select *Create Account.*

- Enter the requested information.
• **Email Address**: must be unique and not used at 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](image)

**NOTES:**

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

2. 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.

![Sign In](image)

• **Select Sign In.**

![Manage Sites](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 chose 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** disables 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 your **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 is 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 allows others to help the Property 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 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 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 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 the **Add Team Members** 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 canceled, and the 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 the ADVANCED tab.
- Select the My Team tab.
- Select the Manage button for the "Invited" Team Member.

- Verify the email address is correct for this Team Member.
• Select **Re-Send Invitation** to try again or **Delete Invitation** as desired.
Schedules Overview

The Property 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, 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 are 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 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 Schedule16.
Creating Device and User Schedules

The Property 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 DEVICES 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 scheduled Start and End times.
Device 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

- See that the new schedules are now listed on the User and Device Schedule screens.
NEXT STEPS:

- The above process defines the User and Device Schedules to be used for the ENGAGE™ managed property.

- Each schedule is now selectable for assignment to individual User(s) or Device(s) when performing those assignments.
  
  o See Assigning Lock Access and User Schedules for assignment of a User Schedules for a resident.

  o See Property Wide Default Device Settings and Adjusting Individual Device Settings for assignment of Device Schedules to a door.
Creating Holiday Schedules

The Property 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 then HOLIDAYS 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 Holidays schedule screen.

![Holidays Schedule Screen]

**NEXT STEPS:**

- The above process defines the Holiday Schedules to be used for the ENGAGE™ managed property.
- Each schedule is now 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 WiFi enabled devices before the Holiday Schedule is active.
Property Wide Default Device Settings

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

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

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

To view/edit Device Defaults:

- Log into the ENGAGE™ Web Application.
- Select ADVANCED 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 is 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.

![Schlage CTE Default Settings](image)

- 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.
- **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 is 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 save time when setting up their property.

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

BEST PRACTICE:

1. Determine if your property requires both Proximity and Smart card credentials.
   a. 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.
   a. Reader sensitivity may be set to HIGH or MAX when small format FOB credentials are used.

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

- Log into the ENGAGE™ Web Application.
- Select ADVANCED.
• 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 are programmed into the device. Subsequently, a Property Administrator may 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, then Devices tab.
- Select the device to update. In this example we chose the Copy Room.

**NOTE:** Devices MUST be commissioned before they are available, for additional device setting updates. See Commissioning and Setup 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 Control™ Lock Settings Tab

Schlage NDE Lock Settings Tab
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 have these options available.

Schlage NDE and LE Reader Settings Tab
• Make all necessary adjustments per your Property Administrator and property needs.
• Select Save.

VERIFY SUCCESS

• See the momentary Device updated. Message.

NEXT STEP(s):

This process sets the programming intentions for each device. After assigning device settings, the Property Administrator is required to perform the following steps before the door settings are honored.

• Sync all affected devices
  o Schlage NDE, LE or CTE device syncing is available via overnight WiFi network call-In
  o See Sync – Updating a Door File
  o 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.
Commissioning and Setup

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

IMPORTANT NOTES:
1. All devices are commissioned using the ENGAGE™ Mobile Application using Bluetooth communication. Commissioning is not performed with the ENGAGE™ Web Application.
2. The device must be “Out-Of-The-Box” or recently Factory Default Reset (FDR) to be available for selection and commissioning.
3. 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.

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

If the MT20W has already been commissioned at your site, skip to the next section: **Updating MT20W Firmware.** If you are starting with a new MT20W (out-of-the-box) or just after a successfully performed Factory Default Reset (FDR), continue:

- Ensure the Schlage MT20W is powered and has completed its boot-up process.
  - The Schlage MT20W LED is solid RED when ready.
- Log into the ENGAGE™ Mobile Application to view the **Devices** screen.
  - One of the following screens is presented.

**NOTE:** Android and iOS devices 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 it is available on the **All Devices** screen(s). The Schlage MT20W is the first device to be commissioned into the 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
- To continue, select the **MT20W** device type in the “Select a device type” screen below that you want to commission.
• 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 as shown below.

**NOTE:** New or recently Factory Default Reset Schlage MT20Ws within range are displayed.
• 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** in the top right-hand corner to continue.

• The **Please wait...** screen displays.
• Immediately followed by **Which data transfer method are you using?**

![Image of a screen displaying options for data transfer methods: USB (recommended) and Wi-Fi.]

• Select **USB (recommended)**.
• The **Preparing your device** screen displays.

![Image of a screen showing two devices connecting and text: Preparing your device.]

• After the device configuration is saved, the checkmark screen displays.
WARNING: Before using the MT20W to add credentials, you MUST complete the Desktop Application installation process below first.

- Click **Next** in the top right-hand corner to continue.
- The USB symbol with the **Send Link** button displays. Selecting the **Send link** button emails an ENGAGE PC Desktop Application link to the Administrator’s email.

- Select **Send Link**.
- The **Notice – Ok** screen displays.
• Select Ok.
• Select Exit in the top right-hand corner to continue.
• The All Devices screen displays showing the recently commissioned MT20W.

NOTE: Before using the MT20W, you MUST complete the MT20W setup by installing the ENGAGE USB PC Desktop Application.
Installing the ENGAGE PC Desktop Application

After the **Send Link** button is selected, the system sends a link to your email. Go to your email and follow the instructions.

- Check Email – look for this item in the System Administrator’s email.

![Allegion ENGAGE™ Desktop App Invitation](image)

- Open the email and select the Correct Operating System version for your PC.

![Engage Set Up](image)

- Select **Windows** or **macOS** operating system button.
- Navigate to the PC “Download” folder.
- Locate the Engage_Setup installation application.

![Engage Setup-1.0.0-win.exe](image)

- Run (Double-Click) the **Engage_Setup-X.x.x-win.exe** installation application to install it.

**NOTE:** PC Administration authority (permissions) are required.
• Observe the installation process where the next screens are immediately shown.

When the installation is successful, the following screens display on the desktop.

**Reader Detected**

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

**Reader Connected**

**NOTE:** Do NOT close this application.
Verifying and Updating MT20W Firmware

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

**NOTE:** For USB communication, the MT20W firmware must be at version **39.02.00** or higher.

Using the Desktop Application

To verify the current MT20W firmware revision:

- Open the ENGAGE Web Application on your desktop.
- Navigate to the **ADVANCED** tab.
- Select **Firmware**.
- Locate the MT20W device in the Device List.
- View the MT20W **Current Firmware Version** versus the **Latest Firmware Version**.

**NOTE:** In this case the MT20W firmware is not at the latest revision.

- If the current firmware version is earlier than version 39.02.00, you must update the firmware using the mobile application to enable USB communication.

Using the Mobile Application

This process assumes that there is a WiFi network already saved and available for use by the mobile application.

Verify the MT20W has latest Firmware by following steps 1 through 3 below:
1. Select MT20W device

2. Select Update Firmware

3. Is Firmware Current?

- When the current firmware version is earlier than version 39.02.00, you must update the firmware when using USB communication.

- Click on the Update button from the mobile app to update the firmware.

- The Initiating firmware download screen displays.

- The firmware is downloaded to the MT20W.
• The **Installing firmware** screen displays.

![Installing firmware screen](image1)

• Click **Finish**.

• The blank **In Range** mobile display is shown.

![Blank In Range mobile display](image2)

• The MT20W automatically finishes its firmware installation process and reboots. Be patient, this may take a few minutes. Wait for all LED flashing to stop.

• The boot-up process is complete and the MT20W is communicating when a solid BLUE LED displays.

![MT20W boot-up process complete](image3)
• The mobile app screen does not update again until the User swipes down to refresh the screen or navigates away and comes back to the All devices or In Range screen.
Setting and Selecting USB Mode

*Connected to MT20W – Toggle from WiFi to USB Communication Mode*

1. Select Settings
2. Select Comm Mode
3. Select USB Mode
Usage – Normal Operation

MT20W light interpretation remains the same.

- Solid blue means the MT20W is communicating; Solid Red, 1 Green Blink, 3 green blinks…

The Desktop Application acts as a transmitter/receiver between the MT20W and the ENGAGE Web Application.

On opening the ENGAGE Desktop Application, the information on the screen instructs you to connect the MT20W to your PC to get started (Figure 1).

**Figure 1: MT20W Direct**

Once you plug the MT20W into the USB port on the PC, the ENGAGE Desktop Application detects the reader and begins communication (Figure 2 & 3).

**NOTE:** The ENGAGE Application does not start automatically when the MT20W is first connected. When using USB communication, the ENGAGE Desktop Application must be running.

After power up, the MT20W must go through a boot up process BEFORE a connection is accomplished. Be patient, this may take a few seconds.

**Figure 2: Reader Detected**
After the connection is established, the serial number and firmware version of the ENGAGE Desktop Application displays on the screen (Figure 3).

**Figure 3: Reader Connected**

![Reader Connected](image)

**NOTE:** If you close the ENGAGE Desktop Application on the PC by clicking on the ‘X’ in the upper right-hand corner, you must restart it again before USB communication is available. The MT20W shows a solid RED LED in this case.

The ENGAGE Icon symbol ![Icon](image) shows in your PC system tray anytime the ENGAGE Application is running.

If any error occurs during the communication, an error message along with the error code displays on the screen along with a notification (Figure 4).

**Figure 4: Error Detected**

![Error Detected](image)
When the reader is un-plugged from the Desktop/System, the Application screen shows that the reader is disconnected (Figure 5).

**Figure 5: Reader Disconnected**
Setting and Selecting WiFi Mode (Optional)

If you intend to use WiFi instead of USB Direct Mode, and the MT20W has already been commissioned in an earlier process, perform the following steps to enable WiFi.

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

- If there are no saved WiFi networks, a new network MUST be added. (see the Adding a new WiFi Network section).
- When a Saved Network is available, the Property Administrator may select that WiFi network for quick and accurate data entry.
- Ensure the Schlage MT20W is in signal range of the local WiFi network access point.

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

Connected to MT20W – Toggle from USB to WiFi Communication Mode

1. Select Settings

2. Select Comm Mode

3. Select WiFi Mode
Next the Property Administrator selects the local WiFi network for the device. There are one of two options available; No Saved or Saved Networks.

*Adding a new WiFi Network*

Initially the Property Administrator MUST select **Add a new network** to enter the WiFi network Security Settings. See the next section when **Selecting a Saved Network**.
• Enter the **WiFi SSID**.
  o This is the name of the local wireless local area network
  o This entry must be EXACT and is CASE SENSITIVE
• Select the **WiFi Security** used by the local area wireless network
  o OPEN, WPA2, WPA2 (PEAP), or WEP

**NOTE:** Depending on the WiFi network security chosen, you may need to enter different information.

In this case we chose **WiFi 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 WiFi network settings can now be programmed into the Schlage MT20W and the Schlage MT20W connects to the local WiFi 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.

![Connecting to Wi-Fi](image)

**WARNING:** If the Schlage MT20W does not provide a solid Blue LED and tries to reconnect but fails, the WiFi network settings are not entered correctly or the local WiFi network is not present.

• **Recheck the WiFi 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 WiFi network connection requirements.

• **Select the Press if Solid Blue** (Connected) Blue bar to continue.
• 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 illuminates solid BLUE after power is applied and boot-up is completed indicating successful connection and communication to the local WiFi Network.
NOTES:

1. The Schlage MT20W solid BLUE “Connected” LED display indicates the Schlage MT20W is connected to the local wireless WiFi network and communicating properly.

2. The Schlage MT20W flashes BLUE quickly while trying to connect with the local WiFi network.

3. When the local WiFi network connection fails, the Schlage MT20W displays a solid RED LED.

4. When the local WiFi network is not available (failed or down for maintenance), the Schlage MT20W automatically retries to reconnect to the local WiFi network every few minutes.

Selecting a Saved Network

- Instead of selecting Add a new network, the Property Administrator may select the appropriate (locally available) WiFi 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 resets and tries to connect to the local WiFi network using the saved network settings. Be patient, wait a few moments while the Schlage MT20W tries to connect to the local WiFi (fast Blue LED blinking) and then provides a solid Blue LED indicating it has successfully connected to the local WiFi 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 WiFi network settings are not correct or the local WiFi network is not present.

- **Recheck or reenter the WiFi 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 WiFi network connection requirements are verified and can be re-entered as a saved network.
• Acknowledge the Setup Complete message and select Exit.
Device Commissioning

Schlage Control™ Smart Lock Commissioning

- Log into the ENGAGE™ Mobile Application while in close proximity to the Schlage Control™ Smart lock being 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 and selectable 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 screenshots is presented.

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

NOTE: The display shows that no devices are commissioned into the property yet. Each device in the system MUST be commissioned before it is shown on the All Devices screen(s).
• The next step is to select the nearby Schlage Control™ Smart lock being commissioned.
  o For iOS mobile devices
    ▪ On the screen above, select the + sign in the upper right-hand corner
  o 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 Control Lock type in the “Select a device type” screen to continue.

![Select a device type](image)

• The next screen displays 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 several devices.
• Answer the question: “Do you want to use the “currently defined” default Control Lock settings for this property?”

NOTES:

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 displayed.

NOTES:

1. All nearby Schlage Control™ Smart locks with RETRACTED deadbolt and available for commissioning are displayed.

2. The 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 E100000001B846.

• Verify that the selected device LED is flashing RED.

  then...

  Select a Control Lock

  Schlage Lock
  E100000001B846

  Schlage Lock
  E100000001EAD9

• Select YES to continue.

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

  Is the light blinking on the device?
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 and selectable for commissioning.
- Log into the ENGAGE™ Mobile Application to view the Devices Screen. Depending on your mobile device, one of the following screens is presented.

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

![iOS Device Menu](image1)

**NOTE:** This display shows that no devices are commissioned into the property yet. Your display may be different, this screen displays each device you have already commissioned into the property.
- The next step is to select the nearby Schlage NDE device being 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 to continue.

• The next screen displays 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.

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

NOTES:

1. Property Administrators can use the currently defined default settings for the 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 “Advertises” 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.
NOTES: If no device information is displayed:
1. Be sure the Schlage NDE battery cover is properly installed. Schlage NDE does not “Advertise” when the battery cover is not 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.

Then...

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

NOTE: Only the Schlage NDE with a recent inside lever turn is 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 on the screen above.

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

- Ensure the Door is physically closed and then select **NEXT**.
NOTES:

1. The NEXT step in the commissioning process ENABLES the WiFi network connection capabilities of the Schlage NDE lock.

2. Administrators may also elect to skip setup of the WiFi network when a network is not available or not needed by selecting Skip on the screen above.

3. The Property Administrator may ENABLE or edit a WiFi network connection setting at any time using the mobile application.

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

NOTE: See Enabling WiFi Network Connection Settings for setup requirements when a WiFi 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 screens is presented.

**NOTE:** Android and iOS devices 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 displays 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?”

NOTES:

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 “Advertises” 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.
**NOTES:** If no device information is displayed:

1. Be sure the Schlage LE battery cover is properly installed.
   - LE does not “Advertise” when the battery cover is not installed properly.
2. Be sure the Schlage LE is Out-Of-The-Box or recently Factory Default Reset.
   - In FDR mode the Schlage LE beeps with each inside lever turn and begins two (2) minutes of advertising for the commissioning process.
3. Be sure the mobile device has Bluetooth turned ON.
4. Be sure the Schlage LE is 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 displays 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?”

**NOTES:**

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.

**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) are displayed.

- Select the desired device for commissioning. In this case we chose, **Schlage Lock LE serial number F10000000F1232EF**.
• Select **Yes**, after verifying the Schlage LE lock LED is flashing.

• 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 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 ENABLES the WiFi network connection capabilities of the Schlage LE lock. Administrators may also elect to skip setup of the WiFi network when a WiFi network is not available or not needed by selecting Skip on the screen above.

**NOTE:** The Property Administrator may ENABLE or edit a WiFi network connection setting at any time using the mobile application.

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

**NOTE:** See Enabling WiFi Network Connection Settings for setup requirements when a WiFi 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 indicates 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 have slightly different screens, however the functions are the same. Depending on your mobile device, one of the following screens is presented.

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

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

- 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 displays 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?**”

**NOTES:**

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 instructions to enable Bluetooth “Advertising” for the desired CTE device. Press and release the Schlage button inside the CTE enclosure.

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

• Select **Next**.
Then...

- Select the **CTE** to be commissioned from the list.

**NOTES:** If no device is displayed, check for the following conditions:

1. Be sure the CTE is Out-Of-The-Box or recently Factory Default Reset (FDR).
   - The FDR Mode LED must be ON.
2. Be sure you are in wireless Bluetooth (BLE) communication range of the CTE.
3. Be sure the CTE is “Advertising” via Bluetooth (BLE).
4. Select **BACK** to return to the Device Type selection screen and **Try Again**.

- Answer the displayed question to verify the CTE being commissioned.
- Select Yes.

then...

then...

- Enter a Name for the CTE (required). In this case we chose Main Entrance.
- Select Next.
- Move through these screens to choose the locking device and any auxiliary equipment that this CTE is required to control.
• Select the desired WiFi network connection setup. In this case we chose Skip.
  o Select Skip to use the CTE without a WiFi connection or to setup the WiFi network later.
  ▪ If you intend to take advantage of the CTE WiFi nightly call-in network capabilities, see Sync – Overnight – Schlage NDE, LE, and CTE.
  ▪ WiFi settings can be updated after this initial setup is completed by connecting to the device and enabling the WiFi settings.
  o Select a displayed Saved WiFi Network, if the WiFi is locally available at the door opening. In this case there are two previously saved WiFi networks available.
  o Select Add a new network, initially or when there are no Saved WiFi networks available locally at the door.
Select Finish to complete the CTE initial setup and return to the Connect screen.

VERIFY SUCCESS

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

NOTES:

1. If you are a No Tour property, it is recommended that unnecessary and unused proximity technology credential types be disabled.
2. Disabling the proximity technology credentials provides for improved battery life and quicker reader and access response. The device does not search for the unused credential technology (Proximity) each time a credential is presented. The device no longer "looks" for proximity cards when a credential is presented.

3. 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 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 entered **New User**.
  - **Email** (optional).
- Enable **ADA** (American Disabilities Act) operation if the resident requires additional time to access doors.
IMPORTANT NOTES:

1. ADA operation does not apply to Schlage Control™ devices.
2. HINT: When modified access timing is needed for a Schlage Control™ deadbolt, adjust the standard Relock Delay settings accordingly.
3. When the ADA setting is moved to ON, an ADA USER is allowed modified access times at the Schlage NDE, LE, and CTE doors to which they are assigned.
4. 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.
5. Sync is required to update new or edited ADA Relock settings into a commissioned device.
6. 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:

1. This process enrolls a User into ENGAGE to make them available for Credential and Access Assignments.

2. Later, the Property Administrator is required to Assign Credentials and Add New Access and User Schedules for this User.

3. 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 a 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, 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 is displayed in the ENGAGE™ Web Application for easy reference.

2. **Proximity** credential enrollments are provided using the ENGAGE™ Web Application and a Schlage MT20 credential reader.

3. Credential enrollments can also 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 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 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 with the (ENGAGE™ Web Application)

- Log into the ENGAGE™ Web Application.
  - Ensure the MT20W is properly powered and commissioned. The LED is solid BLUE when connected and ready for use when using either USB or WiFi communication mode.

**NOTES:**

1. If you are using USB communication mode and the MT20W LED is solid RED, then the ENGAGE Desktop Application is not running.
2. If you are using WiFi communication mode and the MT20W LED is solid RED, then the WiFi connection is not available.

- 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)

![Add Credential](image)

- Present the new credential to the MT20W and wait a few seconds. The MT20W turns GREEN and beeps 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 chose 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.
VERIFY SUCCESS

- See the **Credential Assigned.** momentary confirmation.

![Credential Assigned](image)

- 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.

**NOTES:**

1. There is no need for the ENGAGE Web Application to be running.
2. USB power or a valid WiFi network connection is required depending on how you commissioned the MT20W.
3. Proper MT20W communication is indicated by a solid BLUE LED on the MT20W.

- Plug your commissioned Schlage MT20W into your desktop PC with the ENGAGE Desktop Application running. Verify proper communication. When using WiFi communication mode, only a USB power source and network connectivity is required.

**NOTE:** Wait a few seconds after power application while the MT20W starts (boots up). When ready, the MT20W LED is solid BLUE indicating proper communication.

- Present a new Smart credential to the MT20W and wait a few seconds. The MT20W turns GREEN and beeps 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, signified with a GREEN LED and a beep. In this example we added credentials #18740, #1965 and #5715.

**NOTE:** Keep these enrolled credentials in 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 pick any predefined User from the list.
• Select **Add Credential**.

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

**NOTE:** All credentials enrolled are 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 possible to enroll a credential using the ENGAGE™ Mobile Application and an installed lock.

- 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™ is not 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) do not have the typical credential # (ink stamp) listed, as seen with Schlage MT20W enrolled credentials. Also, credentials enrolled with this method are not 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 and the **specific** user to be assigned a new credential.

**NOTE:** In this case we chose **User, New** to be assigned a new credential.

- **Select** the user being assigned a credential.
• Select the **Credentials** Menu (shows no credentials assigned).

• Select the + sign to identify devices in-range that can be used as an enrollment reader. In this case five (5) devices are in-range. In this example, we use the lock named **Storage** as our enrollment reader.
• Select a specific device from the **Available Enrollment Readers** list. In this case we chose **Storage**.

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

• Present the new credential to the nearby **Storage** device.

**NOTE:** When the device reads the credential, the ENGAGE™ Mobile Application displays a credential "**Value**" with asterisks *******.
• If no credential is presented, the process "Times 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 USERS Menu and Users tab and then pick the NEW USER.
• View the current credential assignments for New User and Credentials.
WARNING: Credentials assigned using the ENGAGE™ Mobile Application and commissioned ENGAGE™ device method (described here) do not have the typical credential # (ink stamp) listed as seen with MT20W enrolled credentials (e.g. Credential 1802 example below).

Credentials enrolled with this method are not 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 is treated as a single assignment when programming the user credential and requires only one credential sector for access to all doors defined in the Group.

IMPORTANT NOTES:

1. Devices must be commissioned before they are available for inclusion into a Device Group.
2. Device Groups should be very static and not require updates frequently.
   - Any updates to a Device Group require Sync of each affected device before the group update is valid.
3. Property Administrators should define any Device Groups before making user access assignments for streamlined access assignment.
4. 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.

- This initial screen displays.
• Select **Add New Group**.

![Add New Device Group]

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

- **Enter a description** of the Group so that others can easily recognize the Group purpose. For this example, we entered:
  - 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 is provided.
NOTE: A device that is already assigned into another Device Group is not available here for selection.

- Select the Unassigned Device(s) you would like to be included in this Device Group. In this case we selected **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:**
1. Initially, all commissioned and unassigned devices are displayed in the **Unassigned Devices** field and are available for selection.
2. Devices already assigned to another Device Group are not listed for selection here.

- Select **Save**.

**VERIFY SUCCESS**
- See the momentary **Devices for group updated successfully** message and the **Pool Access for Residents** Device Group now lists the two Assigned Devices; **Pool 142** and **Pool 286**.
NEXT STEPS:

1. A device Sync with the ENGAGE™ mobile Application must be performed for each device that is added or deleted from a newly defined Device Group.
   a. Any User credentials programmed for this group do not allow access until a device Sync is successfully completed.
   b. Any device (lock) deleted from a Device Group allows access until a device Sync is successfully completed to remove that lock from the Device Group.

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

2. This newly defined Device Group (with the two defined lock assignments) is now 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 Smart credential already assigned and the lock(s) commissioned in the account with all desired User Schedules defined.

- Open the ENGAGE™ Web Application.
- Select USERS tab.
- Select User, New you want to assign access.

**WARNING:** If the User has no Credentials assigned, lock access assignments are not possible. The User MUST have at least one Smart credential assignment to 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 User.
NOTE: The Assign To: Device (individual) 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 chose Apt 5D2B, Garage 141B, Laundry 137, Lobby 83, and Storage.

NOTE: The Credential Sector Usage screen fills 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 access Expiration date now, if desired.

NOTES:

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 are 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.

Check the “Box” by each defined Device Group where access is desired.

- In this case we chose the group Pool Access for Residents, which has Pool 286 and Pool 142 pre-defined in the group.

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

**NOTE:** A Device Group only takes 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 updated **Current Access for New User** screen for the selected **User, New** with seven (7) assigned doors.

![Image of ENGAGE™ software interface showing Users and Current Access for New User screens]

NEXT STEPS:

1. This process assigns a User access rights to individual doors in ENGAGE™. The Property Administrator is still required to perform credential programming for No Tour updates and/or sync before updates are honored at the door.

2. The Property Administrator must now obtain the identified Smart credential and program the newly assigned access rights to it.
   a. In this case we need Smart **Credential 22904** to proceed.

3. Select **Update** in the Credentials screen above with the Smart credential in hand.
• Follow the instruction provided on screen, then Select **Next**.

• Select **Finish** on the screen above.
NOTE: 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 also captures and returns the latest device Audits for review.

The Property Administrator knows 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:

1. Device SYNC mobile updates at the door use the mobile device WiFi (or data) network for an internet connection and communication with ENGAGE™.
2. Mobile devices use Bluetooth (BLE) for communication to the nearby device(s).
3. 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.
4. Door Settings and Device or User Schedule updates MUST be accomplished using a Device SYNC update or using nightly WiFi call-in when available.
5. No Tour credential programming of a device does not update device settings or any type of schedules.

BEST PRACTICE: Turn OFF the device local WiFi 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 displays.

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

- **Select** the device to be updated (Pool 142).
- **Select** Sync to begin the update process.
NOTE: The selected device begins 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 1 removed for **Pool 142 device**.
Sync – Overnight – Schlage NDE, LE, and CTE

Overview

When the Schlage NDE, LE, and CTE device WiFi network settings are entered properly and the device can connect with the local WiFi network, the device automatically syncs and performs “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 WiFi communication.

Enable nightly WiFi updates (Sync)

To enable nightly sync (Door File and Get Audit updates) for Schlage NDE, LE or CTE devices, it is necessary to properly configure the device WiFi network settings for the local WiFi 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 WiFi 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 WiFi menu (under GENERAL).

• Slide the WiFi button to enable and display the WiFi setup menu.

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

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

**VERIFY SUCCESS**

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

• **Select the WiFi menu.**
NOTE: This example is for WPA2 (PEAP) security. Username and Passwords are unique for your WiFi network security.

- Select **Test WiFi Connection** menu.

- Select **Test WiFi** to initiate the test.

**NOTE:** The device LED flashes AMBER while testing the WiFi network connection.
• Acknowledge the **Success** message.

**NOTES:**

1. The selected device now has its WiFi network connection verified and it calls 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 now report WiFi information like connection strength and connection issues for the Property Administrator.
4. Should the WiFi test fail, this message displays.
**WARNING:** If the WiFi network connection fails, recheck your WiFi network SSID and Security settings, then try again.

HINT: You can also check the local WiFi network settings by using your mobile phone to connect to the WiFi network while nearby the device.

**To select a previously saved WiFi network**

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

**WARNING:**
- A saved WiFi 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 WiFi network that is local and available at the installed device location.
- Verify the saved connection using the available **Test WiFi Connection** option(s).
- If not successful, verify the WiFi settings using your mobile device and try again.

- Select **Show Saved Network** menu (below).

![Image of WiFi settings menu](image)

Then...

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

- Pick a saved (local) WiFi network from the list provided. In this case we chose the `610baLWLAN` Saved Network.
WARNINGS:
- Ensure you pick the saved WiFi network that is local to the device being set up and in range for good communication.
- A saved network may not be locally available at the installed device physical location.
- Network settings can be saved from different WiFi access points across your property.
- 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 are unique for your WiFi network security.

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

- See that the new WiFi SSID (610baLWLAN) is now listed on the Devices screen.
- Select the WiFi menu.

**NOTE:** This example is for WPA2 (PEAP) security. Username and Passwords are unique for your WiFi network security.
• Select **Test WiFi Connection** menu.

![Image of Test WiFi Connection menu]

• Select **Test WiFi** to initiate the test.

**NOTE:** The device LED flashes AMBER while testing the WiFi network connection.

![Image of Test WiFi with AMBER LED]

• Acknowledge the **Success** message.

![Image of Success message]

NOTE: The selected device now has its WiFi network connection verified and it calls in every night to sync and apply any Door File updates and to Get Audits. In addition, this device can be enabled for automated firmware updates.

- Should the WiFi test fail, this message is displayed:

![](image)

**WARNING:** If the WiFi network connection fails, recheck your WiFi network SSID and Security settings, then try again.

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

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.

Initial Power up:

Whenever a new Schlage MT20W or a recently reset Schlage MT20W is powered up, it goes through a boot-up process. Wait a few seconds for the boot-up process to complete. The Schlage MT20W beeps, and the LED is 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 first minute after power is applied and after the Schlage MT20W boot up process has completed.

IMPORTANT NOTES:

1. To indicate the successful completion of a Factory Default Reset (FDR), the Schlage MT20W beeps three times and the LED is solid RED.
2. FDR does not affect the current firmware of the Schlage MT20W.
3. FDR de-commissions and erases the WiFi network settings of the Schlage MT20W.
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.

WARNING: Do not remove this label until the device is commissioned!

Be sure 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

Tools needed for lock installation: Phillips screw driver and tape measure.

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. Verify the door thickness, the lock backset, proper hole dimensions and for interconnected units (FE410), the bore-to-bore dimension of 4” or 5½”.
**WARNING:** The Center Lines of the drilled holes and proper alignment MUST be accurate for proper deadbolt and/or latch retraction.

**Installation**

Install the Schlage Control™ Smart lock as indicated in the installation instructions. 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 is reversed.
- The through door cable is routed from the exterior side OVER the top of the latch body and through the door.
• The CAM is in the correct position during installation. The CAM contacts the switch above when in the correct vertical 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 smoothly retract the deadbolt whenever the inside lever is used with no restrictions.

• Upon Power-up the Schlage Control™ device boots up, flashes the GREEN LED and beeps 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 automatically sets the "Facility Code" for all Construction cards to be used at the door. Any credential with the SAME Facility Code is granted access.

NOTE: Construction Mode for other products (Schlage NDE, LE, and CTE) 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 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).
  - All previously valid Construction Credentials no longer function at the door after Commissioning or Factory Default Reset.
  - CAUTION: The Schlage Control™ lock accepts the first card presented after FDR and uses 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.

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 beeps 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 access momentarily. Engage the thumb turn for locking and unlocking access to the door.
Factory Default Reset (FDR)

Things to Know:

- FDR returns the Schlage Control™ Smart lock to its original Settings as shipped from the factory.
- FDR removes any non-default device settings, deletes any construction or user credentials and again allows commissioning or construction mode.
- FDR does not have any effect on the firmware currently on the lock.
- FDR does 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 provides 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 acknowledges successful FDR completion with one long GREEN flash and beep.

VERIFY SUCCESS

- The lock now "Advertises" via Bluetooth and can be 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.
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 – ENGAGE™ Training Videos.

Prepare for Installation

Tools needed for lock installation: Phillips screw driver, pin wrench, tape measure and a T-15 Torx screwdriver (optional).

**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.
- Be sure 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 of 1 ¾”.

1c Connect chassis cable. Route cables.
The cable should be routed on top of the chassis! Connect cable from outside assembly to connector in chassis.

- **LH**
  - Push and tuck cable.
  - Route cable in metal channel.
  - Connect cables.
  - Route cable in plastic channel.

OR

- **RH**
  - Push and tuck cable.
  - Route cable in metal channel.
  - Connect cables.
  - Route cable in plastic channel.

Tuck connected chassis cable into appropriate channel.
• The installed latch and chassis are properly aligned and fully engaged.

![Diagram showing the latch and chassis](image)

Insert the chassis into the installed latch  
Check prong engagement

Proper installation of the latch and chassis interfaces

**WARNING:**

• The latch prongs MUST fully engage the top and bottom chassis slides.
  o 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) are used, additional door prep is 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 performs a Power-On-Self-Test (POST). A few seconds after power is applied the Schlage NDE indicates successful POST.
- Three GREEN flashes and 3 beeps are provided to indicate the lock is ready for Commissioning or Construction Mode operation.
CONSTRUCTION Mode

Things to know:

- A Construction Mode is provided for the Schlage NDE device as it is for the Schlage LE and CTE products. Schlage NDE requires a MASTER Construction Credential that is used to add additional Access Construction Credentials to each installed Schlage NDE.
- The 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 intended to gain momentary access.

- Construction Mode operation provides NORMAL Credential function, and the Schlage NDE always automatically relocks after momentary access is granted.
- Construction Mode must be canceled by performing a Factory Default Reset (FDR). After an FDR, all previously valid Construction Credentials are no longer 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 to the lock. The Schlage NDE requires FDR and all construction credentials 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 (RTE) and present a new credential to become the property Master Construction Credential.
- The Schlage NDE acknowledges the credential presentation with 5 GREEN flashes and enrolls the credential as the Master Credential.

**VERIFY SUCCESS**

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

**NOTE:** The next credential presented is enrolled as a Construction Access Credential and is allowed momentary access to the Schlage NDE when presented again.
Create **Construction Access Credentials**

- To enroll construction credentials that 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 Schlage NDE beeps after successfully enrolling the presented credential.
- Repeat the Master Credential presentation followed by a new Construction Access Credential for each Construction Access Credential that is 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 returns the Schlage NDE to its original settings as shipped from the factory.
- FDR removes any non-default device settings, deletes any construction or user credentials, and allows construction mode to be entered again.
- FDR does not have any effect on the firmware currently on the Schlage NDE.

**NOTE:** FDR does 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 and then perform an FDR.

**Perform a FDR**

- Remove the Schlage NDE battery cover and Press and HOLD the FDR button for 5 seconds. The Schlage NDE beeps and blinks two (2) times.
  
  ![Press and hold the FDR button for five seconds.]

- Turn the inside lever three (3) times within 20 seconds.
  - The Schlage NDE blinks RED and beeps on each lever turn; then provides two GREEN flashes and beeps to indicate success.
VERIFY SUCCESS

- The Schlage NDE now "Advertises" via Bluetooth communication and can be seen in the CONNECT screen as available for commissioning with an ENGAGE™ Mobile Application.

**NOTE:** Bluetooth (BLE) communication requires the battery cover to be properly installed.

- A new Master Construction Credential can be created.
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 – ENGAGE Training Videos.

- Be sure 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

- Tools needed for installation: Phillips screw drivers (#1, #2), needle-nose pliers, and a tape measure.

**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. 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. 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).

**WARNING:** If you are changing the handing direction, be VERY careful not to break the microswitch due to reversing the handing on the installation.

### Verify Installation success

- Once the Schlage LE is properly installed, the inside lever moves the latch in and out of the door and frame smoothly and 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 restriction.
- The door closes properly, and the lever handing is correctly installed.
- Upon power-up, the lock performs a Power-On-Self-Test (POST). A few seconds after power is applied, the Schlage LE indicates 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 for the Schlage LE device as it is for 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 is available Out-Of-The-Box or after a successful Factory Default Reset (FDR).

**NOTE:** Master Construction Credentials for Schlage LE do not provide access through the door. Schlage LE Master Construction Credentials can only add other construction credentials to the lock intended to gain momentary access.

- Construction Mode operation provides NORMAL Credential function and the Schlage LE always automatically relocks after momentary access is granted.
- Construction Mode can be canceled by performing a Factory Default Reset (FDR). After an FDR, all previously valid Construction Credentials are no longer valid.

**NOTE:** No User Audits are stored in Construction Mode because the Schlage LE does not track time or credential numbers.

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

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 acknowledges 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 Schlage LE LED lights GREEN for 20 seconds waiting for another credential to be presented for enrollment as a **Construction Access Credential**.
- The next credential presented is enrolled as a Construction Access Credential and is allowed momentary access to the lock when presented again.

Create Construction Access Credentials

- To enroll construction credentials that 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 beeps after successfully enrolling the presented credential.
- Repeat the Master Credential presentation followed by a new Construction Access Credential for each Construction Access Credential that is 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 returns the Schlage LE to its original Settings as shipped from the factory.
- LE beeps when in FDR mode any time the inside lever is turned.
- FDR removes any non-default device settings, deletes any construction or user credentials and allows for construction mode to be entered again.
- FDR does not have any effect on the firmware currently on the Schlage LE.

**NOTE:** FDR does NOT remove the Schlage LE from your ENGAGE™ account. To re-enroll a Schlage LE into another ENGAGE™ account, you must first delete the Schlage LE 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 beeps and blinks two (2) times.

  Press and hold the FDR button for five seconds.

  ![Press and hold the FDR button for five seconds.](image)

- Turn the inside lever three (3) times within 20 seconds.
  - The Schlage LE blinks RED and beeps on each lever turn, then provides two GREEN flashes and beeps to indicate success.

VERIFY SUCCESS

- Turning the inside lever causes the Schlage LE to beep.
- The Schlage LE "Advertises" via BLE communication and using the ENGAGE™ Mobile Application can been seen in the CONNECT screen as available for commissioning.

**NOTE:** BLE communication requires the battery cover to be properly installed.
- A new Master Construction Credential can now be created.
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. Review all accessory details for the Power Supply, Credential Reader and locking device installation instruction to be sure of their interconnection and mounting requirements.

- Be sure 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

- 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

- Install the Schlage CTE and accessories as indicated in their respective installation instructions. Pay special attention to these installation planning topics for best operational results.
  - The Schlage CTE installation is intended for indoor use ONLY with a temperature range of -35°C to +66°C (-31°F to +151°F).
  - 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 starting (Schlage CTE enclosure, Credential Reader, Locking Device, etc.).

- For best WiFi network and Bluetooth (BLE) wireless communication:
  - The Schlage CTE should not be mounted near large metal objects or inside other metal enclosures or cabinets.
  - 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 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 wiring 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 **electrostatically safe** manner.
Installation: Power Supply

When selecting and installing a power supply, refer to that component’s 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 supports 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:

1. Schlage CTE does not control the Credential Reader beeper.
2. A Configuration Card (CE-401-133) is required to disable the credential reader beeper.
3. The Reader needs to be paired with the Schlage CTE.
4. 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:

![Credential Reader Pairing Steps]

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

Installation: Locking Devices

Schlage CTE supports many different types of electronic locking devices. The installer should review the locking device installation instruction for the device they intend to install and follow its installation requirements.

VERIFY 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 are exercised when the TEST buttons are pressed.

![Relay Outputs Diagram]

**NOTE:** Each output is overcurrent protected. The FAULT LED (circled) illuminates 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 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:

1. Press and Release the **SCHLAGE** button.
2. Quickly press the **FDR** button two (2) times.
3. When wired correctly the Schlage CTE and reader respond with:
   a. Three (3) LED AMBER blinks and three beeps
   b. The RS485 LEDs flash

**Operation in CONSTRUCTION Mode:**

Things to know:

- Construction Mode is provided for the CTE Controller as it is for 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 is available Out-Of-The-Box or after a successful Factory Default Reset. (FDR).
NOTE: Master Construction Credentials for Schlage CTE do not provide access through the door. Schlage CTE Master Construction Credentials can only add other construction credentials to the lock intended to gain momentary access.

- Construction mode operation provides NORMAL Credential function and the Schlage CTE always automatically relocks after momentary access is granted.
- Construction Mode can be canceled by performing a Factory Default Reset (FDR). After an FDR, all previously valid Construction Credentials are no longer valid.

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

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

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 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 acknowledges the credential presentation with 5 GREEN flashes of the Schlage CTE MODE LED and enrolls 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 lights GREEN for 20 seconds waiting for another credential to be presented for enrollment as a **Construction Access Credential**.

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

Create Construction Access Credentials

To enroll a construction credential that allows 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 illuminates GREEN waiting for the next credential presentation.
- While the READER LED and the CTE STATUS LED are solid GREEN, **present a new credential** intended to become a Construction Access Credential.
- The Schlage CTE flashes 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 a new Construction Access Credential for each Construction Access Credential that is 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 returns the Schlage CTE to its original Settings as shipped from the factory.
- FDR removes any non-default device settings, deletes any construction or user credentials, and allows 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 does 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 then perform an FDR.

- The Schlage CTE MODE indicator LED illuminates 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.

- Press the SCHLAGE button three (3) times; there is a beep with each button press.
  - The Schlage CTE STATUS and Credential Reader LED blinks GREEN for one second. This is indicating that the FDR process has been successfully completed.
- The CTE MODE indicator illuminates 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.

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

- Enter the Users’ information.
  - **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 (Doe, John) is now listed in the **Users** tab.

**NEXT STEPS:**
After defining a New User, the new User requires the following steps be completed:
- Assign at least one **Credential Assignment**; 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](#).
- Perform device syncing or No Tour updates with each device 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 User. There are three methods of Credential Enrollment possible depending on the Property Administrator preference.

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

- **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 is entered into ENGAGE™ for No Tour functionality.
  - The credential is assigned to the selected, existing User.
  - Access rights for the User are programmed into the credential, for No Tour credential programming functionality.

- **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 are available in the ENGAGE™ Web Application under the “Select Existing Credential” tab.

- 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 are not 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 begins communication. The LED is solid BLUE indicating it is ready.

- Log into the ENGAGE™ Web Application and Select **Users** then the **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.
- Select the **Add Credential** button.
• Select the **Select Existing Credential** tab.

![Select Existing Credential Tab](image1.png)

• Obtain a new credential from your supply 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 turns GREEN and beeps one (1) time when the card is accepted.

• Repeat card presentation(s) and the enrollment process for each credential you want to make available in the **Select Existing Credential** 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 makes the credential available in ENGAGE™ Web Application for assignment to a User. To complete the process, the Property Administrator may need to also:

• Assign at least one 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.
• Perform device syncing or No Tour updates with each device the User has been granted Access; see Sync – 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 allows bulk enrollments into stock that can be selected and assigned later to individual Users.

**NOTE:** Property Administrators 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 communication.

**NOTE:** The Schlage MT20W takes a few seconds to boot-up and begin communicating. The LED is solid Blue when the MT20W is ready for use.

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

**NOTE:** The Schlage MT20W LED turns GREEN and beeps 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 are listed.

![Add Credential Image]

**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 enrolled into ENGAGE™ for assignment later. Property Administrators 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](#).
- Perform device syncing or No Tour updates with each device the User has been granted Access; see [Sync – Updating a Door File](#).
Enrolling Credentials at a Door

It is possible to assign a credential 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 have one limitation.

The enrolled credentials are not 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.

- Select an existing User to receive the new credential.

**NOTE:** In this case we chose Doe, John 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 displays.

- Select the device you want to use as the enrollment reader from the nearby Available Enrollment Reader list displayed. In this case we chose Storage.

  NOTE: After selection of the Storage device, the LED flashes 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 displays a credential "Value" with asterisks ****** displayed.

### Before Credential Read

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Normal</td>
</tr>
</tbody>
</table>

### After Credential Read

<table>
<thead>
<tr>
<th>Name</th>
<th>Credential 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>********</td>
</tr>
<tr>
<td>Function</td>
<td>Normal</td>
</tr>
</tbody>
</table>

NOTE: If no credential is presented, the process "Times 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**.

![Credential Enrollment Timeout](image1)

• Tap on the **Function** menu setting if the default “Normal” assignment is not wanted. You may set any credential function as needed.

![Credential Config](image2)

• Select **Done**.

• Select **Save**.

• Acknowledge the **Credential Updated Successfully!** Message.

![Credential Updated Successfully!](image3)

• Select **OK**.
VERIFY SUCCESS

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

NEXT STEPS:

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

- Provide Access and Schedule Assignments for the property; see Assigning Lock Access and User Schedules.
- Perform device syncing with each device the User has been granted Access; see Sync – Updating a Door File.

WARNING: The enrolled credential is not searchable in the ENGAGE™ Web Application when using the Badge ID Search Utility.
Assigning Credentials

Overview
Assignment of a credential connects 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 require all devices that the User has assigned access to, to be programmed before the credential is honored. Device programming can be immediate with the No Tour process or provided via syncing (Door File Updates) at the door or overnight WiFi connection when available.

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

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

- Select Add Credential button.

![Image of ENGAGE™ Web Application showing the Users and New User pages with Add User and Add Credential buttons.](image-url)
• Select the Credential to be used from the **Select Existing Credential** tab. In this case credential #1965 has been selected.

![Add Credential](image)

**NOTE:** If no credential is available, you must **Enroll a Credential** now.

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

![Credential Function](image)

**WARNING:** When working with Schlage Control™ devices, a Toggle credential function acts 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 assigns a credential to the User. The Administrator needs to ensure the affected property doors are programmed before the credential access is honored at the door. Administrators 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.
- Perform device syncing with each device the User has been granted Access; see Sync – Updating a Door File.

NOTE: ENGAGE™ displays device Update ICONs indicating the Devices and credentials that need programming.
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 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™ reads the Smart credential serial number of a credential presented to the Schlage MT20W, applies the required updates from the ENGAGE™ database and program updates onto the credential.

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

To begin:

- Make all access assignments, user schedule and updates for the resident in ENGAGE™ as necessary.
- Ensure the Schlage MT20W is powered up and communicating.
  - The Schlage MT20W takes a few seconds to boot-up and begin communicating.
  - The Schlage MT20W LED is solid Blue when the 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™ are programmed onto the Smart credential automatically.

- Place the Users’ Smart credential to be programmed with new Access Rights on the Schlage MT20W.
  - The Schlage MT20W LED turns solid GREEN to begin the programming process, followed by one beep. This indicates 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 indicates that the credential is programmed with the latest updates.

![Before Credential Programming](image1)

![After Credential Programming](image2)

- Complete the **No Tour** programming process by physically presenting the newly programmed credential to all affected devices.
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 displays.

WARNING: If the credential was initially enrolled using an installed device instead of the Schlage MT20W, it is not searchable in the ENGAGE™ database and cannot be found there.

- 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.

VERIFY SUCCESS

- The credential owner and badge ID is displayed: User, New 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’ credential and plan for the credential(s) next use. Here are two scenarios to consider:

1. Resident Moves out and returns their Smart No Tour credential to the Property Administrator who has a new resident available. The new resident requires the SAME access rights as the departing resident. 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 previous resident had access.
   • Deleting the credential from the ENGAGE™ database does the following:
     o Removes all previously programmed door access for that credential
     o Generates the update ICONs in the ENGAGE™ database needed to indicate which doors require Sync updates
   • Sync all doors with required updates.

**WARNING:** The Property Administrator must Sync doors with previous (resident) access to remove the unreturned credential from the lock database and to deny future access.
Deleting Existing Access

When the resident’s credential is not available, you must **Delete Credential** from the ENGAGE™ database and Sync 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 is honored (denied). Sync with each device is required.

**NOTE:** ENGAGE™ displays the "Update" ICON indicating the specific doors that need to be programmed. The update ICON remains 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 tab and the specific User to have a credential deleted on the Users tab.

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

- Select Delete this credential.
• Type the word ‘**delete**’ into the Confirm: Field.
• Select the **Delete** button.

**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 perform No Tour programming before the deleted credential is denied access at the door.

**NOTE:** ENGAGE™ Web Application displays the exclamation point "Update" ICON to indicate which doors with deleted access rights 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 Conference Room for deletion.

- Select the Delete button.
• Confirm the process by typing the word ‘delete’ into the Confirm: box.
• Select the Delete button to continue.

VERIFY SUCCESS

• See the momentary Device deleted. success message.

• 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 chose the **Apt B845** device for deletion.

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

- Select the Delete button.
VERIFY SUCCESS

- The Apt B845 is no longer listed in the Devices screen.

<table>
<thead>
<tr>
<th>Device</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apt 5D2B</td>
<td>E100000000025D2B</td>
</tr>
<tr>
<td>Garage 141 B</td>
<td>A0210000000A0141</td>
</tr>
<tr>
<td>Laundry 137</td>
<td>A0210000000A0137</td>
</tr>
<tr>
<td>Lobby 83</td>
<td>A0210000000A0083</td>
</tr>
<tr>
<td>MT20W Card Reader</td>
<td>C20000000000108</td>
</tr>
<tr>
<td>Pool 142</td>
<td>A0210000000A0142</td>
</tr>
<tr>
<td>Pool 286</td>
<td>A0210000000A0286</td>
</tr>
<tr>
<td>Storage</td>
<td>E10000000F1232EF</td>
</tr>
</tbody>
</table>
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 is still valid at previously programmed doors until the lock is presented with the replacement No Tour credential or a new device sync (door file update) is performed.

- Open the ENGAGE™ Web Application.
- Select **USERS** tab and the effected User in the **Users** tab.

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

**NOTE:** In this case Credential 1171 is 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.

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

- Select **a Replacement Credential** from stock list. In this case we chose Credential #1802.

**WARNING:** Physically verify the ink stamp on the physical credential matches 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 **Existing User** Credentials and the old "Replaced" credential (1171) has been removed from the list.

---

**NOTE:** The **Update** ICON by the credential indicates 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.
NOTE: The ICON by the credential is removed, indicating the credential was programmed successfully and has no additional programming required.

NOTES:

1. ENGAGE™ displays Update ICONs indicating the affected locks that require Sync with new access programming.

2. Schlage NDE, LE, and CTE devices may be updated nightly via automated WiFi network connections.

3. 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.

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 WiFi 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:**

1. Schlage Control™ device firmware must **always** be updated at the door using the ENGAGE™ Mobile Application and **Firmware Updates**.

2. For Schlage NDE, LE, and CTE devices, overnight WiFi network firmware updates can be scheduled by the ENGAGE™ Web Application when a WiFi network connection is available and properly enabled.

3. Schlage NDE, LE, and CTE nightly WiFi updates require WiFi network availability overnight for the scheduled firmware updates to be successful.

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

5. Firmware updates take some time to complete. The devices flash the “Amber” LED while the firmware file is being sent to the device. The device parses the file into its memory while flashing the LED RED and GREEN. This process may 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 all other ENGAGE devices may use a local WiFi network connection for faster firmware updates and scheduled firmware updates.

This example updates a Schlage Control™ device that requires Bluetooth (BLE) for updates. All other devices may 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**.

![Device List]

- Select More …

![Menu Options]

Then...

**NOTE:** The device starts flashing the RED LED when connected and communicating.
• Select **Update Firmware** in the connected device menu.

![Updated Firmware Screen]

**NOTE:** When a firmware update is available, this message is presented.

• Select **Update** in the connected device menu.

![Downloading Firmware Screen]

**WARNING:** This is a local Bluetooth (BLE) firmware update method. The mobile device MUST stay within communication range while downloading firmware. This takes a few minutes – be patient.
• The following screen displays when the firmware update is successful.

![Firmware Update Screen](image)

**NOTE:** The recently updated device loads the new firmware into its memory and REBOOTS itself. This process takes a few minutes – be patient.
Device Firmware Updates – at the door using local WiFi network communication

ENGAGE devices with local WiFi connectivity may have firmware updates performed at the door. This method is preferred over the previous described Bluetooth (BLE) method because it uses the local WiFi 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 update a Schlage LE device using a local WiFi 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 a Schlage LE device with its WiFi network connection properly enabled.
• Select **More** ....

![Image](image1.png)

then...

![Image](image2.png)

• 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 takes 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 blinks the LED RED and GREEN while installing the new firmware update. During this time, the device is inoperative. Once the firmware installation is complete, the device reboots and begins normal operation. This process takes a few minutes, be patient.
Device firmware updates – at the door with no local WiFi network available.

When the device does not have a WiFi network connection available or the local WiFi network is not enabled, the firmware download is performed by temporarily enabling a WiFi connection through the Property Administrator’s mobile device.

In this case the Storage device WiFi 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.

- Select the local device to be updated with the latest firmware. In this case we chose Storage.

  **NOTE:** This is a Schlage LE device with its WiFi 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 WiFi connection.

NOTE: The system knows the device name and the WiFi PASSWORD is stored in the mobile device “Clipboard”.

---

Contact Technical Support @ 1-877-671-7011; Option 2 for ENGAGE™ and supported devices
– Hours of Operation: 8 AM to 8 PM EST –
Page 226 of 262
Perform the following steps on the mobile device:

1. **Leave** the ENGAGE™ mobile Application – temporarily.
2. **Open** the Settings menu on your mobile device.
3. **Select** the WiFi network settings menu.
4. **Connect** with the WiFi with the same name as the device you are connected to.
   a. In this case we must choose **Storage**.
5. **Paste** the PASSWORD into the WiFi 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 WiFi connect information.
   - **Return** to the previous ENGAGE™ mobile Application screen.
   - **Select Next**.
Completing the device Firmware updates after download

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

The device follows 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 performs a reset and begins normal operation.

**IMPORTANT NOTE:**

After a firmware update using this method is successfully accomplished, the device is ready for normal operation. However, ENGAGE does not know that the firmware update process has been accomplished and continues to report the previous firmware revision until the next device Sync reports the new successful firmware update to ENGAGE.

**WARNING:**

1. The firmware internal memory installation takes a few minutes to complete. Be patient.
2. While the device internal firmware installation update is in process, the device LEDs flash RED and GREEN.
3. During the device internal firmware update process the device does not act as a lock. Access attempts are ignored.
4. Wait for the RED and GREEN LED flashing to stop before using the lock for normal access again. Be patient, this takes a few minutes.
5. A device Sync is 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, then 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 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 WiFi network configurations set and working with the local WiFi 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 to the **Latest Firmware Version** that is available.
• When a firmware update is available, check each **Device Name** box that requires a firmware update.

![Device Management Screen](image)

**NOTE:** In this case the **Garage 141B**, **Laundry 137**, **Lobby 83**, **Pool 142** and **Pool 286** firmware is not at the latest revision. Notice 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 same as 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 WiFi network availability overnight - it may have been down
- Verify WiFi 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 WiFi 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 **Audits**.
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.

- 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 been retrieved.
Using Nightly WiFi Updates

Schlage NDE, LE, and CTE devices may be enabled to call in to ENGAGE™ every night when the WiFi network communication settings are properly setup.

New or updated access rights, schedule addition or changes and any Audits are gathered during the nightly WiFi network call in.

**NOTE:** No actions other than ensuring proper WiFi 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 WiFi feature to verify network settings and proper communication.
- See **Sync – Overnight – Schlage NDE, LE, and CTE** for more detail.

**WARNING:** Nightly WiFi network updates (Call-In) is not available with Schlage Control™ Smart locks.
Viewing Audit Information

Overview
Device and User Audits is 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’ WiFi network connection capability.

Audits may be reviewed by either 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 the desired lock from the list – we chose Storage Room.
Select Device Audits button.

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

Displaying Audits for Property Wide Audits

• Open the ENGAGE™ Web Application.
• Select the AUDITS and the Audits tab.

• Use the available Sort and filter options, as desired.
NOTE: Data can be sorted or filtered numerous ways.

1. By Device or User
2. By Audit Type

   ![Audit Type Selection]

   - Battery Audits
   - Credential Audits
   - Debug-Diagnostics
   - Door Action / Switch Audits

3. By START and END times
   - Export Audits using the square EXPORT button (Top-Right corner of screen).
     - Data is saved into a .csv file for easy spreadsheet analysis.
     - Save your audit file to disk for archive and analysis.

NOTE: 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:**

1. Master Credentials are generally used for Property Maintenance and local Fire Department and emergency access to all openings on the property.
2. A Master Credential allows PASS THROUGH credential function access to every ENGAGE™ managed opening on the Property.
3. The Master Credential feature is **DISABLED by default**.
4. When using Master Credential, the feature should be enabled before commissioning.
5. Any device commissioned before the Master Credential feature is enabled requires syncing (Door File update) to enable the feature at the door.
6. 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 is enabled.
7. No Tour programming can ADD Master Credentials. However, to DELETE a Master Credential, the credential must be deleted in the ENGAGE™ database and every lock must be sync’d.
8. Any valid User credential type can be assigned as a Master Credential.
9. Multiple Master Credentials can be generated for the same property.
10. Lost Master Credentials, require every originally programmed device to be re-programmed to remove the lost Master Credential.
11. 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.
12. **DELETED** Master Credentials are permanently **DELETED** and can never be used again in the same ENGAGE™ account – ever. **BEST PRACTICE**: Destroy Deleted Master Credentials.
13. **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**.

![ENGAGE™ Web Application Screenshot]

- Slide the Master Credentials button to **ON** to enable the generation of Master Credentials.

**VERIFY SUCCESS**

- View the momentary **Master Credentials setting updated.** message.

![ENGAGE™ Web Application Screenshot]

- View the **Master Credentials** setting has moved to **ON**.
NEXT STEPS:
This process enables Master Credentials to be generated within the ENGAGE™ Web Application. The Property 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 any devices.

Assign a Credential as MASTER

- Open the ENGAGE™ Web Application.
- Select the **USERS** and **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 picked 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 to choose; *Credential 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**.

![Master Credential Interface](image)

**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 next to the credential indicating it is programmed as a MASTER CREDENTIAL with the PASS-THROUGH function assignment on every lock.

NOTE: This process 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:

1. Every Device now has the **Device Update ICON** displayed to inform the Property Administrator that door updates are needed.

2. The Master Credential itself and all devices are required to be updated before these changes are honored.

3. The Property 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 Property 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 Master Credentials

- Open the ENGAGE™ Web Application.
- Select the ADVANCED and then select the Credentials tab.

To View Master Credentials:

- Select the View All Master Credentials button. All Users with Master Credential assignments are displayed.
To Delete Master credentials:

- Select **Delete Master Credentials** button.

- 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:

1. This process removes the Master Credential from the ENGAGE™ database and schedules the changes needed for the property. All devices in the ENGAGE™ Web Application now show the Device Update ICON 🔄.

2. All devices are required to be updated before the deleted Master Credential change is honored at the door.

WARNING: The Property Administrator should provide sync (Door File updated) to the entire property when a Master Credential is 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™ defaults all User Expiration Dates to five (5) years after enrollment automatically.
- Property Administrators who review and confirm **default settings** before commissioning the first device, save time setting up their property and do 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, requires Sync device updates before the new or updated schedule is followed.
- Common area access **Device Groups** should be defined before User access assignments are attempted. New or modified Device Groups require Sync of devices, before any group update is valid for that device.
  - Remember, devices must be commissioned before they are available to be selected for a Device Group. After assignment of a door into a Device Group, that door’s locking device requires Sync so that it knows to what group it is assigned.

Best Practices – Device Set-up

- Define the Sitewide Device Settings before commissioning devices.
- For best reader response and improved battery life, it is recommended to disable any credential technology on multi-technology readers that are not used.
- For locks that are in spotty WiFi network areas, use the mobile device data connection and turn off the lock WiFi 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 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 do not provide device setting changes.
- The automated nightly WiFi device syncing (Door File updates) is available with Schlage NDE, LE, and CTE only, Schlage Control™ devices do not support WiFi connectivity.
• Schlage Control™ devices only support User Schedules - No Holiday Schedules, No Door Schedules.

• Schlage Control™ devices require an “Audit” request at the nearby device using the ENGAGE™ Mobile Application to gather audits.

• Device Audits are also automatically gathered immediately following a Device Sync Update.

• 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: A schedule change requires the Property 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 to 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 allows 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) indicate 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.

NOTE: The credential update ICON remains 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 needs to be programmed.

NOTE: The device update ICON remains until Audit information is returned to let ENGAGE™ "KNOW" the update at the door has been accomplished.

Once an update is acknowledged in an Audit, ENGAGE™ removes 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 does NOT remove the device from the ENGAGE™ database, it simply 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 saves battery life by not “looking” for unnecessary credentials and improves the user experience when presenting credentials for access with faster response.

• To disable Proximity Credentials, see Device Settings for Schlage NDE and LE Devices.
• The Wall mounted reader used with Schlage CTE requires a Configuration Card to disable Proximity Credentials.
Troubleshooting

All Devices – Diagnostic Audits

Schlage NDE, LE, and, CTE devices provide diagnostic data when requested by the ENGAGE™ Mobile Application. Diagnostic data provided includes; Battery Health, WiFi 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.
- 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

- If an email invitation never arrives:
  - Check SPAM and TRASH folders for misplaced email.
  - Verify the entered email address is correct.
  - Verify your PASSWORD.

Device Commissioning

- If the 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

- If a device does 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

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

Schlage MT20W would not connect to the WiFi Network

- Verify with a Mobile device to determine if the WiFi network (Access Point) is present and available.
- Using a mobile device (phone) to connect to the SAME WiFi the device is using:
  - Verifies proper SSID and Password settings, if applicable.
- Perform Factory Default Reset (FDR) and Commission again.

**NOTE:** Performing a Factory Default Reset (FDR) requires a Configuration card CE-000-040 for a Schlage MT20W.

Schlage Control™ - "Jump Start" Process

- Schlage Control™ devices 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 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 performs its power-on reset and starts up; providing 1 RED LED flash and then 3 GREEN LED flashes and 3 beeps. The lock startup takes a few seconds, be patient.
- While still HOLDING the external battery in place, present a valid credential for access.
The lock unlocks with the normal Relock Delay.
  o 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 with Alkaline ONLY!
  **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.
  o Open the ENGAGE™ Mobile Application.
  o Select the **In Range** menu.
  o Select the nearby device.

  **NOTE:** When connected, the lock LED flashes RED.
  - The Mobile Device Date and Time settings are automatically set into the device.

### Device Firmware Updates Overnight Not Performed

- Verify local WiFi network was operational overnight. Was there an outage?
- Verify the device WiFi network settings, SSID, user name and password.
- Use the “Test Wi-Fi” feature in the Mobile Application.

### 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 is not able to communicate with the Schlage CTE.

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

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

1. How can I determine the local WiFi network settings?
   - Consult with the local property IT responsible person.
   - Use a Mobile Phone to try to connect and verify the local WiFi network.

2. Does ENGAGE™ work with 5.0GHz network routers?
   - ENGAGE™ requires 2.4 GHz 802.11 b/g WiFi and is not compatible with 5.0 GHz routers.

3. What is the WiFi network “Mandatory Data Rate”?
   - The local WiFi 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 WiFi network setting for maximum Mandatory Connection Speed to be 24Mbps or lower.
   - Schlage LE and CTE devices support standard WiFi data rates and always connect to the local WiFi 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 Property Administrator should be as close as possible to the device – a few feet.
   - Bluetooth communication through walls and doors significantly reduces communication range.
   - You 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 connecting with the ENGAGE™ Mobile Application to ensure the highest data rate possible.

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 expire in less than a week.
- Resend of invitations is possible for expired invitations at any time.
- Invitations and Team Members can be deleted at any time.

7. How do I know the Schlage MT20W is working?

- When ready and communicating, the Schlage MT20W LED is solid BLUE.
- If not Commissioned the LED is solid RED after booting up.
- The Schlage MT20W Boots Up upon power application.
  - On Power up, the RED LED flashes and beeps.
  - The BLUE LED begins flashing for a few seconds.
  - The BLUE LED turns solid BLUE when the MT20W is ready for enrollments/programming.

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 provide local feedback to the user at the door when the batteries are low. Low Battery status causes 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 is provided for low battery providing up to 500 operations or about two weeks of normal use.
- Devices enter “Critical Battery” mode after the “Nuisance delay” warning is ignored for a significant time.
- Devices in critical battery mode do 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 display a RED LED ON solid (under the battery cover) when the lock has entered “Critical Battery” mode. The batteries must be replaced to begin normal operation.

10. What is a Nuisance Delay?

- A Nuisance Delay, is a delayed access at a door with a battery-operated device. A Nuisance delay happens any time a valid credential is presented to a device with Low Batteries.
A Nuisance Delay is provided when the device batteries are nearing depletion. The delayed access is intended for the user to report back to the Property Manager that the device needs attention.

A Nuisance Delay is provided for up to 2 weeks of normal operation before “Critical” battery level is reached or approximately 500 normal access attempts.

Battery operated devices begin providing a Nuisance Delay when the batteries are at the following voltage levels or lower:
- Schlage Control™ = +4.60Vdc
- Schlage NDE and LE = +4.40Vdc

When a Nuisance Delay is ignored long enough, the device transitions into "Critical" battery mode and stops 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 display 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 is solid RED to indicate Critical battery.
  - Schlage NDE: LED under the Battery Cover is solid RED to indicate Critical battery.
  - Schlage LE: Outside LED is solid RED to indicate Critical battery.

- No normal lock operations are possible in Critical Battery Mode, except a valid user credential programmed as a “Pass-through” can be used to attempt to gain access.

- Jump Start for Schlage Control™ or keyed access is 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 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 an 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 be deleted from the original ENGAGE™ Managed account.
  - All devices must be Factory Default Reset (FDR).
  - All devices be re-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.
- **As BEST PRACTICE:** Properties planning the use of No Tour should enroll and commission the MT20W before any other devices are commissioned.
  - Commissioning of an MT20W tells ENGAGE™ that the property is a No Tour property and to enable the feature in all newly commissioned devices.

**WARNING:** Any device commissioned prior to the MT20W, is required to be sync’d (door file updated) again before the No Tour feature can be used.

  - Devices enrolled before the MT20W are not No Tour capable until they are 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 (devices) 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 are not able to relock the deadbolt after exiting because the lock denies their credential because it falls 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) do not have a Badge ID and cannot be found using the ENGAGE™ Web Application Badge Search utility.
## APPENDIX A – Property Role Assignment and Capabilities

### Administrator – Manager – Operator Roles

<table>
<thead>
<tr>
<th>ENGAGE™ Feature and Role Assignment</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></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></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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite users as Operator</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Invited users as Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Invited users as Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Invited users as Operator</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign users as Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign users as Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign users as Operator</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Property Administrators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Property Managers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Property Operators</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Commission Devices</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Devices</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Delete Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage People</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Connect to Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync - Update Door Files</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Update Firmware</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Update from Server</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Run Diagnostics</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Get Audits</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>View WiFi Settings</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Change WiFi settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Audits / Alerts</td>
<td>X</td>
<td></td>
<td>X</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 needed or just when you are curious about an operation or a feature.

Videos on “Schlage Electronics How-To” mobile application

Allegion has many videos available on your mobile device to help with all the ENGAGE™ features and options available.

Download the “Schlage Electronics How-To” app 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 locked.
    - Schlage Control™ does not support Toggle credentials. If a Toggle credential is programmed into a Schlage Control™, the lock engages the thumb turn for the defined relock delay period.

- **Freeze**
  - Freezes the lock in its current state (locked or unlocked).
  - Lock remains frozen until a Freeze credential is presented again.
  - The Freeze credential used to “unfreeze” a lock can be the same credential or a different Freeze credential.

- **One Time Use**
  - Allows only one attempt with Normal Access granted.
  - Schlage Control™ does not support One Time Use credentials and denies access anytime a One Time Use credential is presented.

- **Pass Through**
  - Unlocks a lock momentarily.
  - Gains access to a lock in Freeze and Lock Down states.
  - Gains access during scheduled Holiday lockouts.
  - Attempts to unlock a device that is in “Critical Battery Mode”.

- **Lock Down**
  - Changes the state of the lock to locked and disables all normal user credentials.
  - Pass Through credentials gain access when Lock Down is enabled.
  - Freeze credentials must be used to return locks to normal state, from Lock Down.

- **Block**
  - Denies normal access to the lock and records the access attempt as an audit.