



# AVIGILON™ ACCESS CONTROL

System Integration Guide for Schlage® Wireless Locks  
No-Tour

© 2023, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logos, and AVIGILON ALTA are trademarks or registered trademarks of Avigilon Corporation. Android is a trademark of Google LLC. Apple, iPhone, and iPad are trademarks of Apple Inc. Allegion, ENGAGE technology and Schlage are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. All other trademarks are the property of their respective owners.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation  
avigilon.com

20231023-en

# Revisions

---

Guide	Description
1.1	Updated <a href="#">Issue Openpath mobile credentials on page 17</a> ; added <a href="#">Troubleshooting on page 24</a>
1.0	Initial release of guide

---

# Contents

- Revisions ..... 3
- Contents ..... 4
- Before you start ..... 6
  - System overview ..... 6
  - Prerequisites ..... 7
  - System requirements ..... 7
  - For more information ..... 9
    - Technical support ..... 9
    - Product documentation ..... 9
- Step 1: Set up customer organization and Allegion licenses ..... 10**
- Step 2: Sign in to ENGAGE site, download ENGAGE mobile app, and sync ENGAGE account with Control Center ..... 11**
- Step 3: Add Schlage devices to ENGAGE site using ENGAGE mobile app, and sync with Control Center .... 12**
  - Install Schlage Wireless Locks app ..... 12
  - Sync credential enrollment readers with Control Center ..... 12
  - Sync wireless locks with Control Center ..... 13
  - Edit wireless lock information ..... 14
- Step 4: Assign wireless locks to entries and zones in Control Center ..... 15**
  - Add entries ..... 15
  - Add zones ..... 15
- Step 5: Issue credentials and entries to users in Control Center ..... 16**
  - Issue no-tour Schlage user credentials ..... 16
  - Issue Openpath mobile credentials ..... 17
  - Issue all-access credentials for emergency use ..... 17

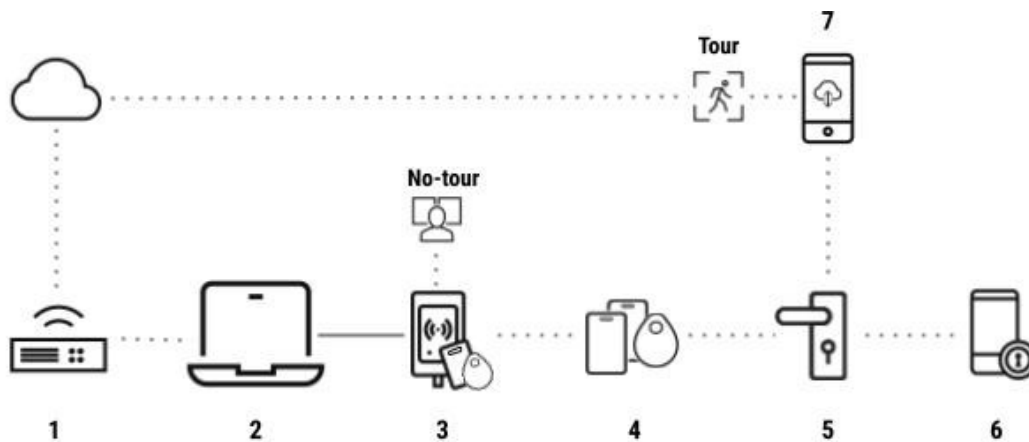
Assign entries to users .....	18
<b>Operation and maintenance .....</b>	<b>20</b>
Manually sync wireless locks with Control Center using Open Admin app .....	20
Unlock wireless locks using Openpath Mobile Access app .....	20
Deactivate user credentials (mark lost) .....	21
Delete all-access user credentials .....	21
Receive alerts by email or SMS .....	22
View dashboards and reports .....	22
View battery status using ENGAGE mobile app .....	23
<b>Troubleshooting .....</b>	<b>24</b>
Unable to swap to USB mode from Wi-Fi mode .....	24

# Before you start

Use the Avigilon Alta access control system integration with Allegion Schlage® wireless locks and ENGAGE™ technology to configure and manage LEB and NDEB series locks, and Control™ smart locks, without gateway hardware. They are offline locks with no connection to the cloud network.

## System overview

- Administrators or operators can visit the wireless locks in person (referred to as *tour*, see 7 below) and use the Open Admin app to sync the wireless locks with the Avigilon Alta access control system; update access rights when a keycard or fob is lost, or when a new tenant is moving in; and update firmware.
- Occupants can use programmed Schlage Smart Fob and keycard credentials, or Openpath mobile credentials using the Openpath Mobile Access app, to unlock entries and update their access rights without requiring the administrator or operator to tour the wireless lock (referred to as *no-tour*, see 3 below).



---

1 Access to Avigilon Alta cloud network

---

2a Avigilon Alta Control Center portal for provisioning wireless locks and access rights (referred to as the Control Center)

**Note:** Only no-tour wireless locks connected to an entry will be billed.

User schedules, entry schedules, entry states, Entry Open Duration setting, remote unlocking, and zone sharing are not applicable to no-tour wireless locks.

---

2b Allegion ENGAGE site, accessed on the Allegion ENGAGE mobile app, for commissioning the Schlage credential enrollment reader and wireless locks

---

- 
- 3 USB-connected Schlage credential enrollment reader for programming Schlage keycard and fob credentials

**Note:** Only USB communication mode is supported when provisioning the credential enrollment reader. Wi-Fi communication mode is not supported.

- 4 Schlage physical keycards and fobs, including Schlage MIFARE® DESFire EV3, and Proximity and Schlage MIFARE DESFire EV3

**Note:** A maximum of 11 entries is supported on each Schlage keycard or fob credential commissioned to the ENGAGE site. The maximum (also referred to as the credential sector limit) covers multiple zones in the same customer organization, and does not apply to Openpath mobile credentials.

If configured, Schlage fob and keycard credentials can be used on Schlage wireless locks that are connected to ENGAGE gateways.

- 
- 5a Battery-powered (offline) Schlage LEB and NDEB wireless locks, typically installed in offices and building amenities

- 5b Battery-powered (offline) Control Smart locks, typically installed in low-rise to mid-rise residences

- 
- 6 Openpath Mobile Access app and Openpath mobile credentials

- 7a Open Admin app for provisioning wireless locks, downloading audit logs, and updating wireless lock information

- 7b Allegion ENGAGE mobile app for commissioning the Schlage enrollment reader and wireless locks into the ENGAGE site, and viewing real-time battery status
- 

## Prerequisites

Contact your integrator to order the Allegion Schlage hardware and to set up a customer organization in the Control Center with the Allegion licenses, credential enrollment readers, and no-tour wireless locks. Connecting to a gateway is not required for these offline locks.

## System requirements

**Note:** Upgrading to the newest Avigilon Alta (formerly Openpath) software releases is recommended to benefit from the latest features in the system integration.

- Avigilon Alta Control Center account
  - Schlage Wireless Locks app from App marketplace
- Open Admin app version 1.6.0 or newer
  - iOS 11.4 or newer for Apple® iPhone® and iPad® mobile devices
  - Android™ 5 or newer for smartphones
- Openpath Mobile Access app version 2.7.0 or newer
  - iOS 12.4 or newer for Apple iPhone and iPad mobile devices
  - Android 6 or newer for smartphones
- Allegion ENGAGE Managed Properties
  - Allegion ENGAGE account
  - ENGAGE software revision 8.1.0
  - ENGAGE mobile application
    - Revision 3.3.142 for iOS 11.1 or newer
    - Revision 4.6.30 for Android 6 or newer
  - LEB wireless mortise lock revision 03.09.09
  - NDEB wireless cylindrical lock revision 03.09.09
  - Control Smart lock revision 04.10.01
  - MT20W enrollment reader revision 40.05.00



## For more information

### Technical support

For additional support documentation, see [help.openpath.com](https://help.openpath.com).

### Product documentation

For additional product documentation, see [avigilon.com/product-documentation](https://avigilon.com/product-documentation).

For information about installing, configuring, and using third-party devices, see [us.allegion.com/en/home/document-library.htm](https://us.allegion.com/en/home/document-library.htm).

- [Schlage ENGAGE Managed Property User's Guide](#)<sup>1</sup>
- [Schlage Enrollment Reader User Guide \(MT20W\)](#)<sup>2</sup>
- [Schlage installation videos](#)<sup>3</sup>

---

<sup>1</sup>See: [https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage\\_ENGAGE\\_User\\_Guide\\_113180.pdf](https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_ENGAGE_User_Guide_113180.pdf)

<sup>2</sup>See: [https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage\\_MT20W\\_Enrollment\\_Reader\\_User\\_Guide\\_111006.pdf](https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_MT20W_Enrollment_Reader_User_Guide_111006.pdf)

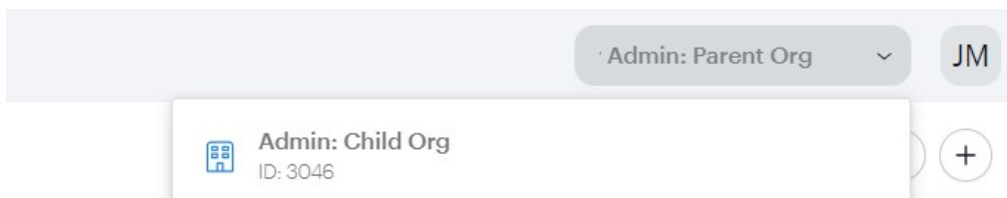
<sup>3</sup>See: <https://www.youtube.com/playlist?list=PLAjG-vLrfaPz6b6UacyckzgXZOeeZvT6>

# Step 1: Set up customer organization and Allegion licenses

1. Register for a partner account (<https://openpath.jotform.com/230034075150845>).

When you receive an invitation in your email inbox to set up your partner account, click the link to change the temporary password for your Avigilon Alta Control Center account.

2. Sign in to [control.openpath.com/login](https://control.openpath.com/login).
3. Ensure your **Partner** organization is selected in the upper-right corner.




4. Create an organization for your customer.
  - a. Select **Partner center** > **Manage organizations**.
  - b. Click the **+** button to enter customer information.
5. Select **Store access** and order the Allegion license and devices for a customer organization.

Options	Procedure
Order online	Select the <b>order online</b> link. Select <b>License</b> , the customer organization, and the term of the license. Click <b>Submit</b> .
Upload PO	Select the <b>digital orders portal</b> link, fill in the order form, upload the PO, and click <b>Submit</b> .
Email sales	Sales@openpath.com

The third-party device credentials will be imported in to the Control Center.

## Step 2: Sign in to ENGAGE site, download ENGAGE mobile app, and sync ENGAGE account with Control Center

**Note:** You can skip this step, if you are not programming Schlage keycards and fobs, or if you already have an ENGAGE account and the ENGAGE app.

1. Sign in to [control.openpath.com/login](https://control.openpath.com/login).
2. Go to  **Devices** > **Wireless locks**.
3. Click the **Send invite** button. An ENGAGE invitation email is sent to your inbox. Click **Accept This Invite** and the terms and conditions.
4. Sign in to the ENGAGE site using your ENGAGE account.

If you need to create an account, enter your information and click **Submit**.

5. Install and configure the Allegion ENGAGE app on your mobile device.

Go to  or .

6. Click the **Reload** button.

Your ENGAGE account is synced with the Control Center.

# Step 3: Add Schlage devices to ENGAGE site using ENGAGE mobile app, and sync with Control Center

**Note:** Schlage devices, such as the credential enrollment readers and wireless locks, can only be added to the ENGAGE site using the ENGAGE mobile app.


When provisioning a credential enrollment reader on the Communication Mode page in the ENGAGE mobile app, ensure `ozone.prod.openpath.com` is entered in the DNS Server field on the USB page. Wi-Fi mode is not supported.

Use your ENGAGE account and follow the on-screen instructions to add the Schlage devices to the ENGAGE site. For more information, see the installation and commissioning procedures in Schlage documentation.

## Install Schlage Wireless Locks app

If not already installed, do the following:


1. Sign in to the Control Center.
2. Go to  **App marketplace** > **Get apps**, click the **Schlage Wireless Locks** tile and then + **Get app**.

On the license purchasing page, add the licenses to the cart and check out. After the app is installed, the Schlage wireless device options are displayed on the  **Devices** page.



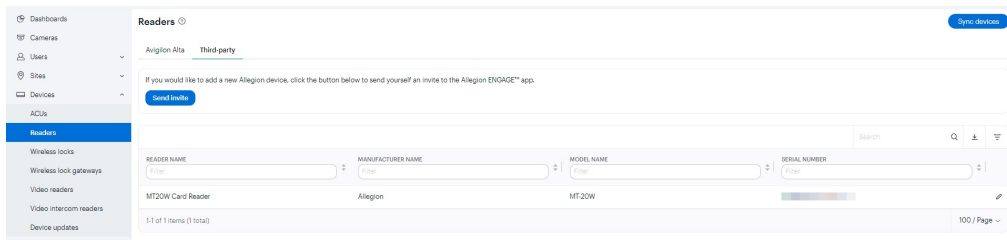
## Sync credential enrollment readers with Control Center

After completing the Schlage procedures, you can sync the Schlage credential enrollment readers with the Control Center.

1. Sign in to the Control Center.
2. Go to  **Devices** > **Readers** and select the **Third-party** tab.

### 3. Click **Sync devices**.

The credential enrollment readers are displayed. You may begin to program credentials onto the Schlage keycards or fobs.

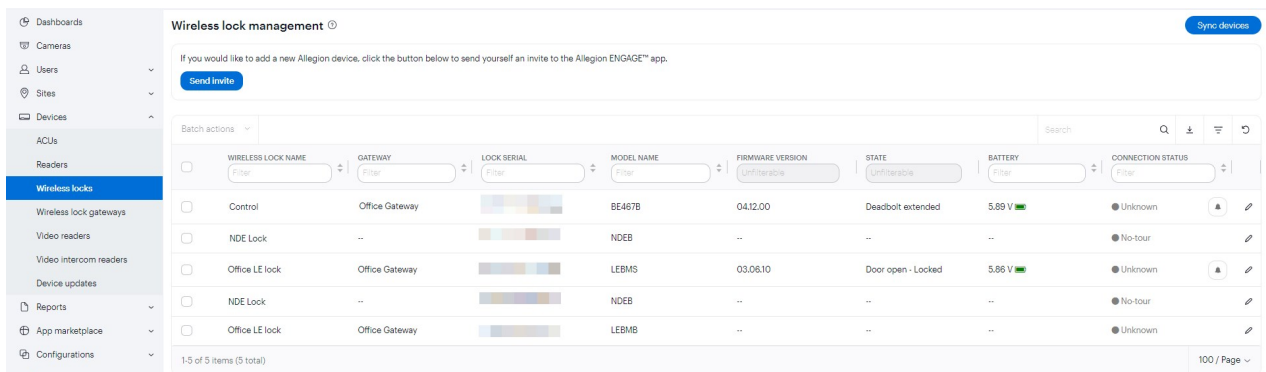


## Sync wireless locks with Control Center

After completing the Schlage procedures, you can sync the Schlage wireless locks with the Control Center.

1. Sign in to the Control Center.
2. Go to **Devices > Wireless locks**.
3. Click **Sync devices**.

The wireless locks are displayed. The colored circle indicates the lock connection status.





**Note:** No-tour wireless lock information is displayed only after a manual sync by visiting the lock in person, as described in [Manually sync wireless locks with Control Center using Open Admin app on page 20](#). Gateway and firmware information are not applicable. For real-time battery information, see [View battery status using ENGAGE mobile app on page 23](#).

## Edit wireless lock information

1. Select a lock and edit the name or serial number.
2. Click **Save**.

# Step 4: Assign wireless locks to entries and zones in Control Center



## Add entries

1. Sign in to the Control Center.
2. Go to  **Sites > Entries**.
3. Click the  button in the upper-right corner.
4. Select **Schlage** and the name of the LEB, NDEB, or control lock in the **Schlage wireless lock** field.

**Note:** The Entry Open Duration and Entry state settings are not applicable to no-tour wireless locks.

5. Enter the required information depending on the device and click **Save**.

## Add zones

1. Go to  **Sites > Zones**.
2. Click the  button in the upper-right corner.
3. Enter a **Name** and description (optional), and select the **Site** to which the zone will be assigned.

**Note:** A zone can only be assigned to one site, but a site can have multiple zones assigned to it. A zone can include a mix of Avigilon locks and Schlage wireless locks.


4. Optional. Add **Access groups** and **Users** to the zone.
5. For Schlage no-tour wireless locks only. In the **Entries** list, click and drag the no-tour locks installed in the zone (left pane) to the zone list (right pane).
6. Optional. If you want to share this zone with a different organization, enter the Org IDs.
7. Click **Save**.

# Step 5: Issue credentials and entries to users in Control Center

## Issue no-tour Schlage user credentials

1. Sign in to the ENGAGE mobile app.

**Note:** Keep the ENGAGE mobile app open throughout the enrollment process to ensure the credential is issued to the user in the Control Center.

- a. Plug the credential enrollment reader into the USB port on your desktop computer.
  - b. Scan the keycard or key fob using the credential enrollment reader.
2. Sign in to the Control Center.
  3. Go to  **Users > Users** and select a user.
    - a. Select the **Credentials** tab.
    - b. Select the **Card: Schlage** user credential.
    - c. Select the badge number from **Badge ID**. Ensure it matches the number printed on the physical keycard or fob.


The No-tour checkbox is selected. The card serial number (CSN) is displayed.

**Note:** The CSN and Badge ID are the unique identifiers of a credential.

- d. Enter the required information depending on the device.
  - e. Click **Save**.
- The credential enrollment reader flashes blue when the user credential is saved to the keycard or fob.
4. Tour the wireless lock to update the lock information, as described in [Manually sync wireless locks with Control Center using Open Admin app on page 20](#).





## Issue Openpath mobile credentials

1. Sign in to the Control Center.
  - a. Select  **Users** > **Users** and select a user.
  - b. On the **Credentials** tab, select the **Mobile** user credential.
  - c. Enter the required information depending on the device and click **Save**.
  - d. Click **Send** to email instructions to the user on how to set up their mobile device as a credential. The Activation Pending column indicates that an email has been sent, but the user has not yet activated their mobile credential. Or click **Resend** to issue another mobile credential to a new mobile device.
2. Instruct the user to go to the inbox on their mobile device, follow the instructions to install the Openpath Mobile Access app, and activate the mobile credential.
3. Tour the wireless lock to update lock access using the Open Admin app, as described in [Manually sync wireless locks with Control Center using Open Admin app on page 20](#).

## Issue all-access credentials for emergency use


An all-access credential can be used by first responders in emergency situations to access every entry in all the zones in a site, where no-tour wireless locks are installed. (An all-access credential works like a credential for gateway-connected wireless locks.)

1. Sign in to the Control Center.
  - a. Go to  **Users** > **Users**.
  - b. Click the  button in the upper-right corner.
  - c. Enter the all-access user's information and click **Save**.
  - d. On the **Credentials** tab, select any type of credential, and click **Save**.

**Note:** If a Schlage keycard or fob is selected, do not select the No-tour checkbox.


- e. On the **Access** tab, do one of the following:

- In **Access groups**, assign the access group for the all-access credential to the all-access user and enter a checkmark next to all the zones in a site in the GROUP ACCESS column. Click **Save**.

If you need to create an access group for the all-access credential, go to  **Users > Access groups** and add the all-access user to the new access group. Assign the access group to all the zones in the site, and click **Save**.

- In the USER ACCESS column, enter a checkmark next to all the zones in a site and click **Save**.
- f. Enable **Override permission** to give the user permission to unlock entries in the Lockdown (Override Only) state. Click **Save**.
2. Sync every no-tour wireless lock in all the zones on site using the Open Admin app, as described in [Manually sync wireless locks with Control Center using Open Admin app on page 20](#).

## Assign entries to users

1. Sign in to the Control Center.
2. Go to  **Users > Users** and select a user.
3. Select the **Access** tab.
4. You can assign up to 11 entries across multiple zones in the same customer organization.

**Note:** A zone can include a mix of Avigilon locks and Schlage wireless locks. The 11 entry limit is not applicable to Openpath mobile credentials. User schedules and zone sharing between customer organizations are not applicable.

**Tip:** If more credentials are needed, you can remove the assignment of unused entries or issue Openpath mobile credentials.

5. Click **Save**.

The key card or key fob is programmed for access at the entries.

The  entry is displayed in the Openpath Mobile Access app on the user's mobile device.

**Tip:** Allow time for the screen to refresh.

# Operation and maintenance

## Manually sync wireless locks with Control Center using Open Admin app

Visit the no-tour wireless lock in person (weekly, monthly, or as needed) and use the Open Admin app to update access rights, download audit logs, retrieve lock events, and more. This task frees up the onboard memory.

1. Sign in to the Open Admin app on your mobile device.
2. Tap the customer organization.
3. Tap **3rd Party Devices** and then **No-Tour Wireless Locks**.

**Note:** You can only connect to locks that are within bluetooth range. If 'out of range' is displayed, move closer to the lock.


4. Tap **CONNECT** next to the lock.
5. Tap the **Sync** button.


**Note:** Keep the app open until the sync is complete.

Lock information is available in the Control Center.

## Unlock wireless locks using Openpath Mobile Access app

**Note:** Users must be within bluetooth range of the lock for the best performance.



1. Sign in to the Openpath Mobile Access app on your device.
2. Go to the list of entries and tap the  entry tile for the entry to be unlocked.

The  is displayed. Lock access is updated automatically.

## Deactivate user credentials (mark lost)

If a user loses or no longer needs access to a **Card: Schlage** credential, deactivate the user credential. A credential that is marked lost cannot be deleted.

If you are deactivating an all-access user credential, see [Delete all-access user credentials below](#).



1. Sign in to the Control Center.
  - a. Go to  **Users > Users** and select the user.
  - b. On the **Credentials** tab, select the  button.
  - c. Enter a checkmark in the **Lost** checkbox.
  - d. Click **Save**.
2. To assign a new credential, see [Issue no-tour Schlage user credentials on page 16](#).

The credential is deactivated when any of the following occurs:

- The lost keycard or fob, or replacement keycard or fob, is placed on the wireless lock.
- The lock information is synced manually by touring the lock, as described in [Manually sync wireless locks with Control Center using Open Admin app on the previous page](#).


## Delete all-access user credentials

If a user loses an all-access credential, you can delete it and assign a new one.

1. Sign in to the Control Center.
  - a. Go to  **Users > Users** and select the user.
  - b. On the **Credentials** tab, click the  button next to the all-access credential.
  - c. Click **Yes**. The credential is deleted.
2. Assign a new all-access credential, as described in [Issue all-access credentials for emergency use on page 17](#).
3. Manually sync every no-tour wireless lock in all the zones on site using the Open Admin app, as described in [Manually sync wireless locks with Control Center using Open Admin app on the previous page](#).

## Receive alerts by email or SMS

**Note:** Alerts are generated only after touring the no-tour wireless lock in person and completing a manual sync. Alerts do not occur in real-time.

1. Sign in to the Control Center.
2. Go to  **Configurations > Alerts**.
3. Set up the following alerts for the no-tour wireless locks:

- **Billing**
- **Entry Ajar**
- **Entry Authentication Failure**
- **Entry Authorization Failure**
- **Entry Unlock Failure**
- **Entry Forced Open**
- **3rd Party Device Communication Lost**
- **3rd Party Device Battery Low/Critical**



For real-time battery status, see [View battery status using ENGAGE mobile app on the next page](#).

- **3rd Party Device Error Detected**
  - **3rd Party Device Tamper Detected**
4. Manually sync the wireless locks using the Open Admin app, as described in [Manually sync wireless locks with Control Center using Open Admin app on page 20](#).

The alerts are generated.

## View dashboards and reports

**Note:** Dashboard and report information are available only after visiting the no-tour wireless lock in person and completing a manual sync using the Open Admin app. Information may be out-of-date.

1. Sign in to the Control Center.
2. Go to  **Dashboards** and view any of the dashboards for the customer organization.
3. Go to  **Reports** and view the following reports for the no-tour wireless lock events:
  - **Activity logs**
  - **Alarms**
  - **Entry activity (by user)**
  - **Entry activity summary**
  - **User activity (by entry)**
  - **User activity summary**
4. Manually sync the wireless locks using the Open Admin app, as described in [Manually sync wireless locks with Control Center using Open Admin app on page 20](#).

The Dashboards and Reports pages are updated.

## View battery status using ENGAGE mobile app

**Note:** Real-time battery information is available only after visiting the no-tour wireless lock in person and completing a manual sync.

1. Sign in to the ENGAGE mobile app.
2. Go to **3rd Party Devices** and tap **No-Tour Wireless Locks**.
3. Select the lock and tap **CONNECT**.
4. Tap **Sync**.

The ENGAGE mobile app page is updated.

# Troubleshooting

## Unable to swap to USB mode from Wi-Fi mode

To resolve this issue, do the following:

- Recommission the credential enrollment reader in USB mode in the ENGAGE mobile app. Refer to Schlage documentation for more information. See also [Step 3: Add Schlage devices to ENGAGE site using ENGAGE mobile app, and sync with Control Center on page 12.](#)