

AVIGILON™
AVIGILON
XE360™ Access
Control System
Integration



AVIGILON XE360™ Access Control System Integration Owner's Manual

[Home](#) » [aVIGILON](#) » AVIGILON XE360™ Access Control System Integration Owner's Manual 

Contents

- 1 [AVIGILON XE360™ Access Control System Integration](#)
- 2 [Specifications](#)
- 3 [Frequently Asked Questions](#)
- 4 [Revisions](#)
- 5 [Before you start](#)
- 6 [Set up customer organization and Allegion licenses](#)
- 7 [Sign in to ENGAGE site, download ENGAGE mobile app, and sync ENGAGE account with Alta Access](#)
- 8 [Add Schlage devices to ENGAGE site using ENGAGE mobile app, and sync with Alta Access](#)
- 9 [Install Schlage Wireless Locks app](#)
- 10 [Assign wireless locks to entries and zones in Alta Access](#)
- 11 [Issue credentials and assign entries to users in Alta Access](#)
- 12 [Operation and maintenance](#)
- 13 [Troubleshooting](#)
- 14 [For more information](#)
- 15 [Documents / Resources](#)
 - 15.1 [References](#)

AVIGILON™

AVIGILON XE360™ Access Control System Integration



Specifications

- Model: XE360TM Series
- Lock Type: Wireless Locks
- Mobile Apps: ENGAGE desktop app, Avigilon Alta Open mobile app, Avigilon Alta Access mobile app

Frequently Asked Questions

Q: How do I troubleshoot issues related to syncing the wireless locks?

A: If you encounter problems with syncing, ensure that you are following the correct steps outlined in the user manual. Make sure your apps are updated, and if issues persist, contact technical support for assistance.

Q: Can I issue credentials using the Avigilon mobile apps?

A: Yes, you can issue Avigilon mobile credentials using the ENGAGE desktop app or the Alta Access mobile app. Refer to the specific instructions provided in the manual for detailed steps.

© 2024, 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.

Revisions

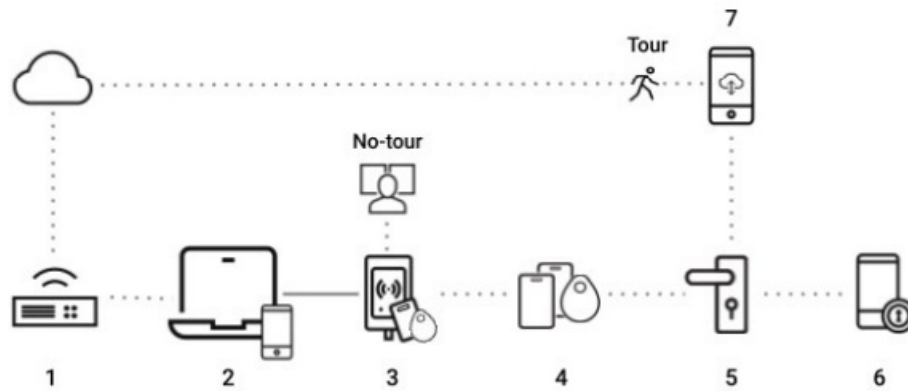
Guide	Description
December 2024	XE360™ Series lock model support: Before you start on For more information on System requirements
October 2024	Credentials report: View dashboards and reports on information or Show, hide, or reset ENGAGE desktop app updates: Before you start on , System requirements on Issue no-tour Schlage user credentials using ENGAGE desktop app and Alta Access or , Unable to swap to USB mode from Wi-Fi mode on Added Replace no-tour Schlage user credentials on
September 2024	Control Center portal renamed to Alta Access
April 2024	Avigilon Alta Open mobile app (formerly, Openpath Mobile Access app), Avigilon Alta Access mobile app (formerly, Open Admin app), version updates: System requirements or Important note about scanning the Avigilon No-Tour Configuration Card: 4b in System overview on , System requirements on Step 3: Add Schlage devices to ENGAGE site using ENGAGE mobile app, and sync with Alta Access on Upgrade and downgrade firmware steps: Upgrade or downgrade firmware using ENGAGE mobile app on
October 2023	Updated Issue Avigilon mobile credentials on ; added Troubleshooting on
August 2023	Initial release of guide

Before you start

Use the Avigilon Alta access control integration with Allegion Schlage® wireless locks and ENGAGE™ technology to configure and manage LEB, NDEB, XE360 Series, 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 Avigilon Alta Access mobile app to sync the wireless locks with Alta Access; 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 mobile credentials using the Avigilon Alta Open mobile 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. 1 Access to Alta Access cloud network

2. 2a Alta Access portal for provisioning wireless locks and access rights

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 Schlage credential enrollment reader and wireless locks, and the Allegion ENGAGE desktop app for updating Schlage physical keycards and fobs

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. 4a 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 Avigilon mobile credentials.

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

4b Avigilon No-Tour Configuration Card, which must be scanned using the enrollment reader each time a Schlage device is added (see 2b)

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

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

Battery-powered (offline) XE360™ Series locks, typically installed in multifamily units

Note: Wi-Fi communication mode is not supported.

6. Avigilon Alta Open mobile app and mobile credentials

7. 7a Avigilon Alta Access mobile 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, viewing real-time battery status, and upgrading or downgrading firmware


Prerequisites

Contact your integrator to order the Allegion Schlage hardware and to set up a customer organization in Alta Access 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 Alta Access software releases is recommended to benefit from the latest features in the system integration.

Alta Access system

- Alta Access account
- Schlage Wireless Locks app from  App marketplace



- Alta Access mobile app
Version 2.3.0 or newer
iOS 11.4 or newer for Apple® iPhone® and iPad® mobile devices Android™ 5 or newer for smartphones



- Alta Open mobile app
Version 3.0.1 or newer
iOS 11.4 or newer for Apple® iPhone® and iPad® mobile devices Android™ 5 or newer for smartphones



- Avigilon No-Tour Configuration Card

Card	Ordering Part Number
No-Tour Configuration Card for Schlage wireless locks that do not connect to an ENGAGE gateway	OP-CE-051-849
EV3-A Configuration Card for Schlage wireless locks that connect to an ENGAGE gateway	OP-CE-050-966
EV3-B Configuration Card for Schlage wireless locks that connect to an ENGAGE gateway	OP-CE-051-850
Card	Ordering Part Number

- Allegion ENGAGE system
 - Allegion ENGAGE account
 - ENGAGE software
Release 8.1.0; desktop application
 - ENGAGE mobile application
3.3.142 for iOS 11.1 or newer



- Wireless locks
- Credential enrollment reader
 - Wireless locks

Model	Ordering Part Number
LEB wireless mortise lock Version 3.10.01 or 03.11.02 (recommended)	OP-LOCK-LE
NDEB wireless cylindrical lock Version 03.10.01 or 03.11.02 (recommended)	OP-LOCK-NDE
Control Smart lock Version 04.12.00 (FE410B, BE467B) or Version 05.11.39 (FE410BM, BE467BM; recommended)	OP-LOCK-FE OP-LOCK-BE
XE360 Series wireless mortise lock	AC-ALTA-SCH-XE360-M-CUSTOM
XE360 Series wireless mortise deadbolt	AC-ALTA-SCH-XE360-M-D-CUSTOM
XE360 Series wireless tubular lock	AC-ALTA-SCH-XE360-T-CUSTOM
XE360 Series wireless exit trim	AC-ALTA-SCH-XE360-EW-CUSTOM

- Credential enrollment reader

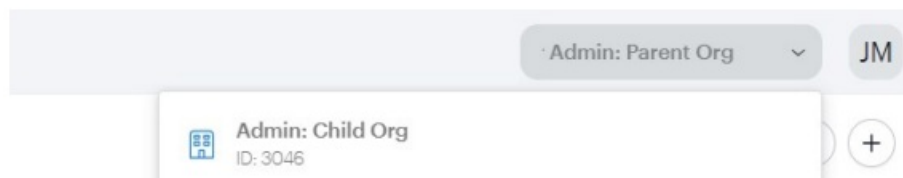
Model	Ordering Part Number
MT20W credential enrollment reader Release 40.05.00	ALGN-MT20W



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 Alta Access account.

2. Go to control.openpath.com/login and sign in.
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 order online link. Select License , the customer organization, and the term of the license. Click Submit .
Upload PO	Select the digital orders portal link, fill in the order form, upload the PO, and click Submit .
Email sales	Sales@openpath.com

The third-party device credentials will be imported in to Alta Access

Sign in to ENGAGE site, download ENGAGE mobile app, and sync ENGAGE account with Alta Access

Note: You can skip this step, if you are not programming Schlage keycards or fobs; if you are using only Avigilon mobile credentials; or if you already have an ENGAGE account and the ENGAGE app.

1. Go to control.openpath.com/login and sign in.
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.



6. Click the Reload button.
Your ENGAGE account is synced with Alta Access.

Add Schlage devices to ENGAGE site using ENGAGE mobile app, and sync with Alta Access

Add and configure Schlage devices

Use your ENGAGE account and follow the on-screen instructions to add the Schlage devices, such as the credential enrollment readers and wireless locks, to the ENGAGE site. For more information, see the installation and commissioning procedures in Schlage documentation.



Note: Schlage devices can only be added to the ENGAGE site using the ENGAGE mobile app. When provisioning a credential enrollment reader on the Communication Mode in the ENGAGE mobile app, ensure ozone.prod.openpath.com is entered in the DNS Server group membership admin field on the USB . Wi-Fi mode is not supported.

Important: Each time you add a Schlage device to the ENGAGE site, remember to complete these steps:

1. Scan the Avigilon No-Tour Configuration Card (OP-CE-051-849) using your credential enrollment reader.
2. Sync the devices with Alta Access. See Sync credential enrollment readers with Alta Access on the or Sync wireless locks with Alta Access on the.

Install Schlage Wireless Locks app

If not already installed, do the following:

1. Go to control.openpath.com/login and sign in.
2. Go to  App marketplace > Get apps, click the Schlage Wireless Locks tile and then + Get app.
3. On the license purchasing , add the licenses to the cart and check out.
4. After the app is installed, the Schlage wireless device options are displayed on the  Devices.

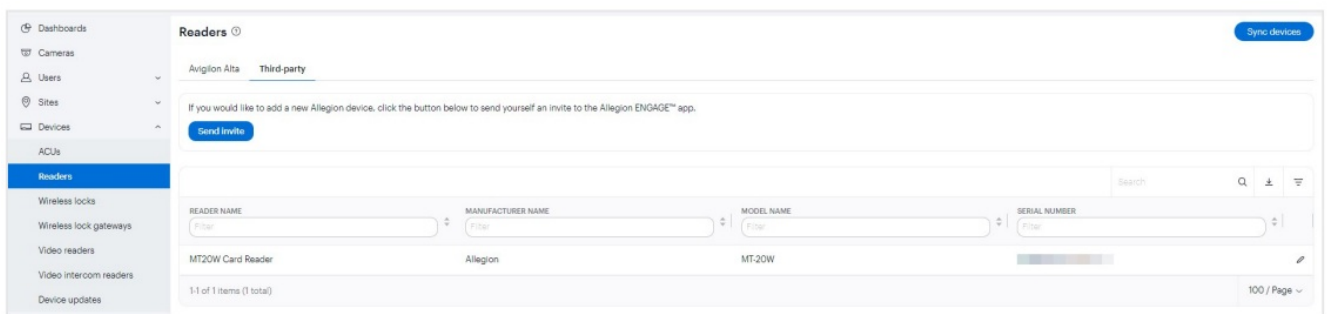


Sync credential enrollment readers with Alta Access

After completing the Schlage procedures including scanning the Avigilon No-Tour Configuration Card, you can sync the Schlage credential enrollment readers with Alta Access.


1. Go to control.openpath.com/login and sign in.
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. See Step 5: Issue credentials and assign entries to users in Alta Access



Sync wireless locks with Alta Access

After completing the Schlage procedures including scanning the Avigilon No-Tour Configuration Card, you can sync the Schlage wireless locks with Alta Access.

1. Go to control.openpath.com/login and sign in.
2. Go to  Devices > Wireless locks.
3. Click Sync devices.

The wireless locks are displayed. The lock connection status is always gray for wireless locks that work in Notour mode.

Wireless lock management Sync devices

If you would like to add a new Allegion device, click the button below to send yourself an invite to the Allegion ENGAGE™ app.

[Send invite](#)

Batch actions	WIRELESS LOCK NAME	GATEWAY	LOCK SERIAL	MODEL NAME	FIRMWARE VERSION	STATE	BATTERY	CONNECTION STATUS
<input type="checkbox"/>	Control	Office Gateway		BE467B	04.12.00	Deadbolt extended	5.89 V	Unknown
<input type="checkbox"/>	NDE Lock	--		NDEB	--	--	--	No-tour
<input type="checkbox"/>	Office LE lock	Office Gateway		LEBMS	03.06.10	Door open - Locked	5.86 V	Unknown
<input type="checkbox"/>	NDE Lock	--		NDEB	--	--	--	No-tour
<input type="checkbox"/>	Office LE lock	Office Gateway		LEBMB	--	--	--	Unknown

1-5 of 5 items (5 total) 100 / Page



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 Alta Access using the Alta Access mobile app on](#). Gateway and firmware information are not applicable. For real-time battery information, see [View battery status using ENGAGE mobile app on](#).

Edit wireless lock information



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

Assign wireless locks to entries and zones in Alta Access

Add entries

1. Go to control.openpath.com/login and sign in.
 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.
 6. 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).
 4. 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.
5. Optional. Add Access groups and Users to the zone.
 6. 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).

7. Optional. If you want to share this zone with a different organization, enter the Org IDs.
8. Click Save.

Issue credentials and assign entries to users in Alta Access

Issue no-tour Schlage user credentials using ENGAGE desktop app and Alta Access

1. Sign in to the ENGAGE desktop app.

Note: Keep the ENGAGE desktop app open throughout the enrollment process to ensure the credential is issued to the user in Alta Access.

- 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. Go to control.openpath.com/login and sign in.

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.


For more information, see [Manually sync wireless locks with Alta Access using the Alta Access mobile app](#) on.

Replace no-tour Schlage user credentials

Tip: A credential can be replaced by having the administrator re-scan the keycard or fob using the credential enrollment reader.

Issue Avigilon mobile credentials

1. Go to control.openpath.com/login and sign in.

- 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. 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 Alta Open mobile app, and activate the mobile credential.



3. Tour the wireless lock to update the lock information.

For more information, see [Manually sync wireless locks with Alta Access using the Alta Access mobile app](#) on.

Issue all-access credentials for emergency use

An all-access (formerly, master) 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. Go to control.openpath.com/login and sign in.

- 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 Alta Access mobile app.

For more information, see [Manually sync wireless locks with Alta Access using the Alta Access mobile app](#).

Assign entries to users

1. Go to control.openpath.com/login and sign in.

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 Avigilon 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 Avigilon mobile credentials.

5. Click Save.

The keycard or fob is programmed for access at the entries.



The  entry is displayed in the Alta Open mobile app on the user's mobile device.

Tip: Allow time for the screen to refresh

Operation and maintenance

Manually sync wireless locks with Alta Access using the Alta Access mobile app

Visit the no-tour wireless lock in person (weekly, monthly, or as needed) and use the Alta Access mobile 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 Alta Access mobile app.
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 Alta Access portal.


Unlock wireless locks using Alta Open mobile app

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

1. Sign in to the Alta Open mobile 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

1. Go to control.openpath.com/login and sign in.
 - 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 using ENGAGE desktop app and Alta Access.

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.

For more information, see Manually sync wireless locks with Alta Access using the Alta Access mobile app.

Delete all-access user credentials

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

1. Go to control.openpath.com/login and sign in.

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.

For more information, see [Issue all-access credentials for emergency use on](#).

3. Manually sync every no-tour wireless lock in all the zones on site using the Alta Access mobile app.

For more information, see [Manually sync wireless locks with Alta Access using the Alta Access mobile app](#)

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. Go to control.openpath.com/login and sign in.

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](#).

- 3rd Party Device Error Detected
- 3rd Party Device Tamper Detected

4. Manually sync the wireless locks using the Avigilon Alta Access mobile app.


For more information, see [Manually sync wireless locks with Alta Access using the Alta Access mobile app](#)

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 Alta Access mobile app. Information may be out-of-date.

1. Go to  control.openpath.com/login and sign in.

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
- Credentials — Select Card: Schlage in Credential management.
- Entry activity (by user)
- Entry activity summary
- User activity (by entry)
- User activity summary

4. Manually sync the wireless locks using the Alta Access mobile app.

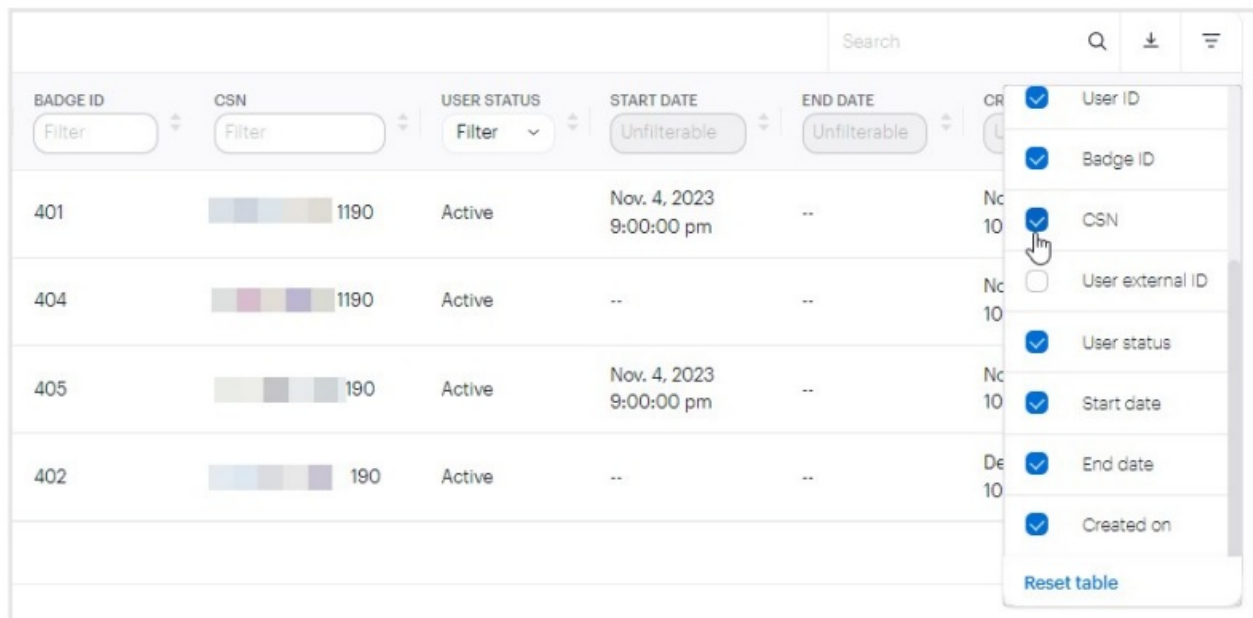
For more information, see [Manually sync wireless locks with Alta Access using the Alta Access mobile app](#)




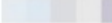
The Dashboards and Reports are updated.

Show, hide, or reset information

- Click the  icon to show or hide information in columns.
- Click Reset table to go back to the default view.

For example, show the CSN column for Schlage card credentials in Credential management.



BADGE ID	CSN	USER STATUS	START DATE	END DATE	CR
401	 1190	Active	Nov. 4, 2023 9:00:00 pm	--	No
404	 1190	Active	--	--	No
405	 190	Active	Nov. 4, 2023 9:00:00 pm	--	No
402	 190	Active	--	--	De

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 is updated.

Upgrade or downgrade firmware using ENGAGE mobile app

Note: You need to visit the no-tour wireless lock in person to upgrade or downgrade ENGAGE firmware. If you have installed a firmware version that is not recommended in System requirements, you can downgrade the installation to the recommended version using the same steps as the upgrade.

1. Sign in to the ENGAGE mobile app.
2. Select the lock from the Devices list and tap Update Firmware.
3. Tap and hold the Update button to view a list of firmware versions.

Note: Tapping without holding the Update button will update to the latest ENGAGE firmware version, which may not be the recommended version.

4. Select the recommended firmware for your device.

The current firmware version 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 using the USB data transfer option during setup 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 Alta Access.

For troubleshooting information, see this [Alta Access article](#).

For more information

Technical support

For additional support documentation, see support.avigilon.com.

Product Documentation

For additional product documentation, see the Alta Access (Cloud Solutions) product suite on avigilon.com.

For troubleshooting information, see this [Alta Access article](#).

Third-party documentation

For information about installing, configuring, and using third-party devices, see

us.allegion.com/en/home/document-library.htm.

- [Schlage ENGAGE Managed Property User's Guide1](#)
 - [Schlage XE360 Series User Guide2](#)
 - [Schlage Enrollment Reader User Guide \(MT20W\)3](#)
 - [Schlage installation videos4](#)
1. See: https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_ENGAGE_User_Guide_113180.pdf
 2. See: https://us.allegion.com/content/dam/allegion-us-2/web-files/schlage/technical-documents/Schlage_XE360-Series_User_Guide_115598.pdf
 3. See: https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_MT20W_Enrollment_Reader_User_Guide_111006.pdf
 4. See: <https://www.youtube.com/playlist?list=PLAjG-vLrfaPz6b6UacyckzgXZOeeZvT6>

Documents / Resources



AVIGILON
Access Control
System Integration Guide for Soligraff Wireless Locks
Rev. 1.0

[AVIGILON XE360TM Access Control System Integration](#) [pdf] Owner's Manual
XE360TM Access Control System Integration, XE360TM, Access Control System Integration, C
ontrol System Integration, System Integration, Integration

References

- [End-to-End Security Solutions | Avigilon \(Openpath & Ava\)](#)
- [Avigilon Support Community](#)
- [Avigilon Support Community](#)
- [Document Library](#)
- [Access](#)
- help.openpath.com/space/EHC/2333278211/Allegion+Wireless+Lock+Troubleshooting+Guide
- [Document Library](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.