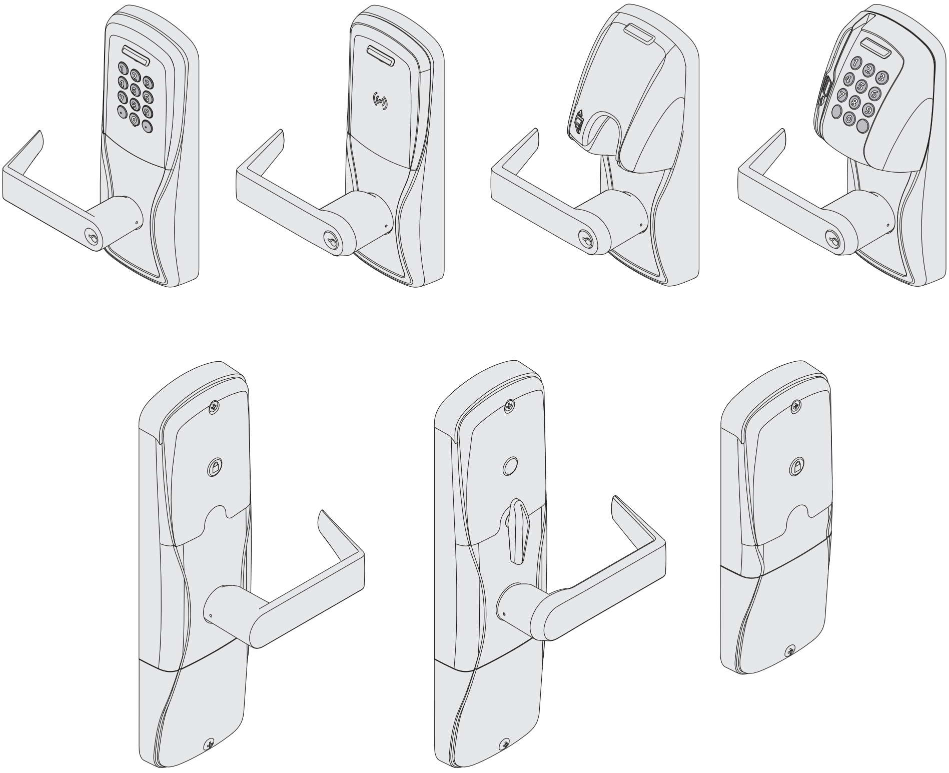
P516-129

AD-200
AD-201

Offline lock user guide

Instructions for AD-Series offline locks



Para el idioma español, navegue hacia www.allegion.com/us.
Pour la portion française, veuillez consulter le site www.allegion.com/us.

Contents

This product is compliant of UL 294 and ULC S319 standard. This product's compliance would be invalidated through the use of any add-on, expansion, memory or other module that has not yet been evaluated for compatibility for use with this UL Listed product, in accordance with the requirements of the Standards UL 294 and ULC S319. This product has been evaluated for CAN/ULC-S319 Class 1.

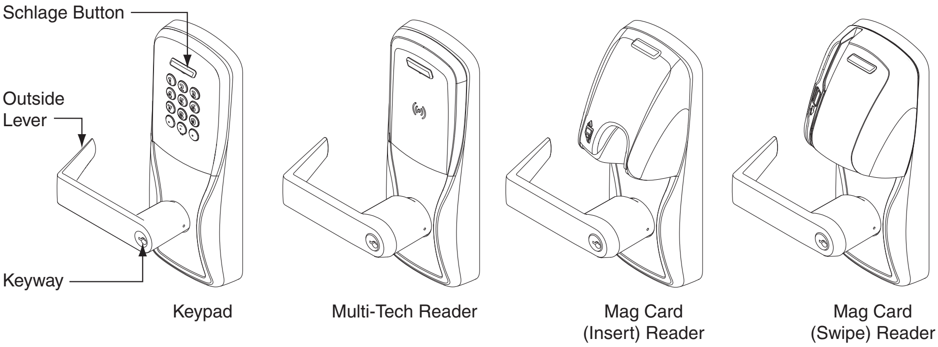
Overview

The Schlage AD-200/AD-201 is an off-line electronic lock in the AD-Series product line.

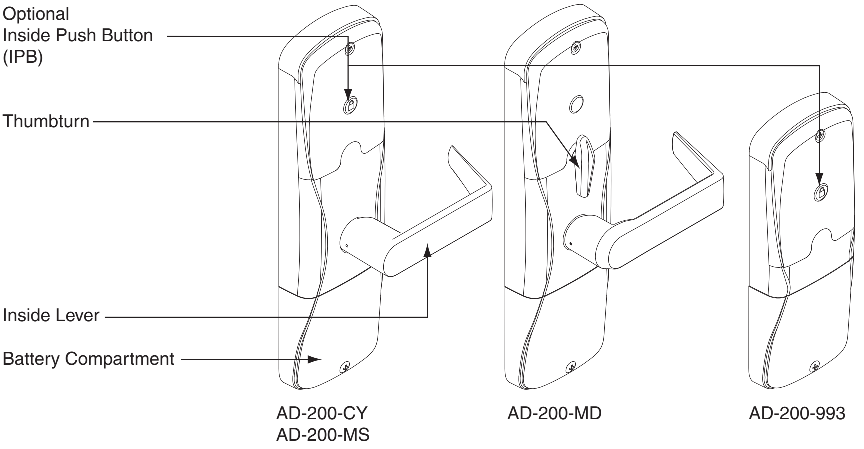
The Schlage AD-201 is a FIPS-201-1 certified off-line electronic lock.

- May be powered by batteries or connected to external power using a UL294 or ULCS318/ULCS319 listed power supply capable of sourcing at least 250 mA @ 12 or 24 VDC. See *Batteries* on page 16, or *External power supply* on page 17 for more information.
- Outside lever is normally locked.
- Inside lever always allows egress.
- The lock maintains an audit trail of events.
- Configured using the Schlage Utility Software (SUS).

Outside



Inside



Additional AD-200 reader options: Mag + Keypad, Multi-Tech + Keypad

Note: Proximity card (PR, PRK) ONLY and Smart card (SM, SMK) ONLY readers have been discontinued and replaced by the Multi-Tech (MT, MTK) readers that provide all the same funcionality as the original Proximity and Smart card readers in a single credential reader.

The AD-201 reader is a FIPS-201-1 certified Multi-Tech + Keypad (FMK) reader.

Lock functions

The AD-200/AD-201 is available in one of four functions:

Privacy (40): Lockset is normally secure. Pressing the Inside Push Button or extending the deadbolt will disable normal electronic access from the outside. Opening the door, retracting the deadbolt or pressing the Inside Push Button a second time deactivates the privacy status.

Office (50): Lockset is normally secure. Inside Push Button may be used to select passage or secured status.

Apartment (60): Lockset is normally secure. Inside Push Button is used to select passage or secure status. While in the secure state, opening the door or pressing the Inside Push Button causes the lockset to toggle unsecured. The door must be closed and a valid credential presented to secure the lockset from the outside.

Classroom/Storeroom (70): Lockset is normally secure. Valid toggle credentials may be used to change to a passage or secure status.

Getting started

Follow these steps when setting up a new lock.

1. Install the lock. See the installation guide that came with the lock, or visit www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library) for more information.
2. Make sure the batteries are installed properly. See *Batteries* on page 16 for instructions.
3. Configure the master construction credential (where applicable). See *Construction access mode* on page 5 for more information. The lock should remain in construction access mode until you are ready to set up the rest of the system.
4. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 13 for more information.
5. When ready to set up for normal use, program the user credentials. ***See*** *Credential types and functions* ***on page 6 for more information.***

ⓘ **Programming the lock with the SUS will remove all credentials that were added using the master construction credential.**

6. Consult the SUS user guide for information about configuring the lock.
7. Familiarize yourself with the information in this guide.

Save this user guide for future reference.

Schlage Utility Software (SUS)

The Schlage Utility Software is used for programming and setup only.

The SUS is used to configure locks. This includes transferring data files between the access control software and locks. For information about the SUS, refer to the SUS user guide.

Construction access mode

Construction access mode is used to allow access before the lock has been programmed, and for testing purposes.

- Enabled by default.
- The lock will remain in construction access mode until the mode is cancelled as described below.
- No audits are captured while lock is in construction access mode.
- Use the same master construction credential for all the locks in the facility.
- If you present the first card to a new lock to create the master construction credential and the card is not accepted, the lock has either been programmed or already has a master construction credential.
- If the master construction credential cannot be located, or to put the lock back into construction access mode, reset the lock to factory settings (see page 15 for details).

Locks with keypads – Construction access mode

In the factory default state, locks with keypads have a default PIN of 13579 and "#", which can be used for installation, testing and construction access. To test, enter default PIN. The Schlage button will blink and the lock will unlock.

The default PIN, 13579 and "#" is automatically deleted when a construction access user credential is added to the lock, or a new programming credential is created, or the lock is programmed with the SUS.

Locks with card readers – Create a master construction credential

The master construction credential is used to program construction access mode credentials.

To create a master construction credential:

1. Press and hold the Schlage button while presenting a credential.
2. The Schlage button will blink green on the left and right as confirmation.
3. Use this card to add construction access mode user credentials.

ⓘ **The master construction credential will not grant access. It is used only to add additional credentials.**

Locks with card readers – Add construction access mode user credentials

Construction access mode credential type	Steps to add construction access mode user credentials				
	1	2	3	4	5
Normal use construction credential Unlocks the lock for relock delay period	Present master construction credential to reader ➔	Green LEDs blink ➔	Present user credential within 20 seconds ➔	Green LEDs blink and credential is added ➔	Repeat steps 3 and 4 for additional credentials. Credentials added with the master construction credential will have 24/7 access.
Toggle construction credential Changes the state of lock from locked to unlocked or vice versa	Present master construction credential to reader ➔	Green LEDs blink ➔	Press and hold Schlage button while presenting user credential within 20 seconds ➔	Green LEDs blink, 2 beeps will sound and credential is added ➔	

Cancel construction access mode

Do one of the following:

- Program the lock with the SUS. See the SUS user guide for more information.
- Reset the lock to factory settings. See *Reset to factory defaults* on page 15 for more information.

When construction mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.

Credential types and functions

Programming credential: A card or 5 digit code used only for lock programming.

Card or PIN credentials: A card that is presented, or a 3-6 digit code entered on the keypad.

Card ID number: When adding any new card credential, a 3-6 digit code is entered prior to presenting the card. This code becomes the Card ID Number. This number can be used to delete a card credential without physically having the card. *Keep a log of all Card ID Numbers for future reference.*

Note: A unique credential must be used for each credential type described below (for example, a single credential may not be used for both normal use and toggle functions).

Credential type	Function
Programming PIN or card	Used only to program the lock. Does not unlock the lock.
Normal use credential	Unlocks the lock *momentarily* after a credential is presented or entered.
Toggle credential	Changes the state of the lock from locked (secured) to unlocked (unsecured), or vice versa, unless in a Freeze state.
Freeze credential	Freezes the lock in the current state. The lock remains frozen until any Freeze credential is presented again. (A pass-through credential will override a lock in frozen state as described below).
Pass-through credential	Unlocks a lock *momentarily*, regardless of state. A valid Pass-through credential can unlock a door set to any secured lockout mode (e.g., Freeze, Privacy, Time Zones, Door Auto-Locks and Holidays). The door will relock after the specified relock time.

Credential forms

Normal, toggle, freeze and pass-through credential types are used in one of three forms:

PIN credential – a 3-6 digit code entered on the keypad.
CARD credential – a card presented to the lock.
CARD + Card ID Number credential – a card (with a unique Card ID number) presented to the lock. (See a description of Card ID number above for more information.)

Steps for designating each form are in the *Manual programming instructions* on the following pages.

Manual programming instructions

Important notes:

- ⓘ **Wait for the Schlage button LEDs to stop flashing before continuing to the next step.**
- ⓘ **Programming mode will time out if no entry is made in 20-25 seconds. Time out is indicated by three left and nine right red blinks of the Schlage button.**
- ⓘ **An incorrect entry is indicated by a solid red left and blinking green right LED on the Schlage button. Refer to *Error codes* on page 12 to interpret error code patterns.**
- ⓘ **A unique credential must be used for each credential type (for example, a single credential may not be used for both normal use and toggle functions).**

PROGRAMMING credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!			
	1	2	3	4
Create new Programming Code (PIN)	Enter ⑨⑦⑤③①⊛ (This is the default programming PIN)	Enter ⑦⊛	Enter new 5 digit Programming code and ⊛ Wait for right green light.	Reenter the new 5 digit Programming code and ⊛ Wait for confirmation: 2 right green blinks.
Create new Programming Card	Enter ⑨⑦⑤③①⊛	Enter ⑦⊛	Present new programming card.	Wait for confirmation: 2 right green blinks.

ⓘ **Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).**

NORMAL USE credentials

Note: Until a new Normal Use PIN is created, the default PIN is ①③⑤⑦⑨#

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Normal Use PIN	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③⊛	Enter new 3-6 digit PIN and ⊛⊛	For another PIN, go back to step 3	Press ⊛ again to finish	Wait for confirmation: 2 right green blinks.
Create a Normal Use CARD	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③⊛	Enter new 3-6 digit Card ID Number and ⊛	Wait for right green light. Present new CARD to lock.	For another CARD, go back to step 3 OR press ⊛ again	Wait for confirmation: 2 right green blinks.
Create a Normal Use CARD + Card ID Number	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③③⊛	Enter ③①①⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.

ⓘ **Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).**

TOGGLE credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Toggle PIN	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ① ⑨ ① ⊛	Enter new 3-6 digit PIN and ⊛ ⊛ Wait for right green light.	For another PIN, go back to step 3 OR press ⊛ again to finish	Wait for confirmation: 2 right green blinks.
Create a Toggle CARD	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ① ⑨ ① ⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD, go back to step 3 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.
Create a Toggle CARD + Card ID Number	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ③ ⑨ ① ⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.

ⓘ **Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).**

FREEZE credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Freeze PIN	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ① ① ⑤ ⊛	Enter new 3-6 digit PIN and ⊛ ⊛ Wait for right green light.	For another PIN, go back to step 3 OR press ⊛ again to finish	Wait for confirmation: 2 right green blinks.
Create a Freeze CARD	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ① ① ⑤ ⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD, go back to step 3 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.
Create a Freeze CARD + Card ID Number	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ③ ① ⑤ ⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.

ⓘ **Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).**

PASS THROUGH credentials

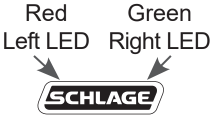
To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	**2**	**3**	**4**	**5**	**6**
Create a Pass Through PIN	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ① ① ⑨ ⊛	Enter new 3-6 digit PIN and ⊛ ⊛ Wait for right green light.	For another PIN, go back to step 3 OR press ⊛ again to finish	Wait for confirmation: 2 right green blinks.
Create a Pass Through CARD	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ① ① ⑨ ⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD, go back to step 3 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.
Create a Pass Through CARD + Card ID Number	Enter Programming PIN and ⊛ OR Present Programming card	Enter ③ ③ ⊛	Enter ③ ① ⑨ ⊛	Enter new 3-6 digit Card ID Number and ⊛ Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press ⊛ again to finish Wait for confirmation: 2 right green blinks.

OTHER programming

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!				
	1	2	3	4	5
Delete a credential	Enter Programming PIN and ⊛ OR Present Programming card	Enter ⑤ ⊛	Enter the PIN or Card ID Number to be deleted and ⊛	To delete another Card credential, go back to step 3 OR press ⊛ again to finish	Wait for confirmation: 2 right green blinks.
Change PIN or Card ID Number length	Enter Programming PIN and ⊛ OR Present Programming card	Enter ⑨ ⑨ ⊛	Enter ④ ⊛	Enter ③, ④, ⑤, OR ⑥ for desired PIN length	Press ⊛ again to finish Wait for confirmation: 2 right green blinks.
Change relock delay period	Enter Programming PIN and ⊛ OR Present Programming card	Enter ⑨ ⑨ ⊛	Enter ① ⊛	Each button press adds to the total delay time Example: ① + ⑨ adds a 10 second delay	Press ⊛ again to finish Wait for confirmation: 2 right green blinks.

Error codes

ⓘ **All error codes are indicated on the Schlage button by a solid red left LED, and a blinking green right LED. The number of green blinks indicates the error code.**



Number of green blinks	Error code description
1	Computer programming error (not complete).
2	Too long programming/user code entered. Programming code must be five (5) digits. User code length cannot exceed six (6) digits.
3	Memory full, too many codes. Delete some codes.
4	Programming code cannot be deleted, only changed.
5	Programming code entries do not match. Programming code not changed.
6	Invalid command. Invalid function code entered.
7	Code not found.
8	Code too short. Programming code length must be five (5) digits. User code minimum length is three (3) digits.
9	Not a unique code.
10	Manual programming not allowed.

Test lock operation

If you encounter problems while performing any of the following tests, review the installation guide and correct any problems.

Mechanical test

1. Rotate the inside lever. Operation should be smooth, and the latch should retract.
2. Insert the key into the keyway and rotate the key or the key and lever to open the door. Operation should be smooth, and the latch should retract.

Electronic test

Test the AD-200/AD-201 in factory default mode

1. For locks with a keypad, press any number key. The lock will beep.
2. Press the Schlage button. The keypad should light blue for a few seconds.
3. For locks with a card reader, present a credential to the reader. The lock will beep and the left side of the Schlage button will blink red one time. When the lock is in factory default mode, no credentials are accepted.
4. In the factory default state, locks with keypads, with or without additional credentials, have a default PIN of **13579** and “**#**”. To test, enter the default PIN. The Schlage button will blink and the lock will unlock.

Test the AD-200/AD-201 in construction access mode

1. When the master construction credential is presented, the lock will beep and the Schlage button will light green for 20 seconds awaiting the presentation of another credential to be granted Construction User Access.
2. When a valid construction access user credential is presented, the lock will unlock for the re-latch delay period (default three seconds), and the left side of the Schlage button will blink green. When the lock relocks after the relock delay period, the left side of the Schlage button will blink red.
3. If an invalid construction access user credential is presented, the lock will beep and the left side of the Schlage button will blink red one time. For more information, see *Construction access mode* on page 5.

ⓘ ***NOTE: Construction access mode is cancelled when the lock is reset to factory defaults. When construction access mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.***

Normal lock operation

After credentials have been programmed, present credentials to operate the lock as follows:

Credential type	Action						
PIN or Card	Present or enter credential to reader			➔	Green blink	➔	Access granted
Card+Card ID Number	Present credential to reader	➔	Press Card ID Number[1]	➔	Green blink	➔	Access granted

[1] The default PIN/Card ID length is six digits. The “#” key must be used as an ENTER key for PINs/Card IDs with fewer than six digits. PIN/Card ID length can be manually configured (refer to *Change PIN or Card ID Number length* on page 12).

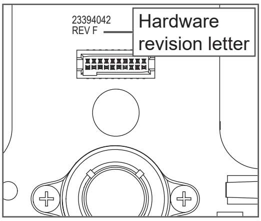
Wired remote release feature

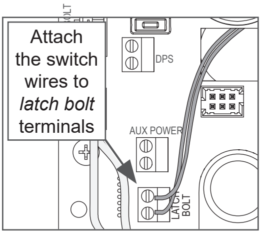
System and hardware requirements

- Available on AD200 storeroom function only
- Compatible with AD200 hardware revision F or higher. See illustration below to locate revision letter on main printed circuit board.
- The AD200 must be programmed with AD-200 version 2.45.1 firmware or higher.

Switch specifications, wire specifications and routing

- Recommended switch: basic SPST (single-pole single-throw) momentary action switch with normally open contact configuration.
- Wire gauge AWG 24, stranded, twisted pair, shielded (shield may be left unterminated).
- Belden 9841 or equivalent.
- Maximum cable length is 1000 feet (305 meters).
- Route wires from the switch, through the door frame and door to the latch bolt terminals as shown below.





Wired remote release operation

IMPORTANT! The remote release feature will function only when the AD-200 inside cover is completely and properly installed.

Operation with firmware version 2.45.1

- When the remote release button is pressed the lock will unlock for the programmed relock delay period. The Schlage LEDs will flash green once to indicate the lock is unlocked. The beeper will not sound.
- After the relock delay period has expired, the Schlage LEDs will flash red once to indicate the lock is relocked.

Operation with firmware version 2.46.1

- When the remote release button is pressed the lock will unlock for the programmed relock delay period. The green Schlage LEDs and the green inside push button LED will turn on to indicate the lock is unlocked. If the beeper function is turned on, the beeper will sound one time to indicate the lock is unlocked.
- After the relock delay period has expired, the green Schlage LEDs and the green inside push button LED will turn off. If the beeper function is turned on, the beeper will sound two times to indicate the lock is relocked.

Wired remote release button action

- If the remote release button is pressed and held, the release will function only one time, even in the event the button is held longer than the relock delay period.
- If the remote release button is quickly pressed repeatedly, the release will function only one time. Any additional button presses during the relock delay period are ignored.
- Once the lock relocks, the next press of the remote release button will activate a new release cycle.

Reset to factory defaults

All information in the lock will be deleted and reset to factory defaults!

Level 1 factory default reset

ⓘ **Level 1 factory default reset will delete configurations and settings in the main controller in the lock.**

ⓘ **Main controller configurations that will reset to factory default include: programming and user codes.**

ⓘ **Level 1 factory default reset *will not* reset configurations and settings in the reader.**

1. Remove the top inside cover.
2. Press and hold the Schlage button until two (2) beeps sound (10 seconds).
3. Release the Schlage button.
4. Press and release the inside push button (IPB) three (3) times within 10 seconds. One beep will sound and one red blink will occur with each press.
5. The Schlage button and IPB will both light green for one second and a one-second beep will be heard. This indicates that the lock has been reset.

ⓘ **If the IPB is not pressed 3 times within 10 seconds, two beeps with two red blinks indicate timeout.**

6. Replace the top inside cover.

Level 2 factory default reset

ⓘ **Level 2 factory default reset will delete all configurations and settings in the lock and the reader.**

ⓘ **Reader configurations that will reset to factory default include: keypad format, magstripe reader track, beeper on/off, and contactless card.**

ⓘ **Days in Use counter and lock type configurations will not reset.**

To complete Level 2 factory default reset, repeat steps 2 through 5 above **within 10 seconds of the confirmation signals of Level 1 factory default reset.** If more than 10 seconds pass after the confirmation signals of Level 1 reset, then Level 1 reset will be repeated.

Batteries

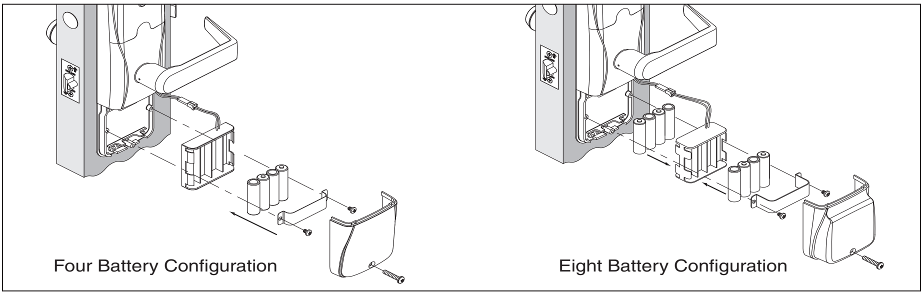
To install or replace batteries

ⓘ **Replacement of batteries does not affect any programmed data.**

ⓘ **Battery voltage can be checked with the SUS.**

1. Remove the battery cover.
2. Remove the battery bracket. **Do not allow the battery pack to hang from the wires.**
3. Install the new batteries (install only new AA Alkaline batteries).
4. Reinstall the battery pack and battery bracket.
5. Reinstall the battery cover. **Be careful not to pinch the battery wires when installing the battery cover.**

CAUTION! Danger of explosion if battery is incorrectly replaced! Replace only with the same or equivalent type. Dispose of used batteries according to the manufacturer's instructions.



Four Battery Configuration

Eight Battery Configuration

This product has been evaluated for ULC-S319 compliance with AA and coin cell batteries listed below. For installations requiring ULC-S319, these battery models should be used.

AA batteries: Duracell PC1500, MN1500; Energizer E91, EN91, AX91, XR91; RayoVac 815, 815-HE

Coin cell batteries: Energizer CR2025, CR2032; Maxell CR2025, CR2032, Panasonic CR2025, CR2032; RayoVac KECR2025, KECR2032.

Low battery indications

ⓘ **During low battery condition, the reader’s beeper will be temporarily disabled. This condition will revert to normal function when batteries (AA or coin cell) are replaced. (While the beeper is in temporary disabled state, the SUS will indicate beeper is “on” as previously set by the user.)**

Condition	Indicator	Solution
Batteries low	After credential is presented, 9 red blinks of Schlage button. (Left = AA, Right = Coin Cell), then normal indicator.	Replace batteries immediately to avoid battery failure. Lock is intended to operate for 500 cycles in low battery condition.
Battery failure (configured by SUS)	No LED or beeps Valid credentials do not grant access	Replace batteries immediately. Mechanical override key must be used to unlock the lock.

Battery failure modes

ⓘ **The battery failure mode is set using the SUS. See the SUS User Guide for more information.**

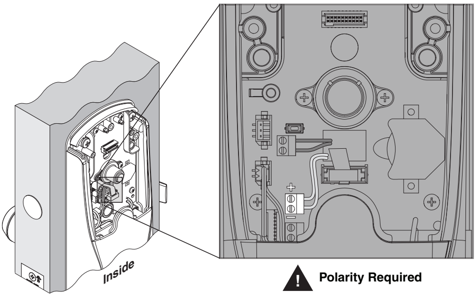
Mode	Description
Fail As-Is (default)	Lock remains in current state until batteries are replaced.
Fail Unlocked[1]	Lock unlocks and remains unlocked until batteries are replaced.
Fail Locked[1]	Lock locks and remains locked until batteries are replaced.

[1] Fail Unlocked and Fail Locked modes are not available if the lock is externally powered.

External power supply

The AD-200/AD-201 may be connected to external power using a UL294 listed Power Supply for UL installations, and a power supply that complies with CAN/UL-S318 or CAN/ULC-S319 for cUL installations. The power supply must be capable of sourcing at least 250 mA @ 12 or 24 VDC (Schlage PS902, PS904, PS906).

ⓘ **When powered with external power supply, the lock will always fail “As-Is” if power is lost.**



LED Reference

Most LED and beep indicators are configured using the SUS. See the SUS user guide for more information.

Schlage button

Condition	Lights
Access denied	2 red blinks
Access denied, user outside time zone	4 red blinks
Valid PIN entered while lock in freeze mode	12 red blinks indicating lockout
Factory default reset	Solid red while clearing memory, then a one-second solid green when complete.
Waiting for Card ID Number (Card + Card ID Number)	5 left red with right green blinks, then solid right green
Low battery indicator, AA batteries	9 left red blinks
Low battery indicator, coin cell battery	9 right red blinks
Momentary unsecured access	1 green blink, then one red blink on relock
Toggle unsecured	2 green blinks
Toggle secure (relocking)	1 red blink
SUS authentication	Left green solid
USB active with no physical connection	Left green blinking

Optional Inside Push Button (IPB)

Action	Lights
Classroom, Office or Apartment Mode	
Press IPB to lock	1 red blink
Press IPB to unlock	1 green blink
Privacy Mode	
With door closed, press IPB to engage privacy	4 green blinks
With door closed, press IPB to release privacy[1]	4 red blinks

[1] If DPS is used, then opening the door will also release privacy. If mortise deadbolt is used, then retracting the deadbolt will also release privacy.

Troubleshooting

Problem	Possible cause	Solution
The lock beeper does not sound and the keypad does not light when the Schlage button is pressed.	The reader may not be properly seated into the front escutcheon. The reader connector may have bent pins. The through door ribbon cable may not be properly plugged in. The battery or wired power may be improperly connected. The batteries may be inserted with incorrect polarity.	Check that the reader is fully seated into the front escutcheon. Check that there are no bent pins in the reader connector. Check that the through door ribbon cable is plugged in correctly. The red wire should be on the left and not pinched in the door. Check that the battery or wired power is connected correctly. Check that the batteries are inserted in the correct polarity. *Refer to the installation instructions that came with the AD-200/AD-201 lock, or this user guide for details on the above mentioned procedures.*
The reader is not working. The Smart card is not reading. The magnetic swipe card is not reading correctly (no beeps or blinks).	The through hole ribbon cable may be pinched. The Smart card default of the card reader may not be correct for the Smart card. The “Mag Track in Use” default for all Magnetic Card Credential Readers is “Track2”. The magnetic swipe card data may be on Track1 or Track3.	Check that the through hole ribbon cable is not pinched. Change the Smart card format using the SUS. Select AD-200/AD-201 “Lock Properties”, “Reader” tab, and “Smart cards in use”. Use the SUS to change “Mag Track in Use”. Select AD-200/AD-201 “Lock Properties”, “Reader” tab, and “MAG Card Track selection”. *Refer to the installation instructions that came with the AD-200/AD-201 lock, or the SUS user guide for details on the above mentioned procedures.*
Wired remote release feature is not working.	The lock may not be compatible with remote release. The hardware or firmware version may not be compatible with remote release. The lock’s inside cover may not be properly or completely installed. The remote release switch may not be functioning correctly.	Wired remote release is available only on the AD-200 storeroom function. Wired remote release is compatible with hardware version F or higher, and with locks programmed with AD-200 version 2.45.1 firmware or higher. Check that the inside cover is completely and properly installed. Check that the switch closes and delivers less than 5 ohms resistance when activated.

FCC/IC Statements

Allegion Agency statements

Compliance Statement

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC interference statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Industry Canada statements

This equipment has been tested and found to comply to Industry Canada ICES-003.

CAN ICES-3(B)/NMB-3(B)

Customer Service

1-877-671-7011 www.allegion.com/us

ALLEGION™

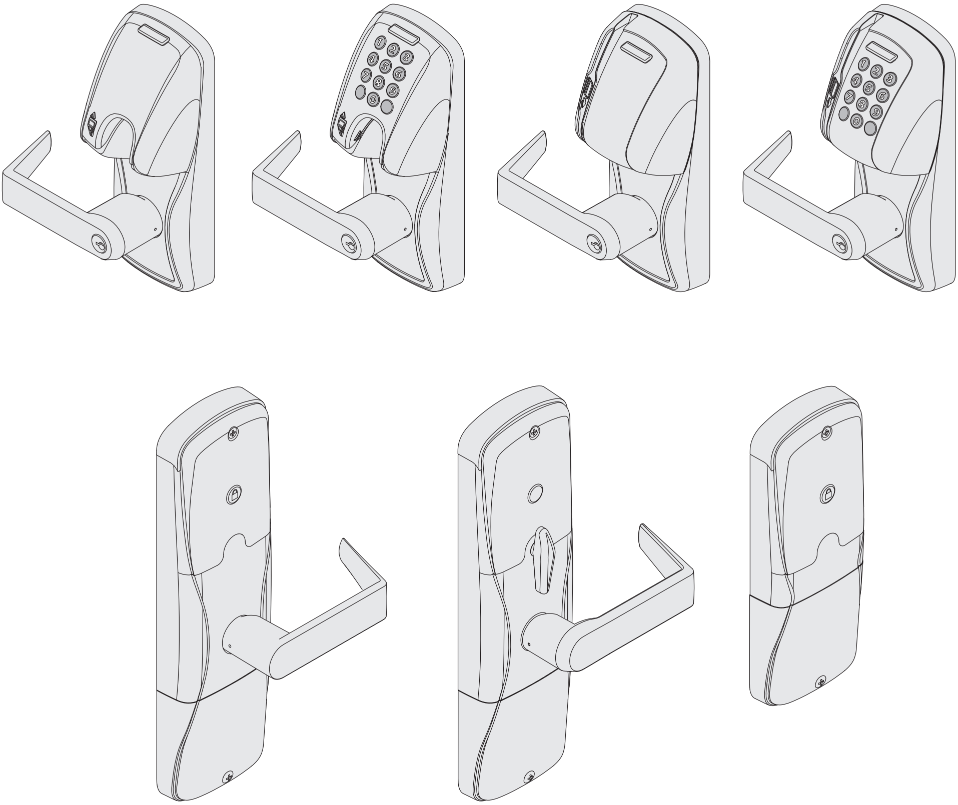
P516-130

SCHLAGE

AD-250

Offline lock user guide

Instructions for programming AD-Series offline locks



Para el idioma español, navegue hacia www.allegion.com/us.
Pour la portion française, veuillez consulter le site www.allegion.com/us.

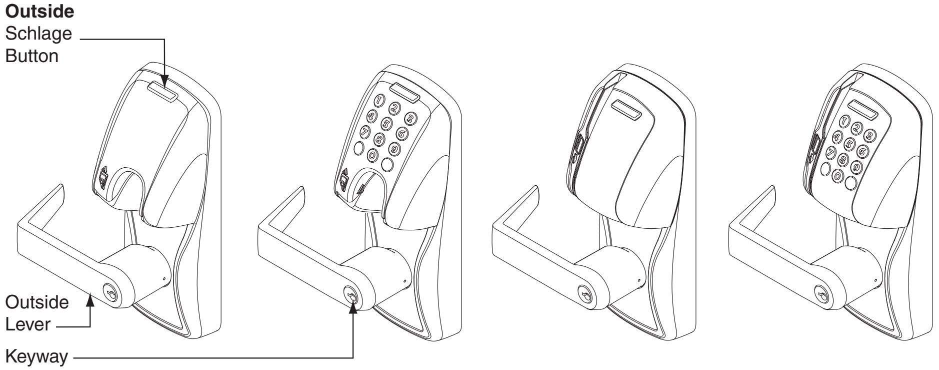
Contents

This product is compliant of UL 294 and ULC S319 standard. This product's compliance would be invalidated through the use of any add-on, expansion, memory or other module that has not yet been evaluated for compatibility for use with this UL Listed product, in accordance with the requirements of the Standards UL 294 and ULC S319. This product has been evaluated for CAN/ULC-S319 Class 1.

Overview

The Schlage AD-250 is a standalone electronic lock in the AD-Series product line.

- May be powered by batteries or connected to external power using a UL 294 or ULC S318/ULC S319 listed power supply capable of sourcing at least 250 mA @ 12 or 24 VDC. See *Batteries* on page 8, or *External power supply* on page 9 for more information.
- Outside lever is normally locked.
- Inside lever always allows egress.
- The lock maintains an audit trail of events.
- Configured using the Schlage Utility Software (SUS). See *Schlage Utility Software (SUS)* on page 4 for more information.

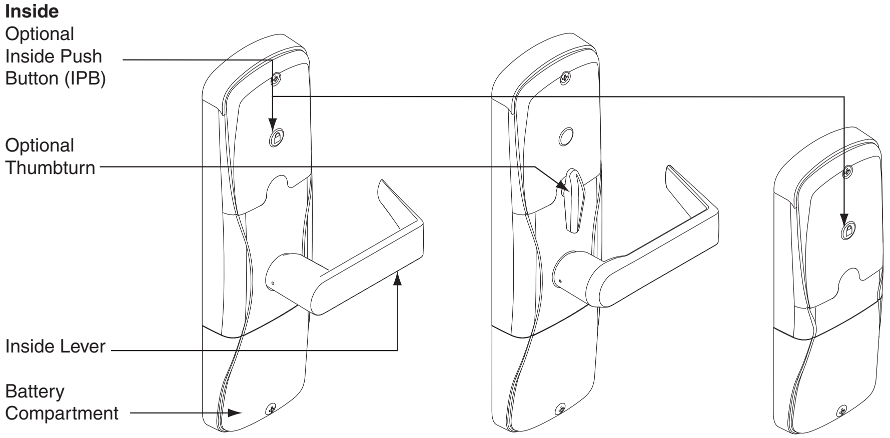


Mag Card (Insert) Reader

Mag Card + Keypad (Insert) Reader

Mag Card (Swipe) Reader

Mag Card + Keypad (Swipe) Reader



Lock functions

The AD-250 is available in one of four functions:

Privacy (40): Lockset is normally secure. Pressing the Inside Push Button or extending the deadbolt will disable normal electronic access from the outside. Opening the door, retracting the deadbolt or pressing the Inside Push Button a second time deactivates the privacy status.

Office (50): Lockset is normally secure. Inside Push Button may be used to select passage or secured status.

Apartment (60): Lockset is normally secure. Inside Push Button is used to select passage or secure status. While in the secure state, opening the door or pressing the Inside Push Button causes the lockset to toggle unsecured. The door must be closed and a valid credential presented to secure the lockset from the outside.

Classroom/Storeroom (70): Lockset is normally secure. Valid toggle credentials may be used to change to a passage or secure status.

Getting started

Follow these steps when setting up a new lock.

1. Install the lock. See the installation guide that came with the lock, or visit www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library) for more information.
2. Make sure the batteries are installed properly. See *Batteries* on page 8 for more information.
3. Configure the master construction credential (where applicable). See *Construction access mode* on page 5 for more information. The lock will remain in construction access mode until you are ready to set up the rest of the system.
4. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 6 for more information.
5. Consult the Schlage Utility Software (SUS) user guide for information about configuring the lock.
6. Familiarize yourself with the information contained in this user guide.

Save this user guide for future reference.

Schlage Utility Software (SUS)

The Schlage Utility Software is used for programming and setup only.

The Schlage Utility Software (SUS) is used to configure locks. This includes transferring data files between the access control software and locks. For further information about SUS, see the SUS user guide.

Construction access mode

Construction access mode is used to allow access before the lock has been programmed, and for testing purposes.

- Enabled by default.
- The lock will remain in construction access mode until the mode is cancelled as described below.
- No audits are captured while lock is in construction access mode.
- Use the same master construction credential for all the locks in the facility.
- If you present the first card to a new lock to create the master construction credential and the card is not accepted, the lock has either been programmed or already has a master construction credential.
- If the master construction credential cannot be located, or to put the lock back into construction access mode, reset the lock to factory settings (see page 7 for details).

Locks with keypads – Construction access mode

In the factory default state, locks with keypads have a default PIN of 13579 and "#", which can be used for installation, testing and construction access. To test, enter default PIN. The Schlage button will blink and the lock will unlock.

The default PIN, 13579 and "#" is automatically deleted when a construction access user credential is added to the lock, or a new programming credential is created, or the lock is programmed with the SUS.

Locks with card readers – Create a master construction credential

The master construction credential is used to program construction access mode credentials.

To create a master construction credential:

1. Press and hold the Schlage button while presenting a credential.
2. The Schlage button will blink green on the left and right as confirmation.
3. Use this card to add construction access mode user credentials.

ⓘ **The master construction credential will not grant access. It is used only to add additional credentials.**

Locks with card readers – Add construction access mode user credentials

Construction access mode credential type	Steps to add construction access mode user credentials				
	1	2	3	4	5
Normal use construction credential Unlocks the lock for relock delay period	Present master construction credential to reader ➔	Green LEDs blink ➔	Present user credential within 20 seconds ➔	Green LEDs blink and credential is added ➔	Repeat steps 3 and 4 for additional credentials. Credentials added with the master construction credential will have 24/7 access.
Toggle construction credential Changes the state of the lock from locked to unlocked or vice versa	Present master construction credential to reader ➔	Green LEDs blink ➔	Press and hold Schlage button while presenting user credential within 20 seconds ➔	Green LEDs blink, 2 beeps will sound and credential is added ➔	

Cancel construction access mode

Do one of the following:

- Program the lock with the SUS. See the SUS user guide for more information.
- Reset the lock to factory settings. See *Reset to factory defaults* on page 7 for more information.

When construction mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.

Test lock operation

If you encounter problems while performing any of the following tests, review the installation guide and correct any problems.

Mechanical test

1. Rotate the inside lever. Operation should be smooth, and the latch should retract.
2. Insert the key into the keyway and rotate the key or the key and lever to open the door. Operation should be smooth, and the latch should retract.

Electronic test

Test the AD-250 in factory default mode

1. For locks with a keypad, press any number key. The lock will beep.
2. Press the Schlage button. The keypad should light blue for a few seconds.
3. Present a credential to the reader. The lock will beep and the Schlage button will blink red one time. When the lock is in factory default mode, no credentials are accepted.

ⓘ **If the lock does not acknowledge the credential presentation, be sure that there is data on Track 2 of the credential. Default settings require data on Track 2.**

4. In the factory default state, locks with keypads, with or without additional credentials, have a default PIN of **13579** and “**#**”. To test, enter default PIN. The Schlage button will blink and the lock will unlock.

Test the AD-250 in construction access mode

1. When the master construction credential is presented, the lock will beep and the Schlage button will light green for 20 seconds awaiting the presentation of another credential to be granted construction user access.
2. When a valid construction access user credential is presented, the lock will unlock for the re-latch delay period (default three seconds), and the Schlage button will blink green. When the lock re-locks after the re-latch delay period, the Schlage button will blink red.
3. If an invalid construction access user credential is presented, the lock will beep and the Schlage button will blink red twice. See *Construction access mode* on page 5 for more information.

ⓘ ***NOTE: Construction access mode is cancelled when the lock is reset to factory defaults. When construction access mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.***

Reset to factory defaults

All information in the lock will be deleted and reset to factory defaults!

Level 1 factory default reset

ⓘ **Level 1 factory default reset will delete configurations and settings in the main controller in the lock.**

ⓘ **Main controller configurations that will reset to factory default include: programming and user codes.**

ⓘ **Level 1 factory default reset *will not* reset configurations and settings in the reader.**

1. Remove the top inside cover.
2. Press and hold the Schlage button until two (2) beeps sound (10 seconds).
3. Release the Schlage button.
4. Press and release the inside push button (IPB) three (3) times within 10 seconds. One beep will sound and one red blink will occur with each press.
5. The Schlage button and IPB will both light green for one second and a one-second beep will be heard. This indicates that the lock has been reset.

ⓘ **If the IPB is not pressed 3 times within 10 seconds, two beeps with two red blinks indicate timeout.**

6. Replace the top inside cover.

Level 2 factory default reset

ⓘ **Level 2 factory default reset will delete all configurations and settings in the lock *and the reader*.**

ⓘ **Reader configurations that will reset to factory default include: keypad format, magstripe reader track, beeper on/off, and contactless card.**

ⓘ **Days in Use counter and lock type configurations will not reset.**

To complete Level 2 factory default reset, repeat steps 2 through 5 above **within 10 seconds of the confirmation signals of Level 1 factory default reset.** If more than 10 seconds pass after the confirmation signals of Level 1 reset, then Level 1 reset will be repeated.

Batteries

To install or replace batteries

ⓘ **Replacement of batteries does not affect any programmed data.**

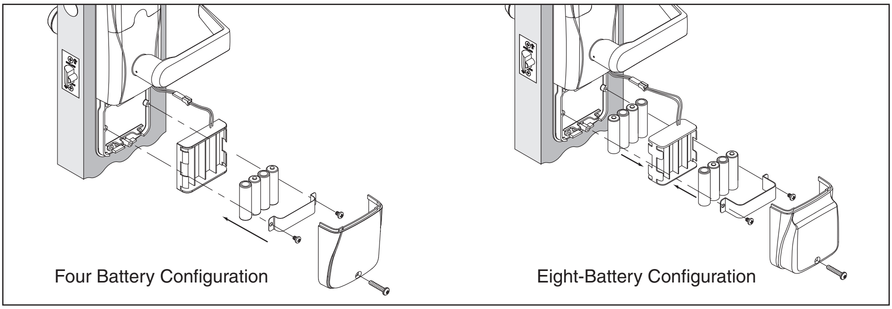
ⓘ **Battery voltage can be checked with the SUS.**

1. Remove the battery cover.
2. Remove the battery bracket.

Do not allow the battery pack to hang from the wires.

3. Install the new batteries (install only new AA Alkaline batteries).
4. Reinstall the battery pack and battery bracket.
5. Reinstall the battery cover. **Be careful not to pinch the battery wires when installing the battery cover.**

CAUTION! Danger of explosion if battery is incorrectly replaced! Replace only with the same or equivalent type. Dispose of used batteries according to the manufacturer's instructions.



Four Battery Configuration

Eight-Battery Configuration

This product has been evaluated for ULC-S319 compliance with AA and coin cell batteries listed below. For installations requiring ULC-S319, these battery models should be used.

AA batteries: Duracell PC1500, MN1500; Energizer E91, EN91, AX91, XR91;
RayoVac 815, 815-HE

Coin cell batteries: Energizer CR2025, CR2032; Maxell CR2025, CR2032,
Panasonic CR2025, CR2032; RayoVac KECR2025, KECR2032.

Low battery indications

ⓘ **During low battery condition, the reader's beeper will be temporarily disabled. This condition will revert to normal function when batteries (AA or coin cell) are replaced. (While the beeper is in temporary disabled state, the SUS will indicate beeper is "on" as previously set by the user.)**

Condition	Indicator	Solution
Batteries low	After credential is presented, 9 red blinks of Schlage button (Left = AA, Right = Coin Cell), then normal indicator.	Replace batteries immediately to avoid battery failure. Lock is intended to operate for 500 cycles in low battery condition.
Battery failure (configured by SUS)	No LED or beeps Valid credentials do not grant access	Replace batteries immediately. Mechanical override key must be used to unlock the lock.

Battery failure modes

ⓘ **The battery failure mode is set using the SUS. See the SUS user guide for more information.**

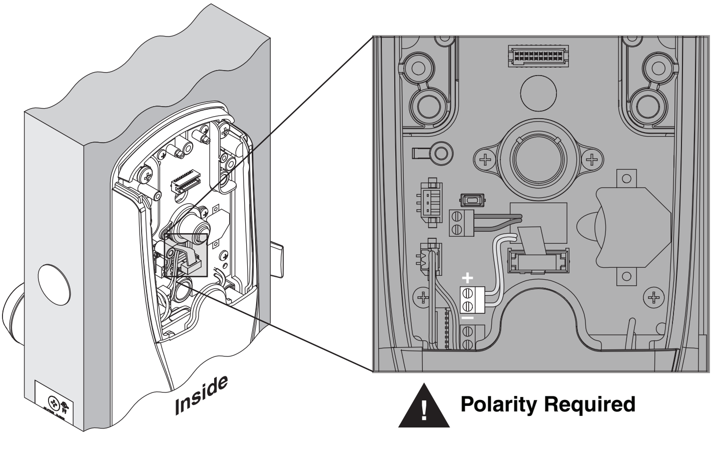
Mode	Description
Fail As-Is (default)	Lock remains in current state until batteries are replaced.
Fail Unlocked[1]	Lock unlocks and remains unlocked until batteries are replaced.
Fail Locked[1]	Lock locks and remains locked until batteries are replaced.

[1] Fail Unlocked and Fail Locked modes are not available if lock is externally powered.

External power supply

The AD-250 may be connected to external power using a UL294 listed Power Supply for UL installations, and a power supply that complies with CAN/UL-S318 or CAN/ULC-S319 for cUL installations. The power supply must be capable of sourcing at least 250 mA @ 12 or 24 VDC (Schlage PS902, PS904, PS906).

ⓘ **When powered with external power supply, the lock will always fail "As-Is" if power is lost.**



Polarity Required

LED reference

Most LED and beep indicators are configured using the SUS. See the SUS User Guide for more information.

Schlage button

Condition	Lights
Access denied	2 red blinks
Access denied, user outside time zone	4 red blinks
Factory default reset	Solid red while clearing memory, then one-second solid green when complete.
Low battery indicator, AA batteries	9 left red blinks
Low battery indicator, coin cell	9 right red blinks
Momentary unsecured access	1 green blink, then one red blink on relock
Toggle unsecured	2 green blinks
Toggle secure (relocking)	1 red blink
SUS authentication	Left green solid
USB active with no physical connection	Left green blinking
Waiting for PIN (Card + PIN)	5 left red with right green blinks then solid right green.

Inside Push Button (IPB)

Condition	Lights
Press IPB to lock (privacy mode disabled)	1 red blink
Press IPB to unlock (privacy mode disabled)	1 green blink
Door closed, IPB pressed to engage Privacy (privacy mode enabled)	4 red blinks
Door closed, IPB pressed to disengage Privacy (privacy mode enabled)	4 green blinks
Door locked (privacy mode enabled or disabled)	One red blink every 15 seconds for first 10 minutes, then one red blink every 30 seconds for the next 50 minutes, then one red blink every 60 seconds after one hour.

Troubleshooting

Problem	Possible cause	Solution
The lock beeper does not sound and the keypad does not light when the Schlage button is pressed.	The reader may not be properly seated into the front escutcheon. The reader connector may have bent pins. The through door ribbon cable may not be properly plugged in. The battery or wired power may be improperly connected. The batteries may be inserted with incorrect polarity.	Check that the reader is fully seated into the front escutcheon. Check that there are no bent pins in the reader connector. Check that the through door ribbon cable is plugged in correctly. The red wire should be on the left and not pinched in the door. Check that the battery or wired power is connected correctly. Check that the batteries are inserted in the correct polarity. *Refer to the installation instructions that came with the AD-250 lock, or this user guide for details on the above mentioned procedures.*
The reader is not working. The magnetic swipe card is not reading correctly (no beeps or blinks).	The through hole ribbon cable may be pinched. The “Mag Track in Use” default for all magnetic card credential readers is “Track2”. The magnetic swipe card data may be on Track1 or Track3.	Check that the through hole ribbon cable is not pinched. Use the SUS to change “Mag Track in Use”. Select AD-250 “Lock Properties”, “Reader” tab, and “MAG Card Track Selection”. *Refer to the installation instructions that came with the AD-250 lock, or the SUS user guide for details on the above mentioned procedures.*

FCC/IC statements

Allegion Agency statements

Compliance Statement

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC interference statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Industry Canada statements

This equipment has been tested and found to comply to Industry Canada ICES-003.

CAN ICES-3(B)/NMB-3(B)

Customer Service

1-877-671-7011 www.allegion.com/us

ALLEGION™

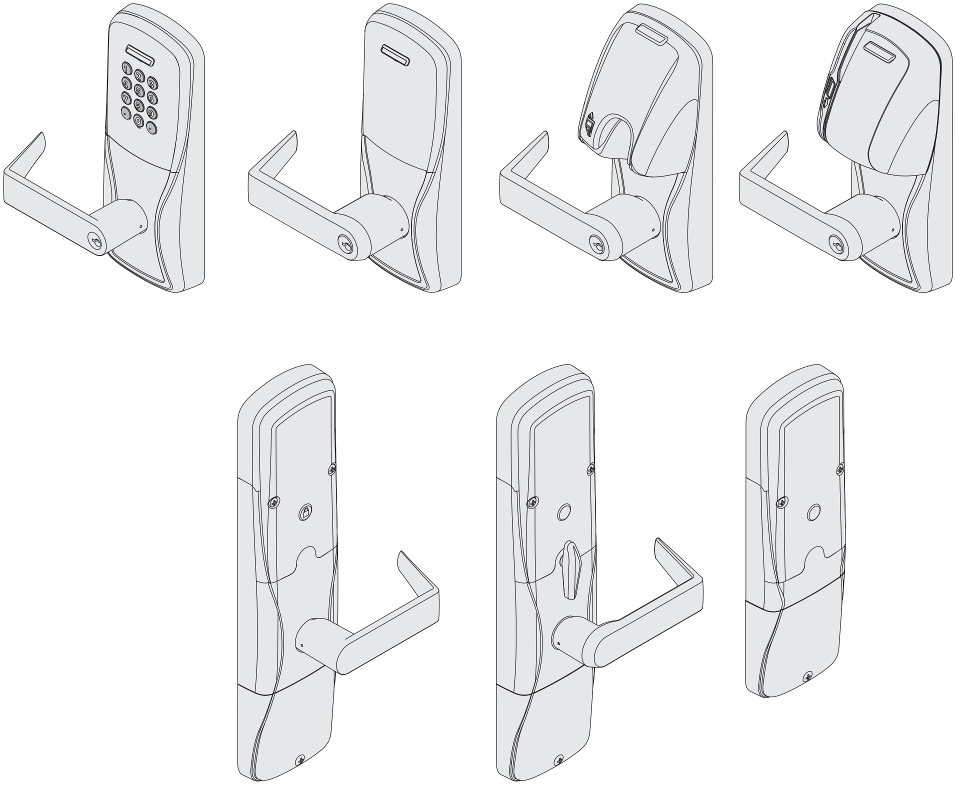
P516-127

SCHLAGE

AD-400
AD-401

Networked wireless lock user guide

Instructions for adaptable series networked wireless locks



Para el idioma español, navegue hacia www.allegion.com/us
Pour la portion française, veuillez consulter le site www.allegion.com/us

Contents

To comply with FCC and Industry Canada RF radiation exposure limits for general population, the antenna(s) used for this transmitter must be installed such that a minimum separation distance of 20 cm is maintained between the radiator (antenna) and all persons at all times and must not be co-located or operating in conjunction with any other antenna or transmitter.

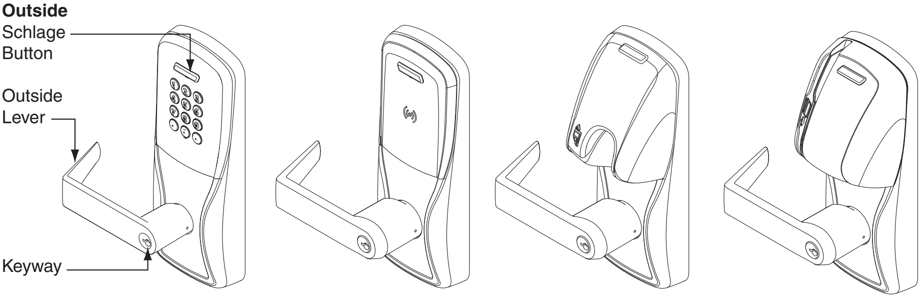
This product is compliant of UL294 and ULCS319 standard. This product's compliance would be invalidated through the use of any add-on, expansion, memory or other module that has not yet been evaluated for compatibility for use with this UL Listed product, in accordance with the requirements of the Standards UL294 and ULCS319. This product has been evaluated for ULC-S319 Class I.

Overview

The Schlage AD-400 is an open architecture Wireless Access Point Module (WAPM) designed to interface with third-party panels through a PIM400.

The Schlage AD-401 is a FIPS-201-1 certified Wireless Access Point Module (WAPM).

- The AD-400/AD-401 communicates with the PIM400 via RF (radio frequency).
- The AD-400/AD-401 may be battery powered or connected to external power using a UL294 or ULCS318/ULCS319 listed power supply. See *Batteries* on page 12 or *External power supply on page 13* for more information.
- The outside lever is normally locked.
- The inside lever always allows egress.
- The AD-400/AD-401 normally operates in on-line mode. Information contained in the user credential is passed to an access control panel (ACP), which controls lock functions. The ACP maintains the audit trail.

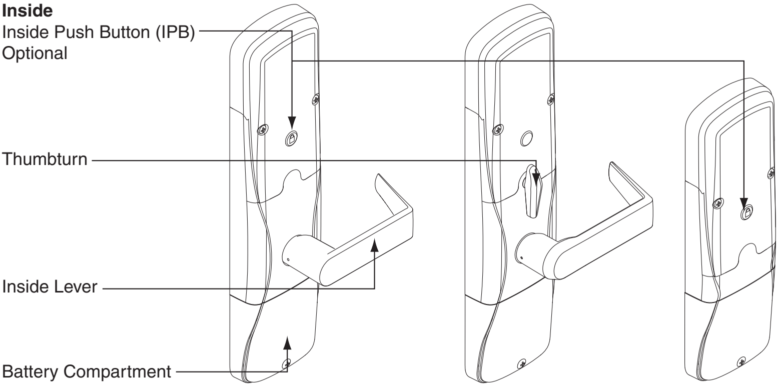


Keypad

Multi-Tech Reader

Mag Card (Insert) Reader

Mag Card (Swipe) Reader



AD-400/AD-401-CY
AD-400/AD-401-MS

AD-400/AD-401-MD

AD-400/AD-401-993

Additional AD-400 Reader options: Mag + Keypad, Multi-Tech + Keypad.

Note: Proximity card (PR, PRK) ONLY and Smart card (SM, SMK) ONLY reader have been discontinued and replaced by the Multi-Tech (MT, MTK) readers that provide all the same funcionality as the original Proximity and Smart card readers in a single credential reader.

The AD-401 reader is a FIPS-201-1 certified Multi-Tech + Keypad (FMK) reader.

Getting started

Follow these steps when setting up a new lock.

1. Install the lock. See the installation guide that came with the lock or visit www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library) for more information.
2. Make sure the batteries are installed properly. See *Batteries* on page 12 for more information.
3. Configure the Master Construction Credential (where applicable). See *Construction access mode* on page 6 for more information. The lock should remain in Construction Access Mode until you are ready to set up the rest of the wireless access system with connection to the PIM400 and the access control panel (ACP).
4. Link the lock to the PIM400. See *Link to a PIM400* on page 8 for more information.
5. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 9 for more information.
6. Consult the SUS User Guide for information about configuring the lock and PIM400.
7. Familiarize yourself with the information contained in this user guide.

Save this user guide for future reference.

Schlage Utility Software (SUS)

The SUS is used to configure locks and the PIM400.

ⓘ **When in a low battery condition the lock may operate but not have sufficient power to communicate with the SUS. When intitiating SUS communication, the Schlage button will light solid red for one second to indicate power is not sufficient. If this should occur, change the batteries immediately. See** *Batteries* **on page 12.**

The SUS is used for programming lock characteristics and setup only. Access rights for the AD-400/AD-401 are set by the access control panel, not by the SUS.

For more information about the SUS, see AD-Series Locks in the SUS User Guide.

Optional inside push button (IPB)

- The inside push button (IPB) state is communicated to the access control panel by the PIM400-485. The manner in which the network access control software utilizes this communication is configured at the host. The IPB may be used to communicate a lock/ unlock request or be completely ignored by the network software.
- AD-400 IPB activity will only be reported to control systems connected to a PIM400-485 with a RS-485 connection.
- The IPB may be configured by the ACP or SUS to take direct action on the lock state in case communication from the control system to the AD-400 fails and the lock remains powered.

User management

User management is controlled by the access control system. If the access control panel has not yet been connected, use Construction Access Mode to add and delete users.

ⓘ See *Construction access mode* on page 6 for more information.

For compliance with the UL Standards UL 294 and ULC S319, the AD-400/AD-401 must be connected to an access control panel (ACP) that is UL listed for UL 294 for UL installations and ULC S319 for cUL installations.

Construction access mode

Construction access mode is used to allow access before the lock has been programmed, and for testing purposes.

- Enabled by default.
- The lock will remain in construction access mode until the mode is cancelled as described below.
- No audits are captured while lock is in construction access mode.
- Use the same master construction credential for all the locks in the facility.
- If you present the first card to a new lock to create the master construction credential and the card is not accepted, the lock has either been programmed or already has a master construction credential.
- If the master construction credential cannot be located, or to put the lock back into construction access mode, reset the lock to factory settings (see page 10 for details).

Locks with keypads – Construction access mode

In the factory default state, locks with keypads have a default PIN of 13579 and “#”, which can be used for installation, testing and construction access. To test, enter default PIN. The Schlage button will blink and the lock will unlock.

The default PIN, 13579 and “#” is automatically deleted when a construction access user credential is added to the lock, or a new programming credential is created, or the lock is programmed with the SUS.

Locks with card readers – Create a master construction credential

The master construction credential is used to program construction access mode credentials.

To create a master construction credential:

1. Press and hold the Schlage button while presenting a credential.
2. The Schlage button will blink green on the left and right as confirmation.
3. Use this card to add construction access mode user credentials.

ⓘ **The master construction credential will not grant access. It is used only to add additional credentials.**

Locks with card readers – Add construction access mode user credentials

Construction access mode credential type	Steps to add construction access mode user credentials				
	1	**2**	**3**	**4**	**5**
Normal use construction credential Unlocks the lock for relock delay period	Present master construction credential to reader ➔	Green LEDs blink ➔	Present user credential within 20 seconds ➔	Green LEDs blink and credential is added ➔	Repeat steps 3 and 4 for additional credentials. Credentials added with the master construction credential will have 24/7 access.
Toggle construction credential Changes the state of the lock from locked to unlocked or vice versa	Present master construction credential to reader ➔	Green LEDs blink ➔	Press and hold Schlage button while presenting user credential within 20 seconds ➔	Green LEDs blink 5 times, 2 beeps will sound and credential is added ➔	

Cancel construction access mode

Do one of the following:

- Program the lock with the SUS. See the SUS user guide for more information.
- Reset the lock to factory settings. See *Reset to factory default settings on page 10* for more information.

When construction mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.

Link to a PIM400

ⓘ **Only one AD-400/AD-401 can be linked at one time. Ensure that no other PIM400 units are in link mode during this process.**

1. Make sure the batteries are installed in the AD-400/AD-401. See *Batteries* on page 12 for information.
2. Make sure the PIM400 is in link mode.
   For PIM400-TD2: Hold down one of the LINK buttons. (LINK button 1 or 2 will assign the AD-400/AD-401 door number).
   For PIM400-485: Use SUS to put the PIM400-485 into LINK mode with the door number tab and assign the AD-400/AD-401 door number. See the SUS User Guide for more information.
3. Open the AD-400/AD-401 door.
4. Create a request-to-exit condition by holding down the inside lever or crash bar.

TIP

During linking, the Schlage button will blink red and green. Green blinks indicate successful packets and red blinks indicate unsuccessful packets. If you get several red blinks, the lock and PIM400 may still link, but you may experience intermittent communication in the future. You should move the PIM400 closer to the lock, select another RF channel or add another PIM400.

ⓘ **If using a crash bar, Request to Exit (RTX) must be installed.**
If RTX is not installed, temporarily short the RTX input on the lock main PCB during this procedure.

5. While holding down the lever or crash bar, present a card to the prox or mag card reader. For a keypad reader, press the "#" key.
6. Continue to hold down the lever or crash bar until the AD-400/AD-401 Schlage button starts to blink green, indicating that the link process has begun (approximately 8 seconds).
7. Release the inside lever or crash bar.
8. The Schlage button will blink green, and the beeper will beep.

ⓘ **The number of green blinks and beeps indicates the frequency channel number on which the lock is linked to the PIM400 (example: 3 blinks and beeps = channel 3).**

9. If the link fails, the Schlage button will blink red three (3) times and five (5) short beeps will sound. The PIM400 will remain in link mode. Carefully repeat steps 1-8 above. If repeated LINK attempts fail, change the frequency channel of the PIM400 and/or move the PIM400, then repeat steps 3-7.
10. Test the lock for normal operation. See *Test lock operation* on page 9 for information.

Re-linking is required anytime the AD-400/AD-401 or the PIM400 is moved or replaced, Dynamic Channel Switching is activated, deactivated, or the frequency channel is manually changed.To re-link, repeat the procedure above. The AD-400/AD-401 link to the PIM400 is retained in the event of power loss.

Link LED and beep reference

Lights	Beeps	Action
1 Red, 1 Green	0	One link request was sent to find a PIM400 in link mode. This will repeat once and then the lock will stop trying to find a PIM400.
1 Green	0	Successful RF packet transmission
1 Red	0	Unsuccessful RF packet transmission
Z Green[1]	Z[1]	Linking was successful[1]
3 Red	5	Linking was unsuccessful

Z = Frequency channel number on which the lock is linked (1-10). The frequency channel number of each PIM400 in the area should be known and recorded. Use this information to make sure the AD-400/AD-401 linked to the intended PIM400.

Test lock operation

If you encounter problems while performing any of the following tests, review the installation instructions and this guide and correct any problems.

Mechanical test

1. Rotate the inside lever. Operation should be smooth, and the latch should retract.
2. Insert the key into the keyway and rotate the key, or the key and lever to open the door. Operation should be smooth, and the latch should retract.

Electronic test

Test the AD-400/AD-401 in factory default mode

1. For locks with a keypad, press any number key. The lock should beep.
2. Press the Schlage button. The keypad should light blue for a few seconds.
3. For locks with a card reader, present a credential to the reader. The lock will beep and the Schlage button will blink red one time. When the lock is in factory default mode, no credentials are accepted and the lock will respond with one red blink indicating the lock is not linked with the PIM400.
4. Locks with keypads, with or without additional credentials, have a default PIN of **13579** and "**#**". To test, enter the default PIN. The Schlage button will blink and the lock will unlock.

Test the AD-400/AD-401 in construction access mode

1. When the master construction credential is presented, the AD-400/AD-401 will beep and the Schlage button will light green for 20 seconds awaiting the presentation of another credential to be granted construction user access.
2. When a valid construction access user credential is presented, the lock will unlock for the re-latch delay period (default three seconds), and the Schlage button will blink green. When the lock
   re-locks after the re-latch delay period, the Schlage button will blink red.
3. If an invalid construction access user credential is presented, the lock will beep and the Schlage button will blink red one time. See *Construction access mode* on page 6 for more information.

NOTE: Construction access mode is cancelled when the lock is either linked to a PIM400, or reset to factory defaults. When construction access mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.

Test with the AD-400/AD-401 linked to the PIM400 and Access Control Panel (ACP)

Once the AD-400/AD-401 is linked to the PIM400, the SUS will indicate a successful link. The SUS will display AD-400/AD-401 operations and communication status with the PIM400.

1. In the SUS "demo/diagnostics" menu display for the PIM400, choose "Select door" and set a door number for the lock being tested. The SUS will display operation and status for: link, reader data, motor, tamper, battery, request-to-enter, request-to-exit and door position switch.

ⓘ **If the SUS demo/diagnostics "UNLOCK ON READ" box is checked, all credentials will unlock the AD-400/AD-401 during demo/diagnostics check.**

2. Present a valid credential to the AD-400/AD-401. The Schlage button will blink green, a beep will sound and the door will unlock for the preset lock delay period. The lock will re-lock after the lock delay period and the Schlage button will then blink red.
3. If an invalid credential is presented, the Schlage button will blink red, a beep will sound and the door will not unlock. Credential data for all credentials is reported to the PIM400 and displayed at the ACP.

Reset to factory default settings

ⓘ **All information in the lock will be deleted and reset to factory defaults!**

Level 1 factory default reset

ⓘ **Level 1 factory default reset will delete configurations and settings in the main controller in the lock.**

ⓘ **Level 1 factory default reset will not reset configurations and settings in the reader.**

1. Remove the top inside cover.
2. Press and hold the Schlage button until two (2) beeps sound (10 seconds).
3. Release the Schlage button.
4. Press and release the inside push button (IPB) three (3) times within 10 seconds. One beep will sound and one red blink will occur with each press.
5. The Schlage button and IPB will both light green for one second and a one-second beep will sound to confirm that the lock has been reset.

ⓘ **If IPB is not pressed 3 times within 10 seconds, two beeps with two red blinks indicate timeout.**

6. Replace the top inside cover.

Level 2 factory default reset

ⓘ **Level 2 factory default reset will delete all configurations and settings in the lock and the reader.**

ⓘ **Reader configurations that will reset to factory default include: keypad format, magstripe reader track, beeper on/off, and contactless card.**

ⓘ **Days in use counter and lock type configurations will not reset.**

To complete Level 2 factory default reset, repeat steps 2 through 5 above **within 10 seconds of the confirmation signals of Level 1 factory default reset**. If more than 10 seconds pass after the confirmation signals of Level 1 reset, then Level 1 reset will be repeated.

Communication properties

Property	Description
Heartbeat	When the lock is idle, the heartbeat is a brief communication from the lock to the PIM400. The heartbeat allows an idle lock to check for messages from the PIM400. By default, this occurs every 10 minutes, but can be adjusted in the range of 15 seconds to many hours. Short heartbeat intervals are suggested only if “Time Zones” accuracy of less than 10 minutes is desired. The value indicates the time between the heartbeats. Set the value to a shorter time (lower number) to achieve more frequent communication while the lock is idle. Set the value to a longer time (higher number) to achieve less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.
Immediate	When the lock is used, there is immediate communication to and from the PIM400 regardless of the heartbeat interval.
Wake-Up On Radio	When enabled, this feature causes the lock to respond within seconds to a centralized command from the access control panel. When disabled, the lock will respond only during its heartbeat, which could result in a delay. Test the function of Wake-Up On Radio, both lock and unlock operations, after all locks are installed. To test, verify that all locks go to the requested state with no assistance or intervention. If test fails, toggle Dynamic Channel Switching (DCS) to its opposite state (off to on, or on to off). Then, re-link all locks and test again.
Cache Mode	When enabled and communicating with the ACP, the lock keeps a local database of successful access grants. In the event of communication failure between the AD-400/AD-401 lock and PIM400, or between the PIM400 and the ACP, access is enabled for facility codes or recent valid users full card numbers. Note: When cache mode is configured for Smart cards, the default of “full card numbers” must be used. The local lock database does not capture audit events. See the SUS User Guide for more information.

Communication failure

When communication fails between the AD-400/AD-401 and the PIM400, the lock will go into communication failure mode. If the ACP or the PIM400 lose power, the AD-400/AD-401 can lock, unlock, remain as-is, or allow valid access without communicating to the ACP or the PIM400. This mode can be configured using the SUS. See the SUS user guide for more information.

Mode	Description
Fail unsecure unlocked	Lock unlocks and remains unlocked until communication is restored.
Fail secure locked	Lock locks and remains locked until communication is restored.
Fail as-is	Lock remains in current state until communication is restored.

In addition, the lock has an internal cache, that can be enabled using the SUS, to allow limited access while the lock is offline. If cache mode is enabled, it is not affected by the communication failure mode configuration. See the SUS User Guide for more information.

Installing or replacing batteries

Approximately one month prior to the end of the battery life, a Low Battery Trouble signal is indicated at the PIM400 and a Trouble signal will be sent to the access control panel.

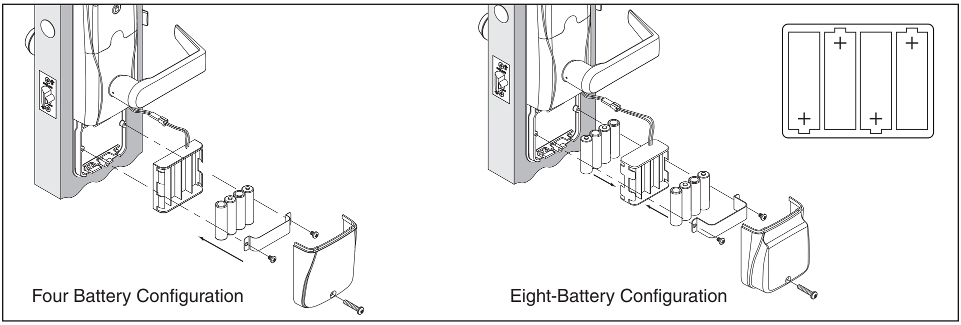
1. Remove the battery cover.
2. Remove the battery bracket. **Do not allow the battery pack to hang from the wires**.
3. Install the new batteries (install only new AA Alkaline batteries). Make sure the batteries are installed in the correct orientation.
4. Reinstall the battery pack and battery bracket.
5. Reinstall the battery cover, making sure the connector is above the battery pack.

CAUTION! Danger of explosion if battery is incorrectly replaced! Replace only with the same or equivalent type. Dispose of used batteries according to the manufacturer's instructions.

This product has been evaluated for ULC-S319 compliance with AA and coin cell batteries listed below. For installations requiring ULC-S319, these battery models should be used.

AA batteries: Duracell PC1500, MN1500; Energizer E91, EN91, AX91, XR91; RayoVac 815, 815-HE

Coin cell batteries: Energizer CR2025, CR2032; Maxell CR2025, CR2032, Panasonic CR2025, CR2032; RayoVac KECR2025, KECR2032



Four Battery Configuration

Eight-Battery Configuration

Low battery indications

ⓘ **Replacement of batteries does not affect any programmed data. Battery voltage can be checked with the SUS.**

ⓘ **When in a low battery condition the lock may operate but not have sufficient power to communicate with the SUS. When intitiating SUS communication, the Schlage button will light solid red for one second to indicate power is not sufficient. If this should occur, change the batteries immediately.**

Condition	Indicator	Solution
Low battery	No beeps Low battery condition is reported to the Access Control Panel.	Replace batteries immediately to avoid failure.
Battery failure (configured by SUS)	No LED or beeps Valid credentials do not grant access	Replace batteries immediately. Mechanical override key must be used to unlock the lock.

Battery failure modes

ⓘ **The battery failure mode is set using the SUS. See the SUS user guide for more information.**

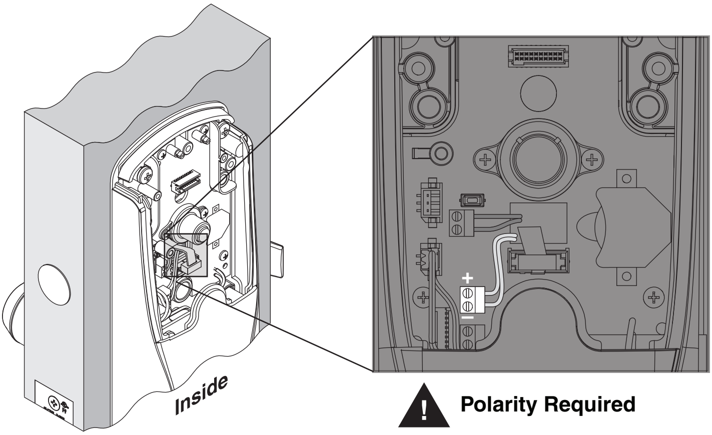
Mode	Description
Fail As-Is (default)	Lock remains in current state until batteries are replaced.
Fail Unlocked[1]	Lock unlocks and remains unlocked until batteries are replaced.
Fail Locked[1]	Lock locks and remains locked until batteries are replaced.

[1] Fail Unlocked and Fail Locked modes are not available if lock is externally powered.

External power supply

The AD-400/AD-401 may be connected to external power using a UL294 listed power supply for UL installations, and a power supply that complies with CAN/UL-S318 or CAN/ULC-S319 for cUL installations. The power supply must be capable of sourcing at least 250 mA @ 12 or 24 VDC (Schlage PS902, PS904, PS906).

DO NOT connect both external power and AA batteries at the same time.



⚠ **Polarity Required**

When externally powered, the lock will always fail as-is if power is lost.

LED and beep reference

The beep indicator may be enabled or disabled using the SUS. See the SUS User Guide for more information.

Action	Schlage button LEDs	Beeps
Extended (Toggle) unlock	2 green	0
Card presented and not read	None	0
Card presented and read	None	1
No communication with PIM400 or the ACP when card presented	1 red	0
Access denied	Controlled by ACP via PIM400	
Access granted, momentary unlock (motor runs)	1 green	0
Relock (motor runs)	1 red	0

Troubleshooting

Problem	Possible cause	Solution
The lock beeper does not sound and the keypad does not light when the Schlage button is pressed.	The reader may not be properly seated into the front escutcheon. The reader connector may have bent pins. The through door ribbon cable may not be properly plugged in. The battery or wired power may be improperly connected. The batteries may be inserted with incorrect polarity.	Check that the reader is fully seated into the front escutcheon. Check that there are no bent pins in the reader connector. Check that the through door ribbon cable is plugged in correctly. The red wire should be on the left and not pinched in the door. Check that the battery or wired power is connected correctly. Check that the batteries are inserted in the correct polarity. *Refer to the installation instructions that came with the AD-400/AD-401 lock, or this user guide for details on the above mentioned procedures.*
The AD-400/AD-401 will not link to the PIM400: When a valid credential is presented, the Schlage button blinks red one time OR PIM400 SUS Diagnostics shows the door status as not linked.	The lock and the PIM400 are not linked. The PIM400 is not in link mode before the link procedure. An incorrect door number was selected when linking the AD-400/AD-401. The Wireless Communication Module is not properly installed. The AD-400/AD-401 is located too far away from the PIM400. Data transmission to the access control panel is not successful even though green blinks are observed when linking to the PIM400.	Repeat the link procedure, making sure the PIM400 is in link mode before beginning the link procedure with the AD-400/AD-401. Check that you selected the correct door number when linking the AD-400/AD-401, and repeat the link procedure. Check that the Wireless Communication Module is installed and fully seated, and that there are no bent pins on the connector. The AD-400/AD-401 and PIM400 must be within 200 feet of each other, and on the same floor. The distance may be increased by using a remote antenna or another PIM400 located closer to the AD-400/AD-401. Check that the PIM400 is wired to the access control panel (ACP). Check that the ACP software has the AD-400/AD-401 door configured properly. On a 993 exit trim, make sure the Request To Exit switch is installed. *Refer to the lock installation instructions, and/or this user guide for details on the above mentioned procedures.*

Problem	Possible cause	Solution
The reader is not working.	The through hole ribbon cable may be pinched.	Check that the through hole ribbon cable is not pinched.
The Smart card is not reading.	The Smart card default of the card reader may not be correct for the Smart card.	Change the Smart card format using the SUS. Select AD-400/AD-401 “Lock Properties”, “Reader” tab, and “Smart cards in use”.
The magnetic swipe card is not reading correctly (no beeps or blinks).	The “Mag Track in Use” default for all Magnetic Card Credential Readers is “Track2”. The magnetic swipe card data may be on Track1 or Track3.	Use the SUS to change “Mag Track in Use”. Select AD-400/AD-401 “Lock Properties”, “Reader” tab, and “MAG Card Track selection”. *Refer to the installation instructions that came with the AD-400/AD-401 lock, or the SUS user guide for details on the above mentioned procedures.*

FCC/IC statements

The communication module is a 900 MHz transceiver for electronic locks and non-lock devices. The communication module links the access device to the Access Control Management System, with feedback control to the Access Device via a wireless means. The module contains the embedded firmware implementing the radio physical and data layers. There are 5 antennas approved for use with this module:

Approved antenna list:

The required antenna impedance is 50 ohms.

1. PCB trace antenna with a 5.7dBi maximum gain
2. p/n: 23520587, dual beam antenna with a 3.5dBi gain (ANT400-REM-HALL)
3. p/n: 23530579, multi band directional panel antenna with 8.5dBi gain (ANT400-REM-I/O+dB)
4. p/n: 23530553, dual band quasi-omni panel antenna with 4.5dBi gain (ANT400-REM-I/O)
5. p/n: 23520561, multi band omni antenna with 2dBi gain (ANT400-REM-CEILING)

Antennas having a gain greater than the antenna type approved in the list are strictly prohibited for use with this device. However, antennas of the same type with a gain equal to or less may be used. Examples of this may include:

- a directional panel antenna with a gain equal to or less than 8.5 dBi may be used with this module
- an omni-directional antenna with a gain equal to or less than 2.0 dBi may be used with this module

Specifications of the radio module:

Power output: 18.6 dBm Modulation: BPSK-40 Operating frequency: 906 -924 MHz

Note: The intended use of this module is not for the general public. It is generally for industry/commercial use only. This transceiver is to be professionally installed in the end product by Allegion, and not by a third party. The Schlage XPB-COMAD400V2 900 MHz Communication Board Module will not be sold to third parties via retail, general public or mail order. In the case of a repair, the transceiver will be replaced by a professional Installer.

Federal Communication Commission interference statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC/IC caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

To comply with FCC/IC RF exposure limits for general population/uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada statements

This Device complies with Industry Canada License-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

This radio transmitter, 8053B-COMAD400V2, has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated.

Approved antenna list:

The required antenna impedance is 50 ohms.

1. PCB trace antenna with a 5.7dBi maximum gain
2. p/n: 23520587, Dual Beam Antenna with a 3.5dBi gain (ANT400-REM-HALL)
3. p/n: 23530579, Multi band Directional Panel antenna with 8.5dBi gain (ANT400-REM-I/O+dB)
4. p/n: 23530553, Dual Band Quasi-Omni Panel Antenna with 4.5dBi gain (ANT400-REM-I/O)
5. p/n: 23520561, Multi band Omni Antenna with 2dBi gain (ANT400-REM-CEILING)

Antennas having a gain greater than the antenna type approved in the list are strictly prohibited for use with this device. However, antennas of the same type with a gain equal to or less may be used. Examples of this may include:

- a directional panel antenna with a gain equal to or less than 8.5 dBi may be used with this module
- an omni-directional antenna with a gain equal to or less than 2.0 dBi may be used with this module.

To comply with IC RF exposure limits for general population/uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.

Customer Service

1-877-671-7011 www.allegion.com/us

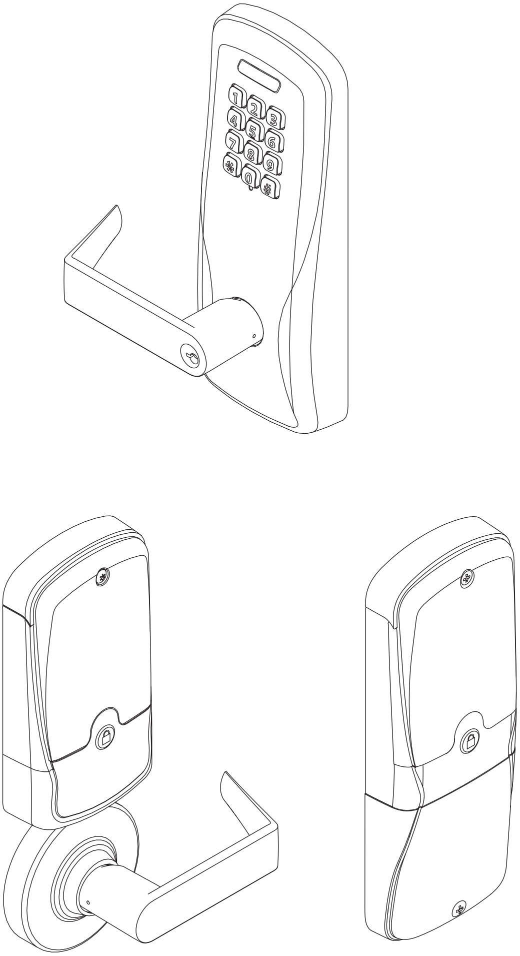
ALLEGION™

P516-270

CO-100

Offline lock user guide

Instructions for CO-Series offline locks



Para el idioma español, navegue hacia *us.allegion.com*.
Pour la portion française, veuillez consulter le site *us.allegion.com*.

Contents

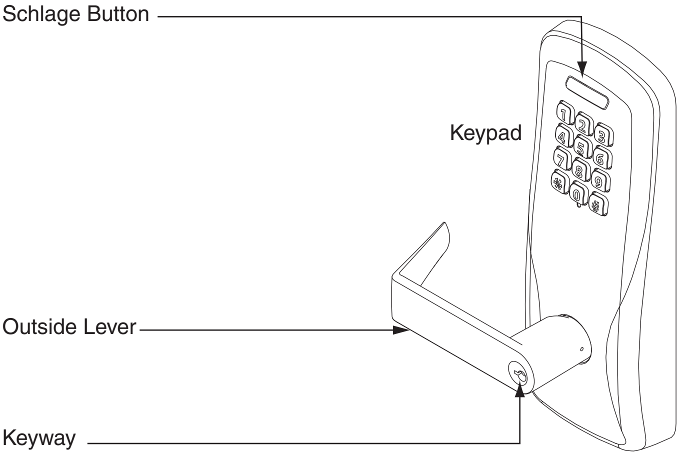
This product is compliant of UL 294 and ULC S319 standard. This product's compliance would be invalidated through the use of any add-on, expansion, memory or other module that has not yet been evaluated for compatibility for use with this UL Listed product, in accordance with the requirements of the Standards UL 294 and ULC S319. This product has been evaluated for ULCS319 Class I.

Overview

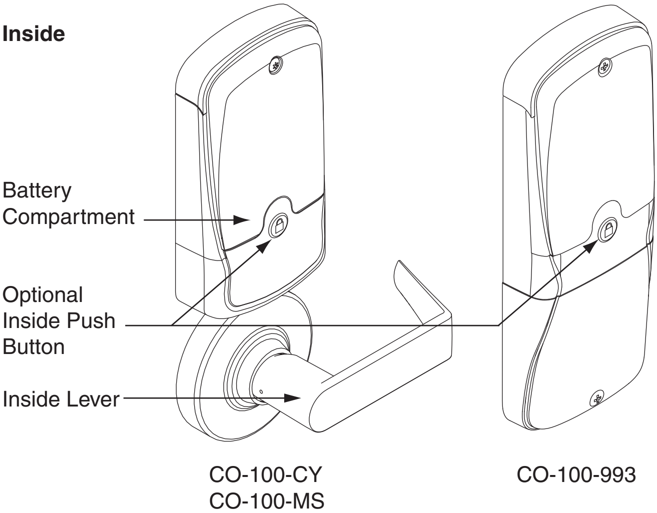
The Schlage CO-100 is a keypad-only off-line electronic lock in the CO-Series product line.

- This product is listed for UL 294 and ULC S319.
- Three factory-configured functions are available: 1) Classroom/Storeroom, 2) Office and 3) Privacy.
- The lock is powered by four (4) AA batteries. See *Batteries* on page 12 for more information.
- Outside lever is normally locked.
- Inside lever always allows egress.

Outside



Inside



Lock functions

The CO-100 lock is available in one of three functions:

Privacy (40): Privacy function is available on locks with firmware version 2.6.2 or higher. Lockset is normally secure. Inside Push Button is pressed to disable normal electronic access from outside (activates privacy). Another press of Inside Push Button restores normal electronic access (deactivates privacy).

Office (50): Lockset is normally secure. Inside Push Button may be used to select passage or secured status.

Classroom/Storeroom (70): Lockset is normally secure. Valid toggle credentials may be used to change to a passage or secure status.

Getting started

Follow these steps when setting up a new lock.

1. Install the lock. See the installation guide that came with the lock or visit us.allegion.com (Support>Document Library>Schlage>Electronic Locks, search on “CO-Series” and select Installation Instructions) for more information.
2. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 8 for more information.
3. When ready to set up for normal use, enter a new programming code, then program the user credentials. See *Manual programming instructions* on page 5.
4. Familiarize yourself with the information in this guide.

Save this user guide for future reference.

Construction access mode

Construction access mode is used to allow access before the lock has been programmed, and for testing purposes. Construction access mode is enabled by default.

Offline locks with keypads have a default PIN of 13579 and “#”, which can be used for installation, testing and construction access.

- To test, enter the default PIN (13579 and “#”).
- The Schlage button will blink and the lock will unlock.
- The default PIN is automatically deleted when a new programming credential is created.

TIP

If you press the default PIN code on a new lock and the code is not accepted, the lock has already been programmed.

If the new PIN is not known, or to put the lock back into construction access mode, reset the lock to factory settings. See *Reset to factory defaults* on page 11 for more information.

Credential types and functions

Programming credential: A 5 digit code used only for lock programming.

PIN credential: A 3-6 digit code entered on the keypad.

Note: A unique credential must be used for each credential type described below (for example, a single credential may not be used for both normal use and toggle functions).

Credential type	Function
Programming PIN	Used only to program the lock. Does not unlock the lock.
Normal use PIN	Unlocks the lock *momentarily* after a credential is entered.
Toggle PIN	Changes the state of the lock from locked (secured) to unlocked (unsecured), or vice versa, unless in a Freeze state.
Freeze PIN	Freezes the lock in the current state. The lock remains frozen until any Freeze credential is entered again. (A pass-through credential will override a lock in frozen state as described below).
Pass-through PIN	Unlocks a lock *momentarily*, regardless of state. A valid Pass-through credential can unlock a door set to any secured lockout mode (e.g., Freeze, Privacy, Time Zones, Door Auto-Locks and Holidays). The door will relock after the specified relock time.

Manual programming instructions

Important notes:

- ⓘ **Wait for the Schlage button LEDs to stop flashing before continuing to the next step.**
- ⓘ **Programming mode will time out if no entry is made in 20-25 seconds. Time out is indicated by three left and nine right red blinks of the Schlage button.**
- ⓘ **An incorrect entry is indicated by a solid red left and blinking green right LED on the Schlage button. Refer to** *Error codes* **on page 8 to interpret error code patterns.**
- ⓘ **A unique PIN must be used for each credential type (for example, a single PIN may not be used for both normal use and toggle functions).**

PROGRAMMING credential

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!			
	1	2	3	4
Create new Programming Code (PIN)	Enter 9 7 5 3 1 ✱ (This is the default programming PIN)	Enter 7 ✱	Enter new 5 digit Programming code and ✱ Wait for right green light.	Reenter the new 5 digit Programming code and ✱ Wait for confirmation: 2 right green blinks.

Note: Programming codes such as 1-1-1-1-1 or 1-2-3-4-5 can be easily selected by non-authorized users and should not be used.

NORMAL USE credentials

Note: Until a new Normal Use PIN is created, the default PIN is 1 3 5 7 9 #

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Normal Use PIN	Enter Programming PIN and *	Enter 3 *	Enter new 3-6 digit PIN and * *	For another PIN, go back to step 3	Press * again to finish	Wait for confirmation: 2 right green blinks.

TOGGLE credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Toggle PIN	Enter Programming PIN and *	Enter 3 3 *	Enter 1 9 1 *	Enter new 3-6 digit PIN and * * Wait for right green light.	For another PIN, go back to step 3 OR press * again to finish	Wait for confirmation: 2 right green blinks.

FREEZE credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Freeze PIN	Enter Programming PIN and *	Enter 3 3 *	Enter 1 1 5 *	Enter new 3-6 digit PIN and * * Wait for right green light.	For another PIN, go back to step 3 OR press * again to finish	Wait for confirmation: 2 right green blinks.

PASS THROUGH credentials

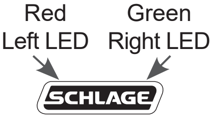
To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Pass Through PIN	Enter Programming PIN and ✱	Enter 3 3 ✱	Enter 1 1 9 ✱	Enter new 3-6 digit PIN and ✱ ✱ Wait for right green light.	For another PIN, go back to step 3 OR press ✱ again to finish	Wait for confirmation: 2 right green blinks.

OTHER programming

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!				
	1	2	3	4	5
Delete a PIN	Enter Programming PIN and ✱	Enter 5 ✱	Enter the PIN to be deleted and ✱	To delete another PIN, go back to step 3 OR press ✱ again to finish	Wait for confirmation: 2 right green blinks.
Change PIN length (Available with firmware version 2.5.0 or higher.)	Enter Programming PIN and ✱	Enter 9 9 ✱	Enter 4 ✱	Enter 3, 4, 5, OR 6 for desired PIN length	Press ✱ again to finish Wait for confirmation: 2 right green blinks.
Change relock delay period	Enter Programming PIN and ✱	Enter 9 9 ✱	Enter 1 ✱	Each button press adds to the total delay time Example: 1 + 9 adds a 10 second delay	Press ✱ again to finish Wait for confirmation: 2 right green blinks.
Disable/ enable beeper	Enter Programming PIN and ✱	Enter 9 9 ✱	Enter 3 ✱	Enter 0 ✱ to disable beeper OR 7 ✱ to enable beeper	Press ✱ again to finish Wait for confirmation: 2 right green blinks.
Disable/ enable remote release feature	Enter Programming PIN and ✱	Enter 9 9 ✱	Enter 2 ✱	Enter 0 ✱ to disable remote release OR 7 ✱ to enable remote release	Press ✱ again to finish Wait for confirmation: 2 right green blinks.

Error codes

ⓘ **All error codes are indicated on the Schlage button by a solid red left LED, and a blinking green right LED. The number of green blinks indicates the error code.**



Number of green blinks	Error code description
2	Too long programming/user code entered. Programming code must be five (5) digits. User code length cannot exceed six (6) digits.
3	Memory full, too many codes. Delete some codes.
4	Programming code cannot be deleted, only changed.
5	Programming code entries do not match. Programming code not changed.
6	Invalid command. Invalid function code entered.
7	Code not found.
8	Code too short. Programming code length must be five (5) digits. User code minimum length is three (3) digits.
9	Not a unique code.

Error code functions have not been verified by Underwriters Laboratories Inc.

Test lock operation

If you encounter problems while performing any of the following tests, review the installation guide and correct any problems.

Mechanical test

1. Rotate the inside lever or depress the push bar to open the door. Operation should be smooth, and the latch should retract.
2. Insert the key into the keyway and rotate the key and the outside lever to open the door. Operation should be smooth, and the latch should retract.

Electronic test

1. Press any number key. The lock will beep. Use the default PIN (13579 and “#”) to verify access.

Normal lock operation

After PIN credentials have been programmed, enter a PIN to operate the lock:

Press a valid PIN. The green LED will blink and access is granted.

The “#” key is used as ENTER key for PINs with fewer than six digits. Default minimum digits is six (6). PIN length may be manually configured so users do not have to push the “**#”** key (see *Change PIN length* on page 7).

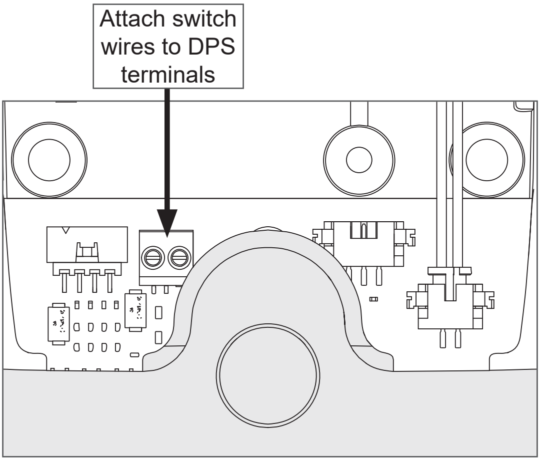
If the PIN credential is entered incorrectly, press “*” to start over.

System requirements

- Available on CO-100 Office function only.
- The CO-100 must be programmed with CO-100 version 2.6.2 firmware or higher.

Switch specifications, wire specifications and routing

- Recommended switch: basic SPST (single-pole single-throw) momentary action switch with normally open contact configuration.
- Wire gauge AWG 24, stranded, twisted pair, shielded. (Shielded cable is optional. If shield is present, only one end of the cable shield should be terminated to chassis ground).
- Belden 9841 or equivalent.
- Maximum cable length is 1000 feet (305 meters).
- Route wires from the switch, through the door frame and door to the door position switch terminals as shown below.



Wired remote release operation

- When the remote release button is pressed the lock will unlock for the programmed relock delay period. The green Schlage LEDs and the green inside push button LED will turn on to indicate the lock is unlocked. If the beeper function is turned on, the beeper will sound one time to indicate the lock is unlocked.
- After the relock delay period has expired, the green Schlage LEDs and the green inside push button LED will turn off. If the beeper function is turned on, the beeper will sound two times to indicate the lock is relocked.

Wired remote release button action

- If the remote release button is pressed and held, the release will function only one time, even in the event the button is held longer than the relock delay period.
- If the remote release button is quickly pressed repeatedly, the release will function only one time. Any additional button presses during the relock delay period are ignored.
- Once the lock relocks, the next press of the remote release button will activate a new release cycle.

Lock status reports

Follow the steps below to obtain lock status reports:

ⓘ **Lock status reporting is available with firmware version 2.5.0 or higher.**

ⓘ **The left and right Schlage button LEDs will blink red once with each button press, followed by the status indicator as described below.**

Function / Report	Press	Indicator/Report result
Initiate report mode	Press and hold SCHLAGE while pressing 9 9 #	Wait until only the right Schlage button LED is on to indicate the lock is in report mode and awaiting an entry. If no entry is made, then timeout will occur in 20 seconds.
Battery status	1	Left LED: Solid green = normal Blinking red = low No indicator = critical battery

Once a status is reported, both left and right LEDs will light green, followed by solid green on the right LED only. The right green LED indicates the lock is awaiting another entry.

Obtain an additional status report as described below, or press * to exit report mode.

Function / Report	Press	Indicator/Report result
Firmware status	3	Left LED blinks green for the version number Decimal point is indicated by one red blink “Zero” is indicated by two red blinks
Hardware status	4	
PCB serial number	6	Left LED blinks green for each number Each number is separated by one red blink Press # after two red blinks to display the next number

If no entry is made within 20 seconds of the solid green right LED, then timeout will occur.

To exit report mode at any time, press * .

Reset to factory defaults

All information in the main controller in the lock will be deleted and reset to factory defaults!

Main controller configurations that will reset to factory default include: programming and user codes.

The door must be locked (not toggled open or in the middle of normal access) before resetting to factory defaults.

Follow these steps to reset to factory defaults.

1. Remove the top inside cover.
2. Remove one battery from the battery pack to disrupt power. Wait 5 to 10 seconds for power to run out in the lock.
3. Press and hold the Schlage button while reconnecting the battery into the battery pack to resupply power.
4. Continue holding the Schlage button, and wait for two beeps to sound and two green blinks of the Schlage button.
5. Release the Schlage button.
6. Press and release the Schlage button three (3) times within 10 seconds of the beeps and blinks at step 4. One beep will sound and one red blink will occur with each press.
7. The Schlage button will light green for one second and a one-second beep will sound, indicating that the lock has been reset.

ⓘ **If the Schlage button is not pressed 3 times within 10 seconds, two beeps and two red blinks indicate timeout.**

8. Replace the top inside cover.

To test, enter 13579 and “#”. The Schlage button will blink and the lock will unlock momentarily.

Batteries

To install or replace alkaline batteries

ⓘ **Changing batteries does not affect any programmed data.**

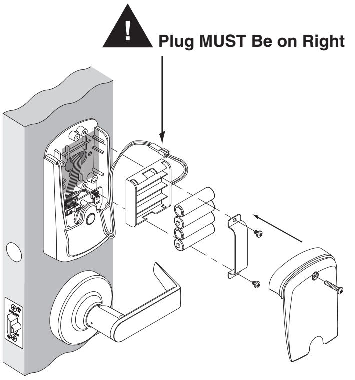
1. Remove the battery cover.
2. Remove the battery bracket. Do not allow the battery pack to hang from the wires.
3. Install the new batteries (install only new AA Alkaline batteries). Make sure the batteries are installed in the correct orientation.
4. Reinstall the battery pack and battery bracket.
5. Reinstall the battery cover, making sure the plug is to the right of the battery pack (CY, MS and MD locks). **Be careful not to pinch the battery wires when installing the battery cover.**

CAUTION! Danger of explosion if batteries are incorrectly replaced! Replace only with new AA alkaline batteries. Dispose of used batteries according to the manufacturer's instructions.

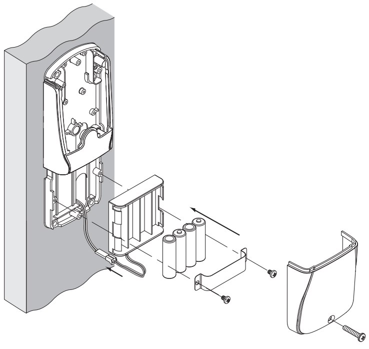
This product has been evaluated for ULCS319 compliance with AA and coin cell batteries listed below. For installations requiring ULCS319, these battery models should be used.

AA batteries: Duracell PC1500, MN1500; Energizer E91, EN91, AX91, XR91;
RayoVac 815, 815-HE

Coin cell batteries: Energizer CR2025, CR2032; Maxell CR2025, CR2032,
Panasonic CR2025, CR2032; RayoVac KECR2025, KECR2032.



CY, MS



993

Low battery indications

Condition	Indicator	Solution
Batteries low	After credential PIN is pressed, 9 red blinks of Schlage button, then normal indicator.	Replace batteries immediately to avoid battery failure. Lock is intended to operate for 500 cycles in low battery condition.
Battery failure	No LED or beeps Valid credentials do not grant access	Replace batteries immediately. Mechanical override key must be used to unlock the lock.

Battery failure mode

In the event of battery failure, the lock will fail As-Is (lock remains in current state, locked or unlocked, until batteries are replaced).

LED reference

Schlage button

Condition	Lights
Access denied	2 red blinks
Valid PIN entered while lock in Freeze mode	12 red blinks indicating lockout
Factory default reset	One-second solid green with one-second beep
Low battery indicator, AA batteries	9 left red blinks
Momentary unsecured access	1 green blink, then one red blink on relock

Optional Inside Push Button (IPB)

Action	Lights
Office Mode	
Press IPB to lock	1 red blink
Press IPB to unlock[1]	1 green blink
Privacy Mode	
With door closed, press IPB to engage privacy	4 green blinks
With door closed, press IPB to release privacy	4 red blinks

[1] Unlocking the lock with the IPB will cause the lock to remain unlocked until the IPB is depressed again.

Problem	Possible cause	Solution
The lock does not function when a valid PIN credential is entered, or the lock beeper does not sound.	The beeper may be turned off. The battery or wired power may be improperly connected. The batteries may be inserted with incorrect polarity. The batteries may be depleted. If applicable, the IPB through-door ribbon cable may not be properly plugged in, or may have bent pins.	Use manual programming to enable the beeper (see *Disable/enable beeper* on page 7). Check that the battery or wired power is connected correctly. Check that batteries are inserted in the correct polarity. Replace batteries. Check that the optional IPB through-door ribbon cable is plugged in correctly (if applicable). The red wire should be on the left and not pinched in the door. Check that there are no bent pins on the optional IPB through-door cable. *Refer to the installation instructions that came with the CO-100 lock, or this user guide for details on the above mentioned procedures.*
Wired remote release feature is not working.	The lock may not be compatible with remote release. The firmware version may not be compatible with remote release. The remote release switch may not be functioning correctly.	Wired remote release is available only on the CO-100 Office function. Wired remote release is compatible with locks programmed with CO-100 version 2.6.2 firmware or higher. Check that the switch closes and delivers less than 5 ohms resistance when activated.

FCC Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. **this device may not cause harmful interference, and**
2. **this device must accept any interference received, including interference that may cause undesired operation.**

Customer Service

1-877-671-7011 www.allegion.com/us

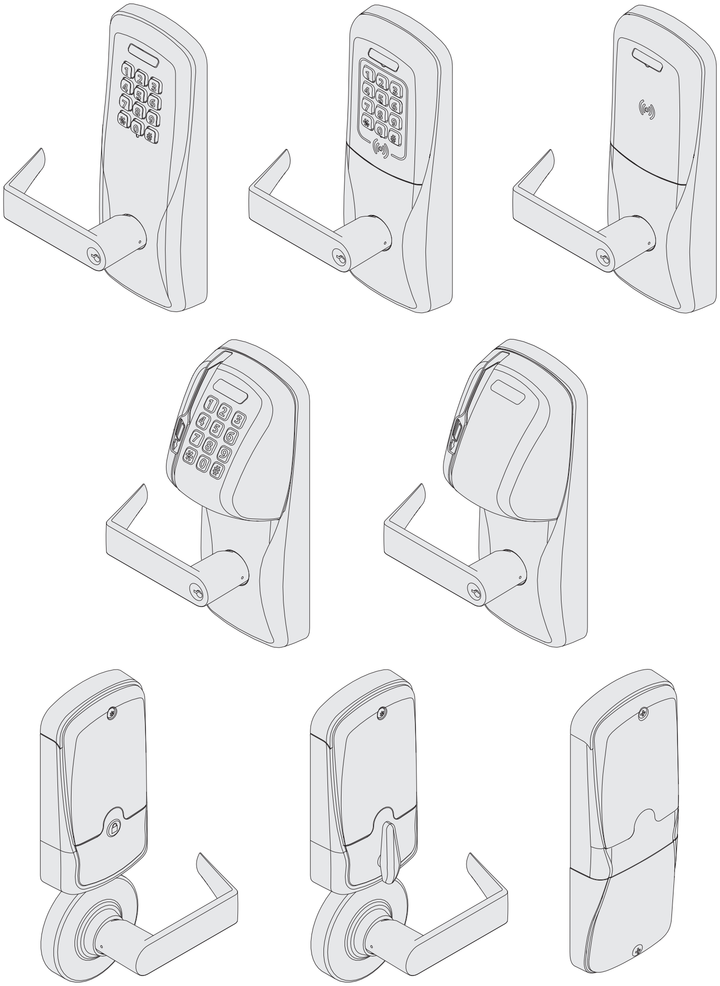
ALLEGION™

P516-271

CO-200

Offline lock user guide

Instructions for CO-Series offline locks



Para el idioma español, navegue hacia www.allegion.com/us.
Pour la portion française, veuillez consulter le site www.allegion.com/us.

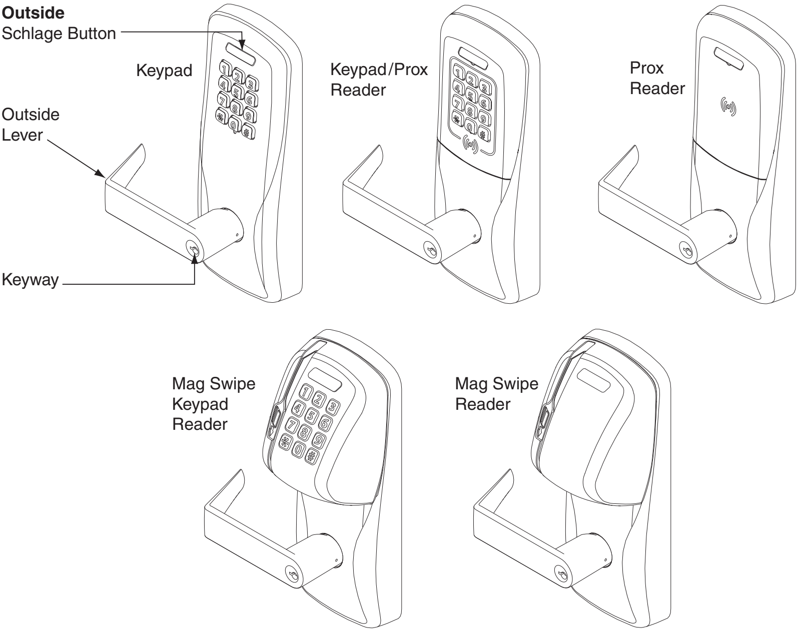
Contents

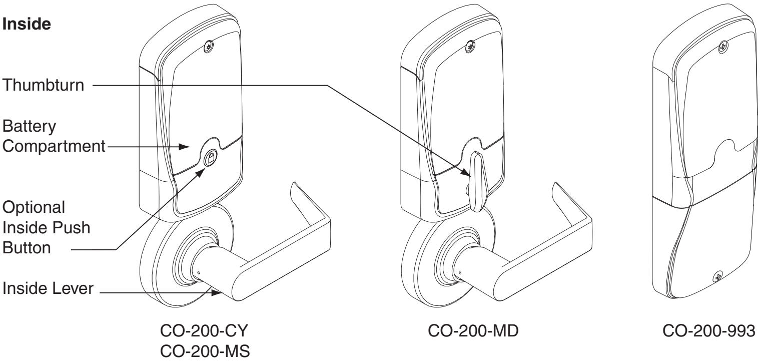
This product is compliant of UL 294 and ULC S319 standard. This product's compliance would be invalidated through the use of any add-on, expansion, memory or other module that has not yet been evaluated for compatibility for use with this UL Listed product, in accordance with the requirements of the Standards UL 294 and ULC S319. This product has been evaluated for ULC-S319 Class I.

Overview

The Schlage CO-200 is an off-line electronic lock in the CO-Series product line.

- This product is listed for UL 294 and ULC S319.
- The lock is configured to operate as Classroom/Storeroom function. Optional Office or Privacy functions are available.
- The lock is powered by four (4) AA batteries. See *Batteries* on page 16 for more information.
- Outside lever is normally locked.
- Inside lever always allows egress.
- The lock maintains an audit trail of events in the normal operating mode.
- The lock is configured using the Schlage Utility Software (SUS). See *Schlage Utility Software (SUS)* on page 4 for more information.





Lock functions

The CO-200 is available in one of three functions:

Privacy (40): Lockset is normally secure. Pressing the Inside Push Button or extending the deadbolt will disable normal electronic access from the outside. Opening the door, retracting the deadbolt or pressing the Inside Push Button a second time deactivates the privacy status.

Office (50): Lockset is normally secure. Inside Push Button may be used to select passage or secured status.

Classroom/Storeroom (70): Lockset is normally secure. Valid toggle credentials may be used to change to a passage or secure status.

Getting started

Follow these steps when setting up a new lock.

1. Install the lock. See the installation guide that came with the lock or visit www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library) for more information.
2. Make sure the batteries are installed properly. See *Batteries* on page 16 for more information.
3. Before programming, the lock may be used in construction access mode. See *Construction access mode* on page 5 for more information. The lock should remain in construction access mode until you are ready to set up the rest of the system.
4. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 14 for more information.
5. When ready to set up for normal use, remove factory default security settings, then program the user credentials. See *Manual programming instructions* on page 7 for more information.
6. Consult the Schlage Utility Software (SUS) user guide for information about configuring the lock.
7. Familiarize yourself with the information in this guide.

Save this user guide for future reference.

Schlage Utility Software (SUS)

The Schlage Utility Software is used for programming and setup only.

The Schlage Utility Software (SUS) is used to configure locks. The SUS configures lock functions that cannot be configured with manual programming, and is used to transfer data files between the access control software and locks.

For more information about the SUS, see the SUS user guide.

Construction access mode

Construction access mode is used to allow access before the lock has been programmed, and for testing purposes.

- Enabled by default.
- The lock will remain in construction access mode until the mode is cancelled as described below.
- No audits are captured while lock is in construction access mode.

Create the master construction credential - locks with card readers

1. Press and hold the Schlage button while presenting a credential.
2. This credential becomes the master construction credential, and is used to program construction access.
3. The Schlage button will blink green on the left and right as confirmation.

After you have created the master construction credential, you can then use that card to add construction access mode user credentials.

ⓘ **The master construction credential will not grant access. It is used only to add additional credentials.**

> **TIP**
>
> Use the same master construction credential for all the locks in the facility.
>
> If you present the first card to a new lock to create the master construction credential and the card is not accepted, the lock has either been programmed or already has a master construction credential.
>
> If the master construction credential cannot be located, or to put the lock back into construction access mode, reset the lock to factory settings. See *Reset to factory defaults* on page 15 for more information.

Locks with card readers – Add construction access mode user credentials

Construction access mode credential type	Steps to add construction access mode user credentials				
	1	2	3	4	5
Normal use construction credential Unlocks the lock for relock delay period	Present master construction credential to reader ➔	Green LEDs blink ➔	Present user credential within 20 seconds ➔	Green LEDs blink and credential is added ➔	Repeat steps 3 and 4 for additional credentials. Credentials added with the master construction credential will have 24/7 access.
Toggle construction credential Changes the state of lock from locked to unlocked or vice versa	Present master construction credential to reader ➔	Green LEDs blink ➔	Press and hold Schlage button while presenting user credential within 20 seconds ➔	Green LEDs blink, 2 beeps will sound and credential is added ➔	

Cancel construction access mode

Construction access mode may be cancelled by one of the following methods:

- load a door file using the SUS
- reset the lock to factory settings (see *Reset to factory defaults* on page 15 for more information).

When construction mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.

Locks with keypads

In the factory default reset state, offline locks with keypads, with or without additional credentials, have a default PIN of 13579 and “#”, which can be used for installation, testing and construction access. To test, enter 13579 and “#”. The Schlage button will blink and the lock will unlock. The default PIN is automatically deleted when a new programming credential is created, construction credentials are created, or the lock is programmed with the Schlage Utility Software (SUS).

Credential types and functions

Programming credential: A card or 5 digit code used only for lock programming.

Card or PIN credentials: A card that is presented, or a 3-6 digit code entered on the keypad.

Card ID number: When adding any new card credential, a 3-6 digit code is entered prior to presenting the card. This code becomes the Card ID Number. This number can be used to delete a card credential without physically having the card. *Keep a log of all Card ID Numbers for future reference.*

Note: A unique credential must be used for each credential type described below (for example, a single credential may not be used for both normal use and toggle functions).

Credential type	Function
Programming PIN or card	Used only to program the lock. Does not unlock the lock.
Normal use credential	Unlocks the lock *momentarily* after a credential is presented or entered.
Toggle credential	Changes the state of the lock from locked (secured) to unlocked (unsecured), or vice versa, unless in a Freeze state.
Freeze credential	Freezes the lock in the current state. The lock remains frozen until any Freeze credential is presented again. (A pass-through credential will override a lock in frozen state as described below).
Pass-through credential	Unlocks a lock *momentarily*, regardless of state. A valid Pass-through credential can unlock a door set to any secured lockout mode (e.g., Freeze, Privacy, Time Zones, Door Auto-Locks and Holidays). The door will relock after the specified relock time.

Credential forms

Normal, toggle, freeze and pass-through credential types are used in one of three forms:

PIN credential – a 3-6 digit code entered on the keypad.
CARD credential – a card presented to the lock.
CARD + Card ID Number credential – a card (with a unique Card ID number) presented to the lock. (See a description of Card ID number above for more information.)

Steps for designating each form are in the *Manual programming instructions* on the following pages.

Manual programming instructions

Important notes:

- ⓘ **Wait for the Schlage button LEDs to stop flashing before continuing to the next step.**
- ⓘ **Programming mode will time out if no entry is made in 20-25 seconds. Time out is indicated by three left and nine right red blinks of the Schlage button.**
- ⓘ **An incorrect entry is indicated by a solid red left and blinking green right LED on the Schlage button. Refer to *Error codes* on page 13 to interpret error code patterns.**
- ⓘ **A unique credential must be used for each credential type (for example, a single credential may not be used for both normal use and toggle functions).**

PROGRAMMING credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!			
	1	2	3	4
Create new Programming Code (PIN)	Enter 9 7 5 3 1 * (This is the default programming PIN)	Enter 7 *	Enter new 5 digit Programming code and * Wait for right green light.	Reenter the new 5 digit Programming code and * Wait for confirmation: 2 right green blinks.
Create new Programming Card	Enter 9 7 5 3 1 *	Enter 7 *	Present new programming card.	Wait for confirmation: 2 right green blinks.

Note: Programming codes such as 1-1-1-1-1 or 1-2-3-4-5 can be easily selected by non-authorized users and should not be used.

ⓘ Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).

NORMAL USE credentials

Note: Until a new Normal Use PIN is created, the default PIN is 1 3 5 7 9 #

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Normal Use PIN	Enter Programming PIN and * OR Present Programming card	Enter 3 *	Enter new 3-6 digit PIN and * *	For another PIN, go back to step 3	Press * again to finish	Wait for confirmation: 2 right green blinks.
Create a Normal Use CARD	Enter Programming PIN and * OR Present Programming card	Enter 3 *	Enter new 3-6 digit Card ID Number and *	Wait for right green light. Present new CARD to lock.	For another CARD, go back to step 3 OR press * again	Wait for confirmation: 2 right green blinks.
Create a Normal Use CARD + Card ID Number	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 3 1 1 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press * again to finish Wait for confirmation: 2 right green blinks.

ⓘ Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).

TOGGLE credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Toggle PIN	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 1 9 1 *	Enter new 3-6 digit PIN and * * Wait for right green light.	For another PIN, go back to step 3 OR press * again to finish	Wait for confirmation: 2 right green blinks.
Create a Toggle CARD	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 1 9 1 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD, go back to step 3 OR press * again to finish Wait for confirmation: 2 right green blinks.
Create a Toggle CARD + Card ID Number	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 3 9 1 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press * again to finish Wait for confirmation: 2 right green blinks.

ⓘ Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).

FREEZE credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Freeze PIN	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 1 1 5 *	Enter new 3-6 digit PIN and * * Wait for right green light.	For another PIN, go back to step 3 OR press * again to finish	Wait for confirmation: 2 right green blinks.
Create a Freeze CARD	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 1 1 5 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD, go back to step 3 OR press * again to finish Wait for confirmation: 2 right green blinks.
Create a Freeze CARD + Card ID Number	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 3 1 5 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press * again to finish Wait for confirmation: 2 right green blinks.

ⓘ Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).

PASS THROUGH credentials

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!					
	1	2	3	4	5	6
Create a Pass Through PIN	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 1 1 9 *	Enter new 3-6 digit PIN and * * Wait for right green light.	For another PIN, go back to step 3 OR press * again to finish	Wait for confirmation: 2 right green blinks.
Create a Pass Through CARD	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 1 1 9 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD, go back to step 3 OR press * again to finish Wait for confirmation: 2 right green blinks.
Create a Pass Through CARD + Card ID Number	Enter Programming PIN and * OR Present Programming card	Enter 3 3 *	Enter 3 1 9 *	Enter new 3-6 digit Card ID Number and * Wait for right green light.	Present new CARD to lock.	For another CARD+Card ID credential, go back to step 4 OR press * again to finish Wait for confirmation: 2 right green blinks.

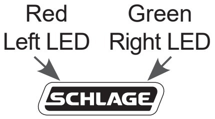
ⓘ Note: Before creating any credential in the following steps, determine which credential form is desired (see *Credential forms* on page 6).

OTHER programming

To complete this action:	Perform the following steps: Wait for SCHLAGE to stop flashing between each step!				
	1	2	3	4	5
Delete a credential	Enter Programming PIN and * OR Present Programming card	Enter 5 *	Enter the PIN or Card ID Number to be deleted and *	To delete another Card credential, go back to step 3 OR press * again to finish	Wait for confirmation: 2 right green blinks.
Change PIN length	Enter Programming PIN and * OR Present Programming card	Enter 9 9 *	Enter 4 *	Enter 3, 4, 5, OR 6 for desired PIN length	Press * again to finish Wait for confirmation: 2 right green blinks.
Change relock delay period	Enter Programming PIN and * OR Present Programming card	Enter 9 9 *	Enter 1 *	Each button press adds to the total delay time Example: 1 + 9 adds a 10 second delay	Press * again to finish Wait for confirmation: 2 right green blinks.
Disable/ Enable Beeper	Enter Programming PIN and * OR Present Programming card	Enter 9 9 *	Enter 3 *	Enter 0 * to disable beeper OR 7 * to enable beeper	Press * again to finish Wait for confirmation: 2 right green blinks.

Error codes

ⓘ **All error codes are indicated on the Schlage button by a solid red left LED, and a blinking green right LED. The number of green blinks indicates the error code.**



Number of green blinks	Error code description
1	Computer programming error (not complete).
2	Too long programming/user code entered. Programming code must be five (5) digits. User code length cannot exceed six (6) digits.
3	Memory full, too many codes. Delete some codes.
4	Programming code cannot be deleted, only changed.
5	Programming code entries do not match. Programming code not changed.
6	Invalid command. Invalid function code entered.
7	Code not found.
8	Code too short. Programming code length must be five (5) digits. User code minimum length is three (3) digits.
9	Not a unique code.
10	Manual programming not allowed.

Error code functions have not been verified by Underwriters Laboratories Inc.

Test lock operation

If you encounter problems while performing any of the following tests, review the installation guide and correct any problems.

Mechanical test

1. Rotate the inside lever or depress the push bar to open the door. Operation should be smooth, and the latch should retract.
2. Insert the key into the keyway and rotate the key and the outside lever to open the door. Operation should be smooth, and the latch should retract. The Schlage button will light solid green until the key is released and the latch is extended.

Test in factory default mode

1. For locks with a keypad, press any number key. The lock will beep and the Schlage button will blink red.
2. The Schlage button will blink red twice when a credential is presented and the lock is in factory default mode, and has no access programming.
3. For locks with keypads, enter the default PIN (13579 and “#”) to verify access. The Schlage button will blink green, a beep will sound, and the door will unlock for the preset relock delay period. After the relock delay period, the lock will relock and the Schlage button will blink red. If the lever retracts and holds the latch through the relock delay period, then the Schlage button will light green until the lever is released.

Test in normal operation mode

1. Present a valid credential. The Schlage button will blink green, a beep will sound and the door will unlock for the preset lock delay period. The lock will re-lock after the lock delay period and the Schlage button will then blink red. If the lever retracts and holds the latch through the relock delay period, then the Schlage button will light green until the lever is released.
2. If an invalid credential is presented, the Schlage button will blink red, a beep will sound and the door will not unlock.

Normal lock operation

After credentials have been programmed, present credentials to operate the lock as follows:

Credential type	Action			
PIN or Card	Present or enter credential to reader ➔ Green blink and access granted			
Card+Card ID Number	Present credential to reader ➔	Press Card ID Number [1] ➔	Within 5 seconds, Press # [2] ➔	Green blink and access granted

[1] If the Card ID is entered incorrectly, press “*” to start over.

[2] The default PIN/Card ID length is six (6) digits. The "#" key must be used as an ENTER key for PINs/Card IDs with fewer than six digits. PIN length can be configured using the SUS, so users do not have to press "#" key.

Reset to factory defaults

All information in the lock will be deleted and reset to factory defaults!

The door must be locked (not toggled open or in the middle of normal access) before resetting to factory defaults.

Level 1 factory default reset

ⓘ **Level 1 factory default reset will delete configurations and settings in the main controller in the lock.**

ⓘ **Main controller configurations that will reset to factory default include: programming and user codes.**

ⓘ **Level 1 factory default reset will not reset configurations and settings in the reader.**

1. Press and hold the Schlage button. Wait for the lock to beep twice and two green blinks of the Schlage button, indicating confirmation.
2. After confirmation signals, release the Schlage button.
3. Rotate the mechanical key within 10 seconds and hold. The Schlage button will light green. Continue holding the key until confirmation signals are observed (the Schlage button light will turn off one second and a one second beep will sound). After confirmation signals, release the mechanical key.
4. The Schlage button will light green for one second and a one-second beep will sound to confirm reset to factory defaults.

ⓘ **If the mechanical key is not rotated within 10 seconds, two beeps and two red blinks indicate timeout.**

Level 2 factory default reset

ⓘ **Level 2 factory default reset will delete all configurations and settings in the lock and the reader.**

ⓘ **Reader configurations that will reset to factory default include: keypad format, magstripe reader track, beeper on/off, and contactless card.**

ⓘ **Days in Use counter and lock type configurations will not reset.**

To complete Level 2 factory default reset, repeat steps 2 through 4 **within 10 seconds of the confirmation signals of level 1 factory default reset.**

If more than 10 seconds pass after the confirmation signals of level 1 reset, then level 1 reset must be repeated prior to performing level 2 reset.

Batteries

Battery voltage can be checked with the SUS. Changing batteries does not affect any programmed data.

To install or replace alkaline batteries:

1. Remove the battery cover.
2. Remove the battery bracket. **Do not allow the battery pack to hang from the wires.**
3. Install the new batteries (install only new AA Alkaline batteries). Make sure the batteries are installed in the correct orientation.
4. Reinstall the battery pack and battery bracket.
5. Reinstall the battery cover, making sure the plug is to the right of the battery pack (CY, MS and MD locks). **Be careful not to pinch the battery wires when installing the battery cover.**

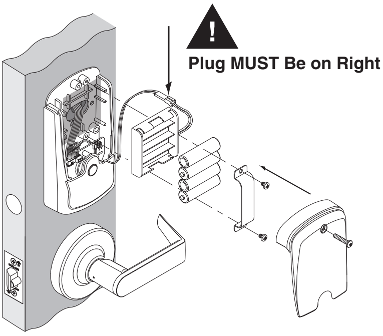
ⓘ **For coin cell battery installation or replacement, refer to instructions at www.allegion.com/us.**

CAUTION! Danger of explosion if batteries are incorrectly replaced! Replace only with the same or equivalent type. Dispose of used batteries according to the manufacturer's instructions.

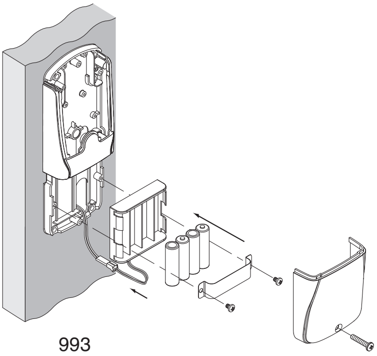
This product has been evaluated for ULC-S319 compliance with AA and coin cell batteries listed below. For installations requiring ULC-S319, these battery models should be used.

AA batteries: Duracell PC1500, MN1500; Energizer E91, EN91, AX91, XR91;
RayoVac 815, 815-HE

Coin cell batteries: Energizer CR2025, CR2032; Maxell CR2025, CR2032,
Panasonic CR2025, CR2032; RayoVac KECR2025, KECR2032.



CY, MS, & MD



993

Low battery indications

Condition	Indicator	Solution
Batteries low	After credential is presented– 9 red blinks of Schlage button (Left = AA batteries Right = Coin Cell battery) then normal indicator	Replace batteries immediately to avoid battery failure. Lock is intended to operate for 500 cycles in low battery condition.
Battery Failure (configured by SUS)	No LED or beeps and valid credentials do not grant access	Replace batteries immediately. Mechanical override key must be used to unlock the lock.

Battery failure modes

ⓘ **The battery failure mode is set using the SUS. See the SUS user guide for more information.**

Mode	Description
Fail As-Is (default)	Lock remains in current state until batteries are replaced.
Fail Unlocked	Lock unlocks and remains unlocked until batteries are replaced.
Fail Locked	Lock locks and remains locked until batteries are replaced.

LED reference

Most LED indicators are configured with the SUS. See SUS user guide for more information.

Schlage button

Condition	Lights
Access denied	2 red blinks
Access denied, user outside time zone	4 red blinks
Factory default reset	One-second solid green with one-second beep
Waiting for PIN	5 left red with right green blinks, then solid right green
Low battery indicator, AA batteries	9 left red blinks
Low battery indicator, coin cell battery	9 right red blinks
Momentary unsecured access	1 green blink, then one red blink on relock
USB active with no physical connection	Left green blinking
An incompatible reader is on the lock	2 red blinks and 2 beeps with each card or key press, or 5 red blinks and 5 beeps on power-up

Optional Inside Push Button (IPB)

Action	Lights
Office Mode –Allows lock to toggle between locked (normal) and unlocked state	
Press IPB to lock	1 red blink
Press IPB to unlock[1]	1 green blink
Privacy Mode – Allows the lock to toggle between normal access and a state in which normal credentials are ignored	
With door closed, press IPB to engage privacy[2]	4 green blinks
With door closed, press IPB to release privacy[3]	4 red blinks

[1] Unlocking the lock with the IPB will cause the lock to remain unlocked until the IPB is depressed again.

[2] On locks configured with a mortise-deadbolt, throwing the deadbolt will also engage privacy.

[3] If DPS is used, then opening door will also release privacy. If a mortise-deadbolt is used, then retracting the deadbolt will also release privacy.

Problem	Possible cause	Solution
The lock beeper does not sound and the keypad does not light when the Schlage button is pressed.	The beeper may be turned off. The battery or wired power may be improperly connected. The batteries may be inserted with incorrect polarity. The reader may not be properly seated into the front escutcheon. The reader connector may have bent pins. The through-door cable may not be properly plugged in.	Use manual programming or the SUS to enable the beeper (see *Disable/Enable Beeper* on page 12 or the SUS user guide for more information) Check that the battery or wired power is connected correctly. Check that the batteries are inserted in the correct polarity. Check that the reader is fully seated into the front escutcheon. Check that there are no bent pins in the reader connector. Check that the through-door cable is plugged in correctly. The red wire should be on the left and not pinched in the door. *Refer to the installation instructions that came with the CO-200 lock, or this user guide for details on the above mentioned procedures.*
The connection with the SUS is not successful.	The triangles on the outside lock assembly (cylindrical and mortise locks only) may not be properly aligned.	Check the outside lock assembly (cylindrical and mortise locks only). The triangles on the back of the lock assembly must be properly aligned. *Refer to the installation instructions that came with the CO-200 lock for details.*
The Schlage button is always on solid green.	The triangles on the outside lock assembly may not be properly aligned (cylindrical and mortise locks only).	Check the outside lock assembly (cylindrical and mortise locks only). The triangles on the back of the lock assembly must be properly aligned. *Refer to the installation instructions that came with the CO-200 lock*
The reader is not working. The Smart card is not reading. The magnetic swipe card is not reading correctly (no beeps or blinks).	The through door cable may be pinched. The Smart card default of the card reader may not be correct for the Smart card. The “Mag Track in Use” default for all magnetic card credential readers is “Track2”. The magnetic swipe card data may be on Track1 or Track3.	Check that the through door cable is not pinched. Change the Smart card format using the SUS. Select CO-200 “Lock Properties”, “Reader” tab, and “Smart cards in use”. Use the SUS to change “Mag Track in Use”. Select CO-200 “Lock Properties”, “Reader” tab, and “MAG Card Track selection”. *Refer to the installation instructions that came with the CO-200 lock, or the SUS user guide for details on the above mentioned procedures.*

Problem	Possible cause	Solution
The LEDs and beeper indicate an incompatible reader (2 red blinks and 2 beeps with each card or key press, or 5 red blinks and 5 beeps on power-up).	The reader is not the original reader matched with the lock at the factory.	The lock must be installed with the original reader that came with the lock.

FCC Statements

Allegion Agency Statements

Compliance Statement (Part 15.19)

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning (Part 15.21)

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Interference Statement (Part 15.105 (b))

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Statement

To comply with FCC/IC RF exposure requirements for mobile transmitting devices, this transmitter should only be used or installed at locations where there is at least 20 cm separation distance between the antenna and all persons.

Section 7.1.5 of RSS-GEN

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Customer Service

1-877-671-7011 www.allegion.com/us

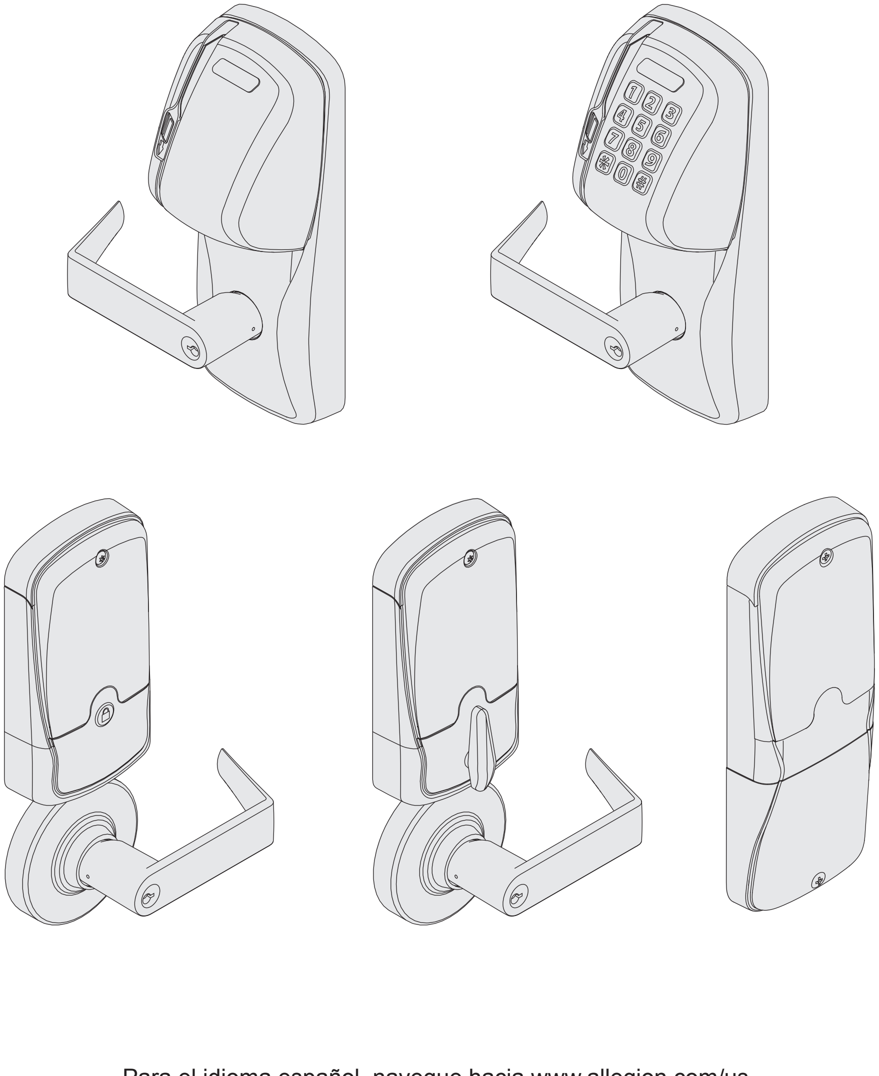
ALLEGION™

P516-272

CO-250

Offline lock user guide

Instructions for programming CO-Series offline locks



Para el idioma español, navegue hacia www.allegion.com/us.
Pour la portion française, veuillez consulter le site www.allegion.com/us.

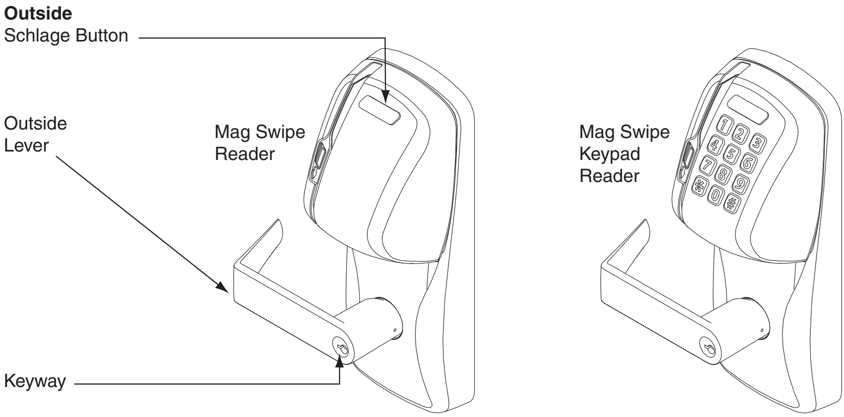
Contents

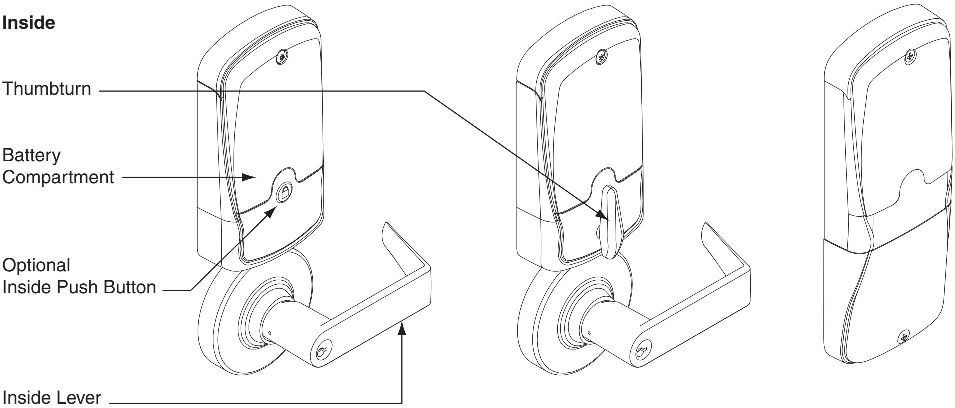
This product is compliant of UL 294 and ULC S319 standard. This product's compliance would be invalidated through the use of any add-on, expansion, memory or other module that has not yet been evaluated for compatibility for use with this UL Listed product, in accordance with the requirements of the Standards UL 294 and ULC S319. This product has been evaluated for ULC-S319 Class 1.

Overview

The Schlage CO-250 is an off-line electronic lock in the CO-Series product line.

- This product is listed for UL 294 and ULC S319.
- The lock is powered by four (4) AA batteries. See *Batteries* on page 9 for more information.
- Outside lever is normally locked.
- Inside lever always allows egress.
- The lock maintains an audit trail of events.
- The lock is configured using the Schlage Utility Software (SUS). See *Schlage Utility Software (SUS)* on page 4 for more information.





CO-250-CY
CO-250-MS

CO-250-MD

CO-250-993

Lock functions

The CO-250 is available in one of three functions:

Privacy (40): Lockset is normally secure. Pressing the Inside Push Button or extending the deadbolt will disable normal electronic access from the outside. Opening the door, retracting the deadbolt or pressing the Inside Push Button a second time deactivates the privacy status.

Office (50): Lockset is normally secure. Inside Push Button may be used to select passage or secured status.

Classroom/Storeroom (70): Lockset is normally secure. Valid toggle credentials may be used to change to a passage or secure status.

Getting started

Follow these steps when setting up a new lock.

1. Install the lock. See the installation guide that came with the lock or visit www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library) for more information.
2. Make sure the batteries are installed properly. See *Batteries* on page 9 for more information.
3. Configure the master construction credential (where applicable). See *Construction access mode* on page 5 for more information. The lock should remain in construction access mode until you are ready to set up the rest of the system.
4. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 7 for more information.
5. Consult the Schlage Utility Software (SUS) user guide for information about configuring the lock.
6. Familiarize yourself with the information contained in this user guide.

Save this user guide for future reference.

Schlage Utility Software (SUS)

The Schlage Utility Software is used for programming and setup only.

The Schlage Utility Software (SUS) is used to configure locks. The SUS configures lock functions that cannot be configured with manual programming, and is used to transfer data files between the access control software and locks.

For more information about the SUS, see the SUS user guide.

Construction access mode

Construction access mode is used to allow access before the lock has been programmed, and for testing purposes.

- Enabled by default.
- The lock will remain in construction access mode until the mode is cancelled as described below.
- No audits are captured while lock is in construction access mode.

Create the master construction credential - locks with card readers

1. Press and hold the Schlage button while presenting a credential, and is used to program construction access.
2. This credential becomes the master construction credential.
3. The Schlage button will blink green on the left and right as confirmation.

After you have created the master construction credential, you can then use that card to add construction access mode user credentials.

ⓘ **The master construction credential will not grant access. It is used only to add additional access credentials.**

TIPS

Use the same master construction credential for all the locks in the facility.

If you present the first card to a new lock to create the master construction credential and the card is not accepted, the lock has either been programmed or already has a master construction credential.

If the master construction credential cannot be located, or to put the lock back into construction access mode, reset the lock to factory settings. See *Reset to factory defaults* on page 8 for more information.

Locks with card readers – Add construction access mode user credentials

Construction access mode credential type	Steps to add construction access mode user credentials				
	1	2	3	4	5
Normal use construction credential Unlocks the lock for relock delay period	Present master construction credential to reader →	Green LEDs blink →	Present user credential within 20 seconds →	Green LEDs blink and credential is added →	Repeat steps 3 and 4 for additional credentials. Credentials added with the master construction credential will have 24/7 access.
Toggle construction credential Changes the state of lock from locked to unlocked or vice versa	Present master construction credential to reader →	Green LEDs blink →	Press and hold Schlage button while presenting user credential within 20 seconds →	Green LEDs blink, 2 beeps will sound and credential is added →	

Cancel construction access mode

Construction access mode may be cancelled by one of the following methods:

- load a door file using the SUS
- reset the lock to factory settings (see *Reset to factory defaults on page 8* for more information).

When construction mode is cancelled, the master construction credential and all other credentials added using the master construction credential will no longer function.

Locks with keypads

In the factory default reset state, offline locks with keypads, with or without additional credentials, have a default PIN of 13579 and “#”, which can be used for installation, testing and construction access. To test, enter 13579 and “#”. The Schlage button will blink and the lock will unlock. The default PIN is automatically deleted when a new programming credential is created, or the lock is programmed with the Schlage Utility Software (SUS).

Test lock operation

If you encounter problems while performing any of the following tests, review the installation guide and correct any problems.

Mechanical test

1. Rotate the inside lever or depress the push bar to open the door. Operation should be smooth, and the latch should retract.
2. Insert the key into the keyway and rotate the key and the outside lever to open the door. Operation should be smooth, and the latch should retract. The Schlage button will light solid green until the key is released and the latch is extended.

Test in factory default mode

1. For locks with a keypad, press any number key. The lock will beep and the Schlage button will blink red.
2. The Schlage button will blink red twice when a credential is presented and the lock is in factory default mode, and has no access programming.
3. For locks with keypads, enter the default PIN (13579 and "#") to verify access. The Schlage button will blink green, a beep will sound, and the door will unlock for the preset relock delay period. After the relock delay period, the lock will relock and the Schlage button will blink red. If the lever retracts and holds the latch through the relock delay period, then the Schlage button will light green until the lever is released.

Test in normal operation mode

1. Present a valid credential. The Schlage button will blink green, a beep will sound and the door will unlock for the preset lock delay period. The lock will re-lock after the relock delay period and the Schlage button will then blink red. If the lever retracts and holds the latch through the relock delay period, then the Schlage button will light green until the lever is released.
2. If an invalid credential is presented, the Schlage button will blink red, a beep will sound and the door will not unlock.

Normal lock operation

After the lock has been programmed, present credentials to operate the lock as follows:

Credential type	Action	
Credential	Present credential to reader ➔	Green blink and access granted
+ PIN credential	Present + PIN credential to reader ➔	Green blink and access granted

1 If the PIN is entered incorrectly, press "*" to start over.

Reset to factory defaults

All information in the lock will be deleted and reset to factory defaults!

The door must be locked (not toggled open or in the middle of normal access) before resetting to factory defaults.

Level 1 factory default reset

ⓘ **Level 1 factory default reset will delete configurations and settings in the main controller in the lock.**

ⓘ **Main controller configurations that will reset to factory default include: programming and user codes.**

ⓘ **Level 1 factory default reset will not reset configurations and settings in the reader.**

1. Press and hold the Schlage button. Wait for the lock to beep twice and two green blinks of the Schlage button, indicating confirmation.
2. After confirmation signals, release the Schlage button.
3. Rotate the mechanical key within 10 seconds and hold. The Schlage button will light green. Continue holding the key until confirmation signals are observed (the Schlage button light will turn off one second and a one second beep will sound). After confirmation signals, release the mechanical key.
4. The Schlage button will light green for one second and a one-second beep will sound to confirm reset to factory defaults.

ⓘ **If the mechanical key is not rotated within 10 seconds, two beeps and two red blinks indicate timeout.**

Level 2 factory default reset

ⓘ **Level 2 factory default reset will delete all configurations and settings in the lock and the reader.**

ⓘ **Reader configurations that will reset to factory default include: keypad format, magstripe reader track, beeper on/off, and contactless card.**

ⓘ **Days in Use counter and lock type configurations will not reset.**

To complete level 2 factory default reset, repeat steps 2 through 4 **within 10 seconds of the confirmation signals of level 1 factory default reset.**

If more than 10 seconds pass after the confirmation signals of level 1 reset, then level 1 reset must be repeated prior to performing level 2 reset.

Batteries

Battery voltage can be checked with the SUS. Changing batteries does not affect any programmed data.

To install or replace alkaline batteries:

1. Remove the battery cover.
2. Remove the battery bracket. **Do not allow the battery pack to hang from the wires.**
3. Install the new batteries (install only new AA Alkaline batteries). Make sure the batteries are installed in the correct orientation.
4. Reinstall the battery pack and battery bracket.
5. Reinstall the battery cover, making sure the plug is to the right of the battery pack (CY, MS and MD locks). Be careful not to pinch the battery wires when installing the battery cover.

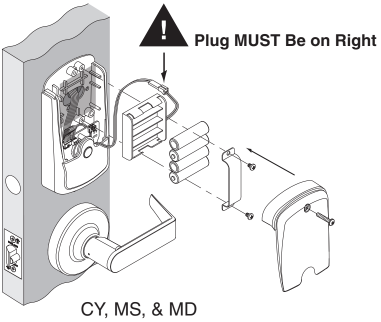
ⓘ **For coin cell battery installation or replacement, refer to instructions at www.allegion.com/us.**

CAUTION! Danger of explosion if batteries are incorrectly replaced! Replace only with the same or equivalent type. Dispose of used batteries according to the manufacturer's instructions.

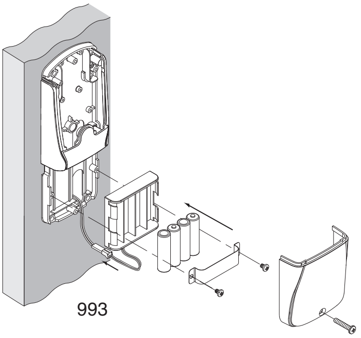
This product has been evaluated for ULC-S319 compliance with AA and coin cell batteries listed below. For installations requiring ULC-S319, these battery models should be used.

AA batteries: Duracell PC1500, MN1500; Energizer E91, EN91, AX91, XR91; RayoVac 815, 815-HE

Coin cell batteries: Energizer CR2025, CR2032; Maxell CR2025, CR2032, Panasonic CR2025, CR2032; RayoVac KECR2025, KECR2032.



CY, MS, & MD



993

Low battery indications

ⓘ **Replacement of batteries does not affect programmed data. Battery voltage can be checked with the SUS.**

Condition	Indicator	Solution
Batteries low	After credential is presented, 9 red blinks of Schlage button (Left = AA batteries, Right = coin cell battery), then normal indicator.	Replace batteries immediately to avoid battery failure. Lock is intended to operate for 500 cycles in low battery condition.
Battery failure (configured by SUS)	No LED or beeps Valid credentials do not grant access	Replace batteries immediately. Mechanical override key must be used to unlock the lock.

Battery failure modes

ⓘ **The battery failure mode is set using the SUS. See the SUS user guide for more information.**

Mode	Description
Fail As-Is (default)	Lock remains in current state until batteries are replaced.
Fail Unlocked	Lock unlocks and remains unlocked until batteries are replaced.
Fail Locked	Lock locks and remains locked until batteries are replaced.

LED reference

Most LED and beep indicators are configured using the SUS. See the Schlage Utility Software (SUS) user guide for more information.

Schlage button

Condition	Lights
Access denied	2 red blinks
Access denied, user outside time zone	4 red blinks
Factory default reset	One-second solid green with one-second beep
Low battery indicator, AA batteries	9 left red blinks
Low battery indicator, coin cell	9 right red blinks
Momentary unsecured access	1 green blink, then one red blink on relock
Toggle unsecured	2 green blinks
Toggle secure (relocking)	1 red blink
SUS authentication	Left green solid
USB active with no physical connection	Left green blinking
Waiting for PIN (Card + PIN)	5 left red with right green blinks then solid right green.
An incompatible reader is on the lock	2 red blinks and 2 beeps with each card or key press, or 5 red blinks and 5 beeps on power-up

Optional Inside Push Button (IPB)

Action	Lights
Office Mode –Allows lock to toggle between locked (normal) and unlocked state	
Press IPB to lock	1 red blink
Press IPB to unlock[1]	1 green blink
Privacy Mode – Allows the lock to toggle between normal access and a state in which normal credentials are ignored	
With door closed, press IPB to engage privacy[2]	4 green blinks
With door closed, press IPB to release privacy[3]	4 red blinks

[1] Unlocking the lock with the IPB will cause the lock to remain unlocked until the IPB is depressed again.

[2] On locks configured with a mortise-deadbolt, throwing the deadbolt will also engage privacy.

[3] If DPS is used, then opening door will also release privacy. If a mortise-deadbolt is used, then retracting the deadbolt will also release privacy.

Troubleshooting

Problem	Possible cause	Solution
The lock beeper does not sound and the keypad does not light when the Schlage button is pressed.	The reader may not be properly seated into the front escutcheon. The reader connector may have bent pins. The through door ribbon cable may not be properly plugged in. The battery or wired power may be improperly connected. The batteries may be inserted with incorrect polarity.	Check that the reader is fully seated into the front escutcheon. Check that there are no bent pins in the reader connector. Check that the through door ribbon cable is plugged in correctly. The red wire should be on the left and not pinched in the door. Check that the battery or wired power is connected correctly. Check that the batteries are inserted in the correct polarity. *Refer to the installation instructions that came with the CO-250 lock, or this user guide for details on the above mentioned procedures.*
The connection with the SUS is not successful.	The triangles on the outside lock assembly (cylindrical and mortise locks only) may not be properly aligned.	Check the outside lock assembly (cylindrical and mortise locks only). The triangles on the back of the lock assembly must be properly aligned. *Refer to the installation instructions that came with the CO-250 lock for details.*
The reader is not working. The Smart card is not reading. The magnetic swipe card is not reading correctly (no beeps or blinks).	The through door ribbon cable may be pinched. The Smart card default of the card reader may not be correct for the Smart card. The "Mag Track in Use" default for all Magnetic Card Credential Readers is "Track2". The magnetic swipe card data may be on Track1 or Track3.	Check that the through hole ribbon cable is not pinched. Change the Smart card format using the SUS. Select CO-250 "Lock Properties", "Reader" tab, and "Smart cards in use". Use the SUS to change "Mag Track in Use". Select CO-250 "Lock Properties", "Reader" tab, and "MAG Card Track selection". *Refer to the installation instructions that came with the CO-250 lock, or the SUS user guide for details on the above mentioned procedures.*
The LEDs and beeper indicate an incompatible reader (2 red blinks and 2 beeps with each card or key press, or 5 red blinks and 5 beeps on power-up).	The reader is not the original reader matched with the lock at the factory.	The lock must be installed with the original reader that came with the lock.

FCC statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Customer Service

1-877-671-7011 www.allegion.com/us

ALLEGION™

ALLEGION™

SCHLAGE®

Schlage Utility Software

For Pidion BM-150 / BM-170 Devices
User's Guide

Important Information

Customer Service

U.S.A.: 877-671-7011

www.schlage.com/support

Copyright

Revision

This document has been updated for SUS Rev 6.5.3.

Check **www.schlage.com/support** for latest SUS revisions.

Warranty

LIMITED WARRANTY: COMMERCIAL APPLICATIONS

12 Month Limited Warranty

Schlage Lock Company (the “Company”) extends a 12 month limited warranty from the original date of purchase to the Original User of the products manufactured by the Company (the “Product”) against defects in material and workmanship. Certain Products contain restrictions to this limited warranty, additional warranties or different warranty periods. Please see below for specific Product warranty information.

The provisions of this warranty do not apply to Products: (i) used for purposes for which they are not designed or intended; (ii) which have been subjected to alteration, abuse, misuse, negligence or accident; (iii) which have been improperly stored, installed, maintained or operated; (iv) which have been used in violation of written instructions provided by Schlage; (v) which have been subjected to improper temperature, humidity or other environmental conditions (i.e., corrosion); or (vi) which, based on Schlage’s examination, do not disclose to Schlage’s satisfaction non-conformance to the warranty. Additionally, Schlage will not warrant ANSI A156.2 Grade 2 lever Product installed in educational facilities and student housing.

Small Format Interchangeable Core (SFIC) Warranty: This limited warranty also applies to Schlage locks and housings when used with another manufacturer’s cores, or to Schlage cores (i.e. SFIC) when used in another manufacturer’s locks and housings. The use of unauthorized cylinder cams or other components with the Products shall void this warranty.

Everest® Primus® Limited Lifetime Key Breakage Warranty: A limited lifetime warranty is provided to the Original User against key breakage, subject to the restrictions of this limited warranty.

AD-Series 1-Year Warranty for electronic locks, reader modules, PIM400, and PIB300: A limited warranty is provided to the Original User for one (1) year from the date of installation, not to exceed 24 months from date of shipment from the factory, subject to the restrictions of this limited warranty.

CO-Series 1-Year Warranty for electronic locks, reader modules: A limited warranty is provided to the Original User for one (1) year from the date of installation, not to exceed 24 months from date of shipment from the factory, subject to the restrictions of this limited warranty.

ADDITIONAL TERMS & CONDITIONS APPLYING TO COMMERCIAL APPLICATIONS OF COMMERCIAL PRODUCTS

What the Company Will Do: Upon return of the defective Product to the Company, the Company’s sole obligation, at its option, is to either repair or replace the Product, or refund the original purchase price in exchange for the Product.

Original User: This warranty only applies to the Original User of Products. This warranty is not transferable.

What is Not Covered: The following costs, expenses and damages are not covered by the provisions of this limited warranty: (i) labor costs including, but not limited to, such costs as the removal and reinstallation of Products; (ii) shipping and freight expenses required to return Products to Schlage; and (iii) any other incidental, consequential, indirect, special and/or punitive damages, whether based on contract, warranty, tort (including, but not limited to, strict liability or negligence), patent infringement, or otherwise, even if advised of the possibility of such damages. Some local laws do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.

How Local Law Applies: This warranty gives you specific legal rights, and you may also have other rights as otherwise permitted by law. If this Product is considered a consumer product, please be advised that some local laws do not allow limitations on incidental or consequential damages or how long an implied warranty lasts, so that the above limitations may not fully apply. Refer to your local laws for your specific rights under this warranty.

Warranty Claims: If you have a claim under this warranty, please contact Schlage Customer Service (877-671-7011) for repair, replacement or refund of the original purchase price in exchange for the return of the Product to Schlage.

Miscellaneous: The Company does not authorize any person to create for it any obligation or liability in connection with the Product. The Company’s maximum liability hereunder is limited to the original purchase price of the Product. No action arising out of any claimed breach of this warranty by the Company may be brought by the Original User more than one (1) year after the cause of action has arisen.

Contents

Overview

The Schlage Utility Software is an application that runs on the Schlage Handheld Device (HHD). It is used to configure, edit and program all supported devices.

Supported Devices

Locks and Controllers		HHD Model Compatiblity	
		BM-150	BM-170
AD-Series Locks	AD-200	▪	▪
	AD-201	▪	▪
	AD-250	▪	▪
	AD-300	▪	▪
	AD-301	▪	▪
	AD-400	▪	▪
	AD-401	▪	▪
CO-Series Locks	CO-200	▪	▪
	CO-220	▪	▪
	CO-250	▪	▪
Legacy Locks	KC2-5100	▪	▪
	KC2-5500	▪	▪
	KC2-9000	▪	▪
	CM5100	▪	▪
	CM5500	▪	▪
	CM5200	▪	▪
	CM5600	▪	▪
	CM5700	▪	▪
	CM993	▪	▪
	CL5100	▪	▪
	CL5500	▪	▪
	CL5200	▪	▪
	CL5600	▪	▪
	CL993	▪	▪
	BE367	▪	▪

Locks and Controllers			HHD Model Compatiblity	
			BM-150	BM-170
AD-Series and Legacy Controllers	PIM400		▪	▪
	WRI400		▪	▪
	WPR400		▪	▪
	PIB300		▪	▪
	CT5000 Controller		▪	▪
	CT500 Controller		▪	▪
	CT1000 Controller		▪	▪
	Legacy PIM	WRI[1]	▪	▪
		WPR[1]	▪	▪
		WPR2[1]	▪	▪
		WSM[1]	▪	▪
	CL Campus Lock Controller		▪	▪

[1] These devices cannot be configured directly. They are configured through the legacy PIM.

SUS Functions by Device

AD-Series Devices	AD-200[2]	AD-250	AD-300[2]	AD-400[1,2]	CT5000	PIB300	PIM400	WPR400[1]	WRI400[1]
Collect Audits	•	•			•				
Edit Lock Properties	•	•	•	•	•				
Edit PIB300 properties						•			
Edit PIM400 properties							•		
Edit Door Properties				•			•	•	•
Update Firmware	•	•	•	•	•	•	•	•	•
Couple HHD to Device	•	•	•	•	•	•	•	•	•
Set Date/Time	•	•	•	•	•				•
Diagnostics							•		
Change Lock Class	•	•	•	•	•			•	•

[1] AD-Series wireless device properties may also be viewed or edited through the PIM400.

[2] These devices work with the FIPS201 standard and will become AD-201, AD-301, and AD-401 when a FMK reader is attached.

CO-Series Devices	CO-200	CO-220	CO-250
Collect Audits	•	•	•
Edit Lock Properties	•	•	•
Update Firmware	•	•	•
Couple HHD to Device	•	•	•
Set Date/Time	•	•	•

Legacy Devices	KC2	CM	CL	BE367	CT500/1000	CL Controller	Legacy PIM	WA[1]	WPR2[1]	WSM[1]	WRI[1]
Collect Audits	•	•	•	•	•	•					
Edit Lock Properties	•	•	•	•	•	•					
Update Firmware Update	•	•	•	•	•	•	•				
Edit Legacy PIM properties							•				
Edit WAPM Properties							•	•	•	•	•
Diagnostics							•				

[1] Legacy wireless access point devices cannot be configured directly. They are configured through the legacy PIM.

Getting Started

The Schlage Utility Software (SUS) is a software application that runs on a Windows CE based handheld device. It is used to transfer data files between the access control software and locks and controllers.

Quick Start

To begin using the SUS, review the following topics:

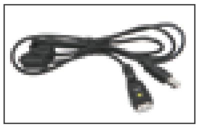
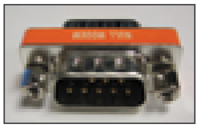
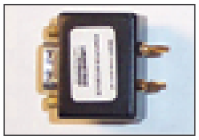
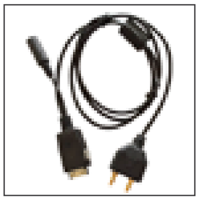
1. Download and Install Synchronization Software **(page 9)**
2. Connect the HHD to your PC **(page 13)**
3. Configure the Synchronization Software **(page 10)**
4. Update SUS **(page 13)**
5. Start SUS **(page 15)**
6. Connectng the Handheld Device to a Lock or Non-Lock Device **(page 20)**

Handheld Devices

BM-150 HHD

BM-170 HHD

System Components

ID	BM-150	BM-170	Description
HHD KIT	▪	▪	Handheld Device pre-loaded with SUS, USB Cable
HH-USB 	▪	▪	Cable used to connect HHD to AD- and CO-Series products.
HH-Serial 	▪	n/a	Cable used to connect HHD to CIP for programming legacy CM/CL/KC products.
	▪	▪	Cable used to connect HHD to Null converter for programming WA Series Legacy PIM.
PIMWA-CV 	▪	▪	Null converter used to connect HHD to WA Series Legacy PIM, using the HH-Serial Cable.
CIP (P512-112) 	▪	n/a	CIP Module used with HH-Serial Cable for programming legacy CM/CL/KC products.
HH-2PIN Serial Black 	▪	▪	Cable used to connect HHD for programming legacy CM/CL/KC products. Must have SUS 6.3.3 in HHD to support the HH-2PIN Serial cable.
HH-2PIN Serial Gray 	▪	▪	Cable used to connect HHD for programming legacy BE367/FE210 products. Must have SUS 6.5.3 in HHD to support the HH-2PIN Serial cable.

Synchronization Software

About Synchronization Software

Synchronization software is software that your computer uses to interface and synchronize with the handheld device. This software is used to install and update software applications on your handheld device. When installed and configured properly, files will be automatically transferred between your computer and the handheld device when the handheld device is connected to the computer.

➔ This software may already be installed on your computer.

Download and Install Synchronization Software

1. Download the software that matches your operating system.
   - Windows 10, Windows 8, Windows 7 and Windows Vista:
     - 32 Bit: **http://www.microsoft.com/en-us/download/details.aspx?id=14**
     - 64 Bit: **http://www.microsoft.com/en-us/download/details.aspx?id=3182**
   - Windows XP and Windows 2000:
     - 32 and 64 Bit: **http://www.microsoft.com/en-us/download/details.aspx?id=15**
2. Launch the installer and follow the on-screen instructions.

Configure Synchronization Software

Microsoft ActiveSync

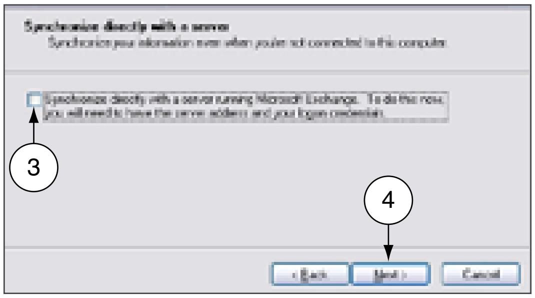
Microsoft ActiveSync is for use with Windows XP and Windows 2000 operating systems.

1 Connect the handheld device to the computer's USB port. The **Synchronization Setup Wizard** will appear.

2 Click the **Next** button.

3 Uncheck the check box next to **Synchronize directly with a server**.

4 Click the **Next** button.

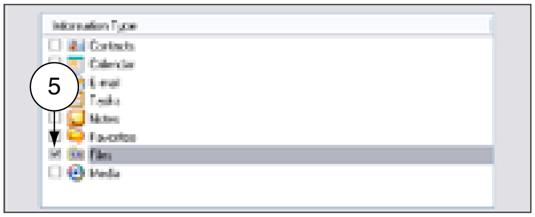


Synchronize directly with a server

Synchronize your information even when you're not connected to this computer.

☐ Synchronize directly with a server running Microsoft Exchange. To do this now, you will need to have the server address and your logon credentials.

5 Uncheck all the check boxes except for the check box next to **Files**.

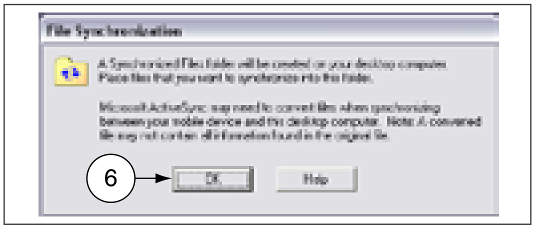


Information Type

☐ Contacts
☐ Calendar
☐ E-mail
☐ Tasks
☐ Notes
☐ Favorites
☑ Files
☐ Media

A new folder will be created on the computer to store the synchronized files.

6 The **File Synchronization** window will appear. Click **OK**.

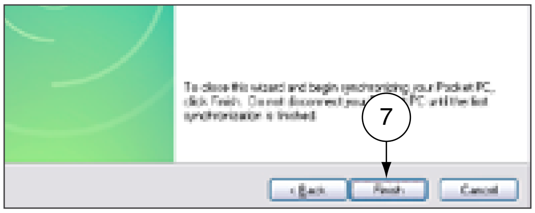


File Synchronization

A Synchronized Files folder will be created on your desktop computer. Place files that you want to synchronize into this folder.

Microsoft ActiveSync may need to convert files when synchronizing between your mobile device and this desktop computer. Note: A converted file may not contain all information found in the original file.

7 Click the **Finish** button.



To close this wizard and begin synchronizing your Pocket PC, click Finish. Do not disconnect you PC until the first synchronization is finished.

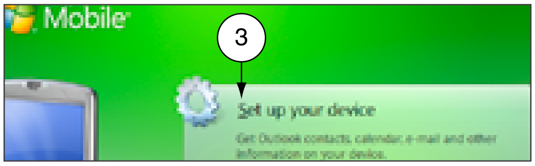
Microsoft Windows Mobile Device Center is for use with Windows 10, Windows 8, Windows 7 and Windows Vista operating systems.

Microsoft Windows Mobile Device Center

1 Open the Windows Mobile Device Center from the computer.

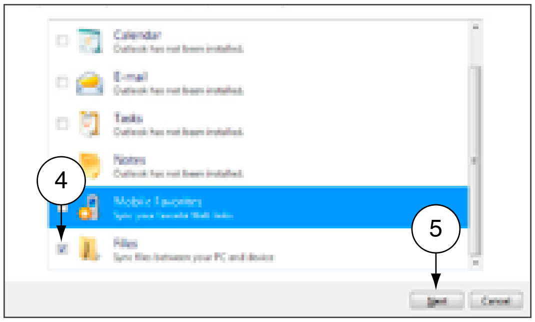
2 Connect the handheld device to your computer's USB port.

3 Click **Setup your device**.


Mobile
3
Set up your device
Get Outlook contacts, calendar, e-mail and other information on your device.

4 Click to uncheck all check boxes except for the **Files** check box.

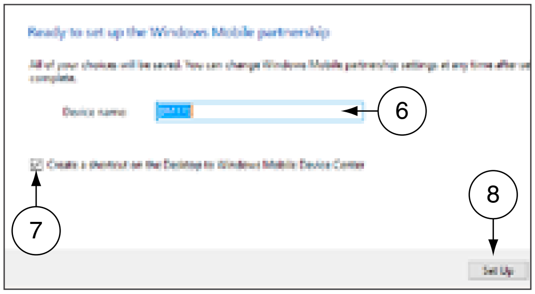
5 Click the **Next** button.


□ Calendar
Outlook has not been installed.
□ E-mail
Outlook has not been installed.
□ Tasks
Outlook has not been installed.
Notes
Outlook has not been installed.
Mobile Favorites
Sync your favorite Web links
☑ Files
Sync files between your PC and device
4
5
Next
Cancel

6 Type a name for the device in the **Device name** box.

7 Check the **Create a shortcut on the Desktop...** checkbox.

8 Click the **Set Up** button.


Ready to set up the Windows Mobile partnership

All of your choices will be saved. You can change Windows Mobile partnership settings at any time after se complete.

Device name:
6
☑ Create a shortcut on the Desktop to Windows Mobile Device Center
7
8
Set Up

Synchronization software must be installed so that the handheld device can communicate with the computer. See **Synchronization Software** on page **9** for more information.

Locate the Synchronization Folder

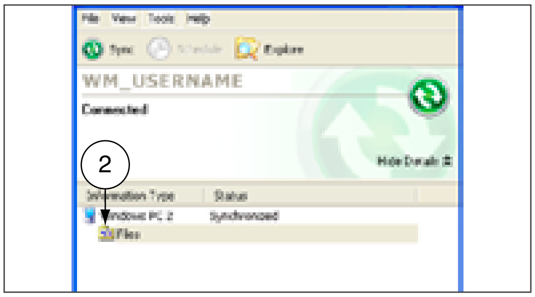
The synchronization software looks in this folder for files that should be synchronized with the handheld device. When you configure your access control software, you need to know the location of this file on your computer.

Microsoft ActiveSync

1 Connect the HHD to the PC and allow ActiveSync to start.

- ➔ If Microsoft ActiveSync does not open automaticaly, click on **Start** > **Programs** > **Microsoft ActiveSync**.

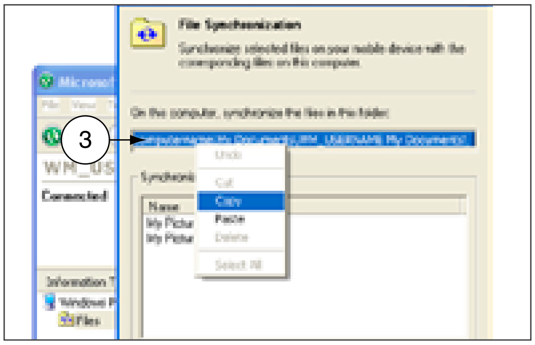
2 In the bottom half of the ActiveSync screen, double click on the **Files** folder.



3 Look for the box, under the text **On this computer, synchronize the files in this folder:**. This box contains the path to the synchronization folder.

- ➔ This path may extend beyond the edges of the box. Make sure to view the entire path.

4 To ensure the path is entered into the access control software correctly, highlight the path and then copy (Ctrl + C) and paste (Ctrl + V) it into the access control software.


File Synchronization

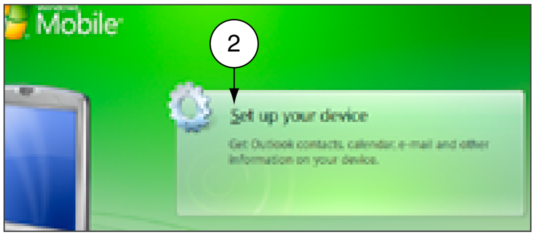
Synchronize selected files on your mobile device with the corresponding files on this computer.

On this computer, synchronize the files in this folder:

Microsoft Windows Mobile Device Center

1 If Microsoft Windows Mobile Device is not already open, click on **Start > Programs > Microsoft Windows Mobile Device Center**.

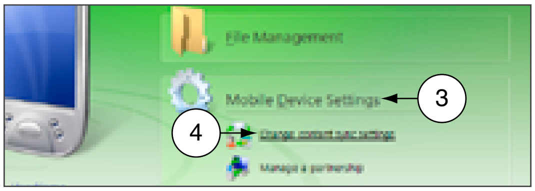
2 Click **Set up your device**.



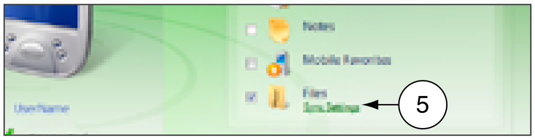
Get Outlook contacts, calendar, e-mail and other information on your device.

3 Click **Mobile Device Settings**.

4 Click **Change content sync settings**.

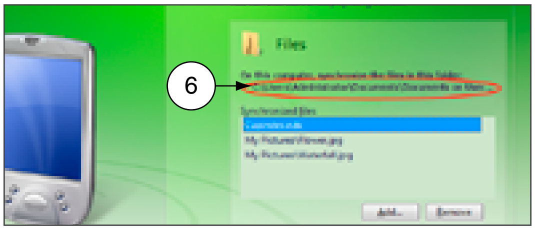


5 Click **Sync Settings**.



6 The sync folder path is located below the **Files** icon.

7 To ensure the path is entered into the access control software correctly, highlight the path and then copy (Ctrl + C) and paste (Ctrl + V) it into the access control software.



On this computer, synchronize the files in this folder:

C:\Users\Administrator\Documents\Documents on Mem...

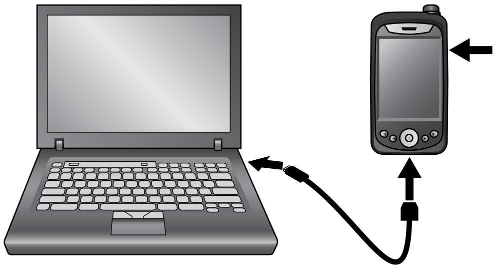
Connect the Handheld Device to the PC

If the HHD does not automatically synchronize with the PC, be sure that the SUS application is not running. The SUS will prevent USB communication with your PC.

1 Locate the HH-USB cable that came in the box with the handheld device. Insert the USB end into the computer's USB port.

2 Power on the handheld device.

3 Insert the other end of the cable into the bottom of the handheld device.



Connecting the Handheld Device to the PC

Install/Update Schlage Utility Software

Although SUS is already installed on your handheld device, you should make sure you have the latest revision of the software.

Synchronization software must be installed and configured on your computer in order for these steps to work properly. See **Download and Install Synchronization Software** on page **9** for more information.

1 Download the installer (Schlage Utility Setup Ver x.x.xx.exe, version will vary) from **www.schlage.com/support**.

2 Make sure you have already installed and configured the synchronization software.

3 Make sure the handheld device is connected to the computer's USB port and is turned on.

4 Launch the installer.

5 Follow the on-screen instructions. The synchronization software will automatically transfer the software to the handheld device.

6 When updating Schlage Utility Software all passwords are reset to their defaults.

➔ See **Appendix A: SUS Update Guide** on page **75** for detailed instructions about upgrading the Schlage Utility Software on the Handheld Device.

Icon Definitions

🔒	Lock
📟	Non-Lock Device
✗	New lock data file has not been updated
✓	Lock update completed
ℹ	Information
⚠	Warning
⊗	Error
🔄	Information is being exchanged with the device
Ⓟ	Firmware Package

Logging In

You can log in to the Schlage Utility Software (SUS) as either a Manager or an Operator. The Manager role has access to all commands. The Operator role has access only to limited commands.

	Manager	**Operator**
Lock Properties	·	·
Program Lock	·	·
Firmware Update	·	
Change Lock Class	·	
Couple HHD to Device	·	
Set Date/Time	·	
Diagnostic Data Log	·	·
Door Properties	·	·
PIM properties	·	·
Diagnostics	·	
SUS Password	·	·
Coupling Password	·	
Language	·	·
Auto/Manual Update	·	·
List All/Pending Doors	·	·
USB/Serial Connection	·	·

Start the Schlage Utility Software

See **Log in as a Manager on page 16** or **Log in as an Operator on page 16** for more information.

1 On your handheld device, tap the **Start** menu.

2 Tap **Programs**.

3 Tap the **Schlage Utility Software** icon.

4 Log on as either a Manager or an Operator.

5 If you are starting the SUS for the first time, change the Manager and Operator passwords, and the Coupling Password, to maintain security.

- ➔ See **SUS Password** on page **18** for more information.
- ➔ See **Coupling Password** on page **18** for more information.

The default password for both the Manager and Operator is 123456.

If the password is lost, you must reinstall SUS. Customer service cannot retrieve a lost password.

Log in as a Manager

1. If you have not already started the Schlage Utility Software, do so now.
   ➔ See **Start the Schlage Utility Software** on page **15** for more information.
2. Choose **Manager** from the drop-down list.
3. Enter the manager password in the password box.
4. Select the **Login** button.
   ➔ See **SUS Password** on page **18** for more information.

Log in as an Operator

1. If you have not already started the Schlage Utility Software, do so now.
   ➔ **See Start the Schlage Utility Software on page 15 for more information.**
2. Choose **Operator** from the drop-down list.
3. Enter the operator password in the password box.
4. Select the **Login** button.
   ➔ See **SUS Password** on page **18** for more information.

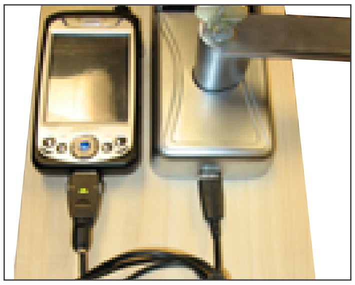
Schlage Utility Software Options

Connection Type

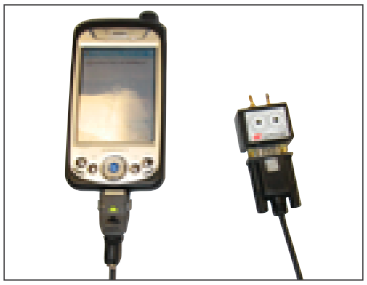
AD/CO-Series devices communicate with the SUS via USB connection. Legacy devices communicate with the SUS via Serial connection. Select this option to match the device type to which you are connecting. If you have both types of devices in your facility, you will need to change this setting during a tour.

1. Select **SUS Options**.
2. Select **Connection Type**.
3. Select **USB Connection** or **Serial Connection**.

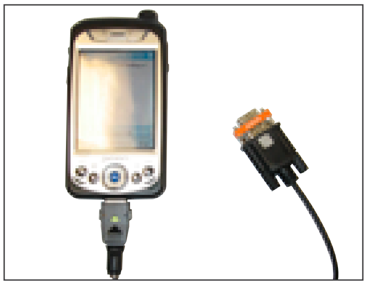
Connection Examples



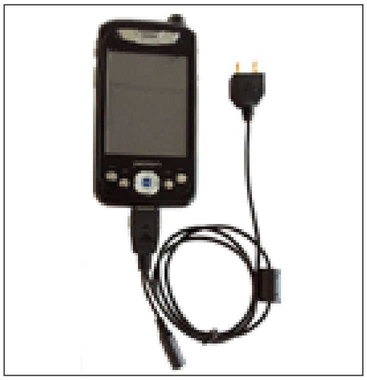
USB Connection with BM-150



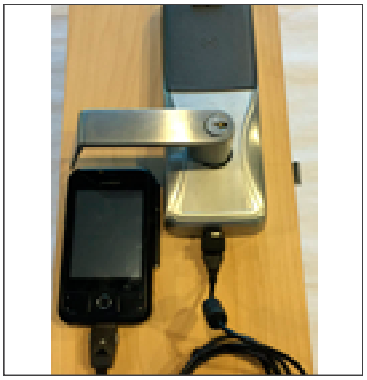
Serial Communication with CIP (BM-150 only)



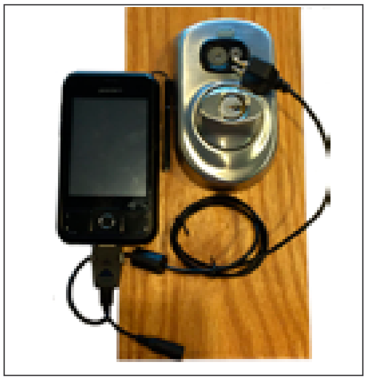
Serial Communication with Null Modem (PIMWA-CV) (BM-150)



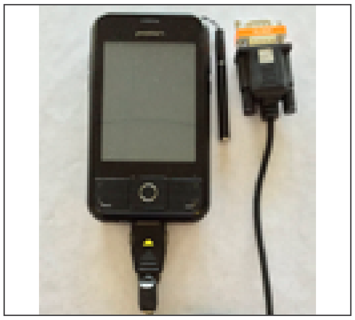
Serial Communication with 2PIN Serial Cable (BM-150)



USB Connection with BM-170



Serial Communication with 2PIN Serial Cable (BM-170)



Serial Communication with Null Modem (PIMWA-CV) (BM-170)

Door List

If you want to display only the doors that need to be toured, set this setting to **List Pending Doors**.

Select **List All Doors** to display all doors that have been updated and pending.

1. Select **SUS Options**.
2. Select **Door List**.
3. Select **List All Doors** or **List Pending Doors**.

Update Mode

When Auto Update is selected, the SUS will automatically set the date and time in the lock to which it is connected, retrieve the audit and program the lock. When Manual Update is selected, the functions must be independently performed by the user.

➔ Manual Update is recommended when managing Legacy Locks.

1. Select **SUS Options**.
2. Select **Update Mode**.
3. Select **Auto Update** or **Manual Update**.

SUS Password

You must be logged in to a role to change the password for that role.

1. Select **SUS Options**.
2. Select **SUS Password**.
3. Enter the old password into the **Old Password** box.
4. Enter the new password into the **New Password** box.

   ➔ The new password must be between four (4) and eight (8) characters long and can include capital and lowercase characters, numbers, and symbols.
5. Enter the new password again into the **Confirm New Password** box.
6. Select the **Submit** button.

Coupling Password

This function is available only when logged into the handheld device as a manager.

The default Coupling Password is 123456.

1. Select **SUS Options**.
2. Select **Coupling Password**.
3. Enter the old password into the **Old Password** box.
4. Enter the new password into the **New Password** box.

   ➔ The new password must be between four (4) and eight (8) characters long and can include capital and lowercase characters, numbers, and symbols.
5. Enter the new password again.
6. Select **Submit**.

Language

1. Select **SUS Options**.
2. Select **Language**.
3. Select the button for the language to which you want to change.
4. Select the **OK** button.

Device Template Feature

The Device Template feature facilitates creation, modification and duplication of Device Properties settings across multiple devices. In addition, the Device Template will also report additional device status parameters for a complete summary of the device's health.

Locating the Device Template Feature:

1. Select Device Options
2. Select Lock Properties for the connected device
3. Select the Edit or Reader tab
4. The Device Template is at the bottom of the screen

➔ For details on the Device Template feature, see **Appendix D: Device Template** on page **89**.

Diagnostic Data Log Feature

This new feature provides a simple method for AD-Series customers to quickly gather and save important lock-status information in a file.

➔ For details see **Appendix E: Diagnostic Data Log** on page **91**.

Connecting the HHD

Connecting the Handheld Device

The Schlage button will flash green while the lock is waiting to communicate with the HHD. The Schlage button will begin to flash red when communication between the lock the HHD is established.

When communication is established, the device name will be displayed on the SUS main screen.

AD-Series and CO-Series Locks

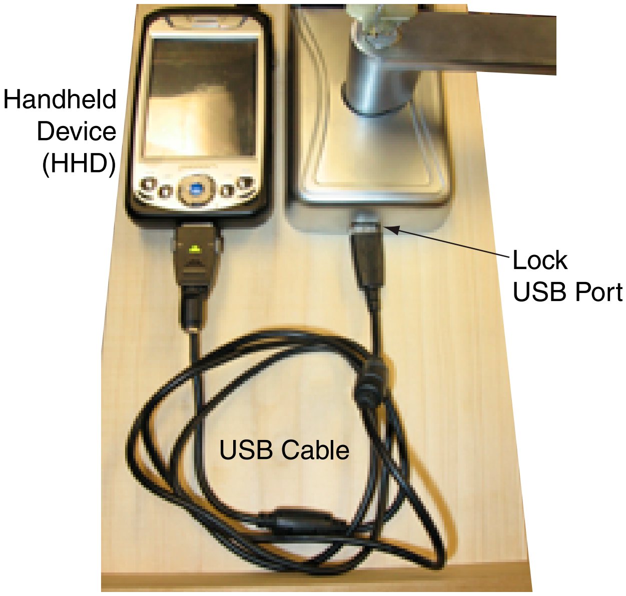
1 Start the Schlage Utility Software.

2 Make sure the HHD is in USB Connection Mode. See **Connection Type** on page **17** for more information.

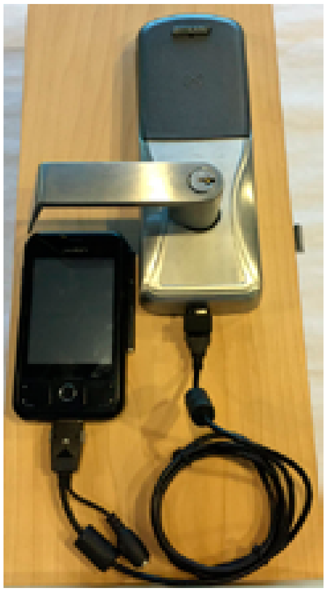
3 Connect the USB cable to the HHD.

4 Plug the HHD USB cable into the lock's USB port located in the bottom of the exterior housing.

5 Press the Schlage button twice.



BM-150



BM-170

When communication is established, the device name will be displayed on the SUS main screen.

AD-Series Controllers

1 Start the Schlage Utility Software.

2 Make sure the HHD is in USB Connection Mode. See **Connection Type** on page **17** for more information.

3 Connect the USB cable to the HHD.

4 Plug the HHD USB cable into the controllers's USB port. Communication will begin automatically

When communication is established, the device name will be displayed on the SUS main screen.

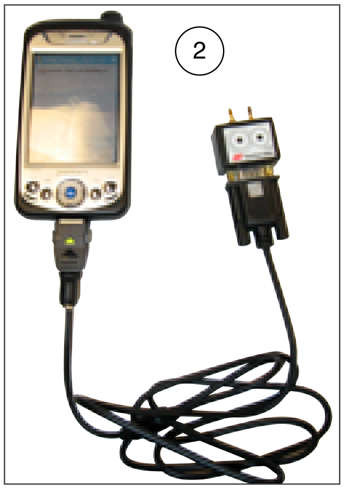
Legacy CM and CL Locks (BM-150 with Serial Cable and CIP ONLY)

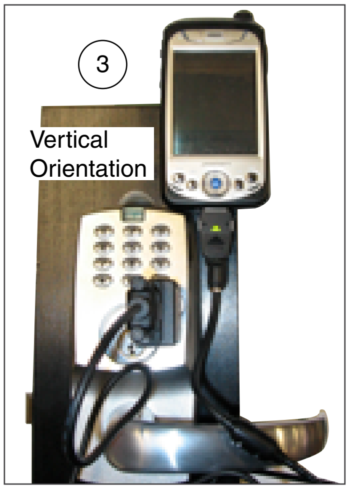
1 Start the Schlage Utility Software.

2 Make sure the HHD is in Serial Connection Mode. See **Connection Type** on page 17 for more information.

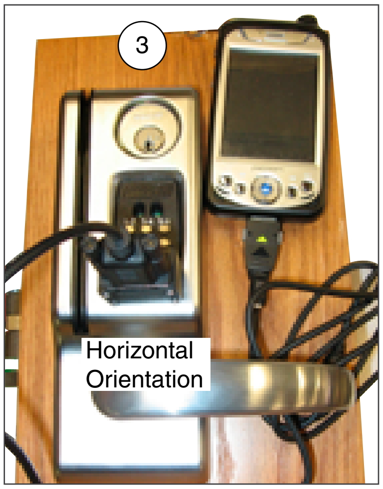
3 Connect the serial cable (HH-Serial) to the HHD and the CIP.

4 Connect the CIP to the legacy lock port.





OR

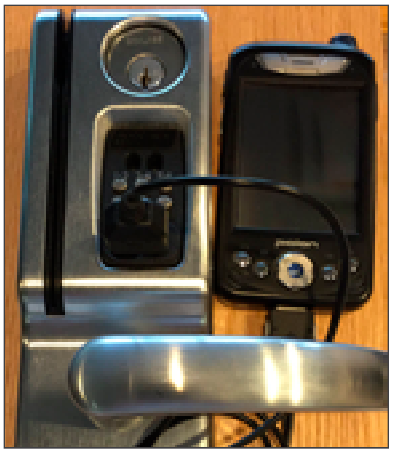


Legacy CM and CL Locks (BM-150 and BM-170 with 2PIN serial cable)

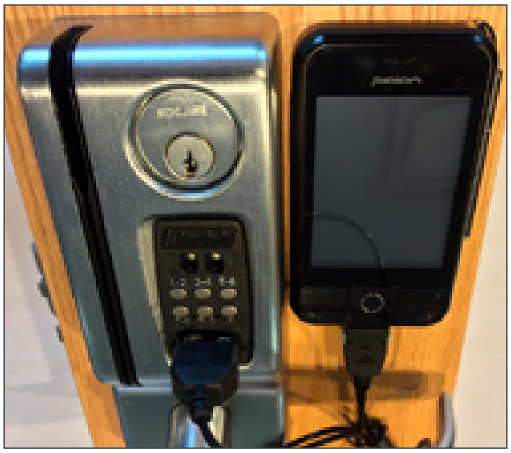
1 Start the Schlage Utility Software

2 Make sure the HHD is in Serial Connection Mode. See **Connection Type** on page 17 for more information.

3 Connect the 2PIN serial cable to the (HHD) and the Legacy lock port.



BM-150



BM-170

Legacy BE367 and FE210 Locks (BM-150 with Serial Cable and CIP ONLY)

1 Start the Schlage Utility Software.

2 Make sure the HHD is in Serial Connection Mode. See **Connection Type** on page **17** for more information.

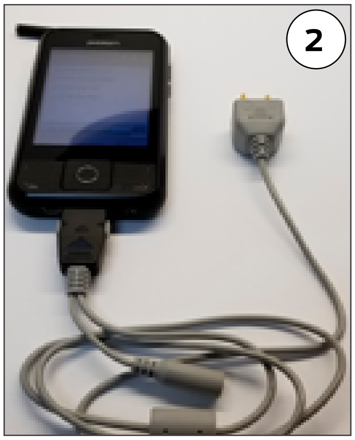
3 The deadbolt must be retracted if this is the first time programming the lock.

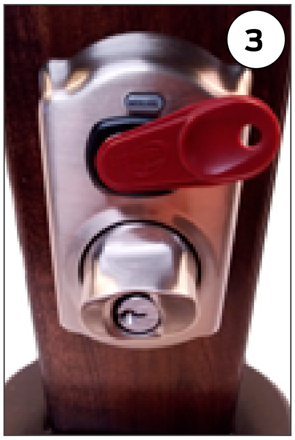
4 Connect the serial cable (HH-Serial) to the HHD and the CIP.

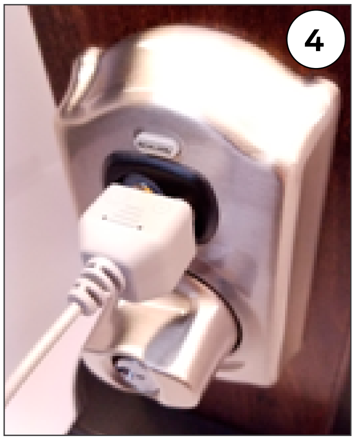
5 Present the red programming iButton to the lock.

6 Connect the CIP to the lock port.

➔ Rotate the thumbturn to the horizontal position, as shown, before connecting the CIP to the lock.







Legacy BE367 and FE210 (BM-150 and BM-170 with 2PIN serial cable)

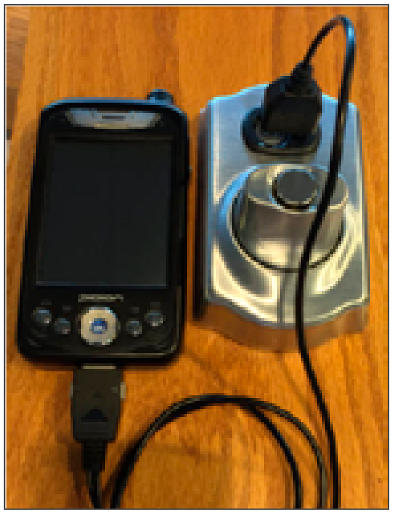
1 Start the Schlage Utility Software

2 Make sure the HHD is in Serial Connection Mode. See **Connection Type** on page **17** for more information.

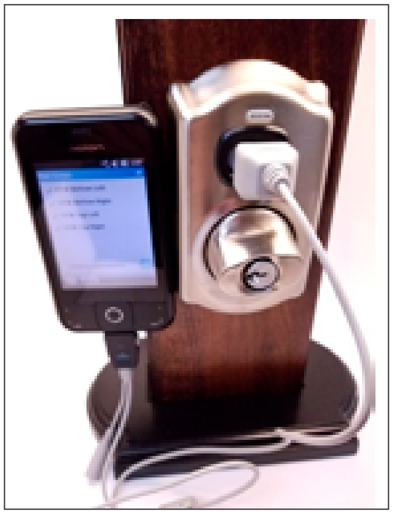
3 The deadbolt must be retracted if this is the first time programming the lock.

4 Present the Red programming iButton to the lock.

5 Connect the 2PIN serial cable to the (HHD) and the lock port.



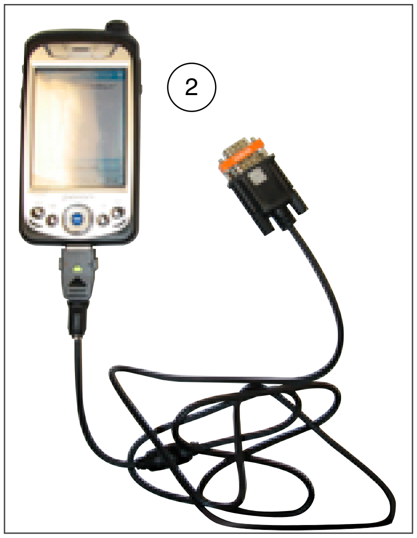
BM-150



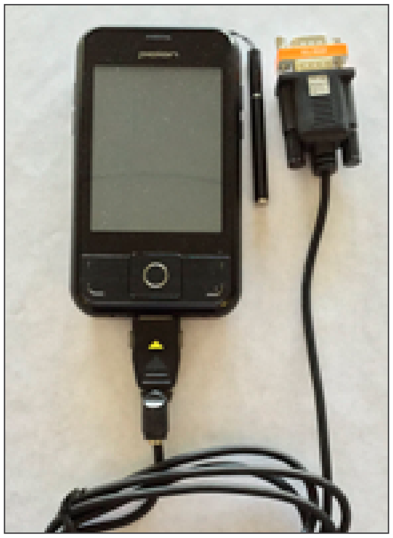
BM-170

Legacy PIM

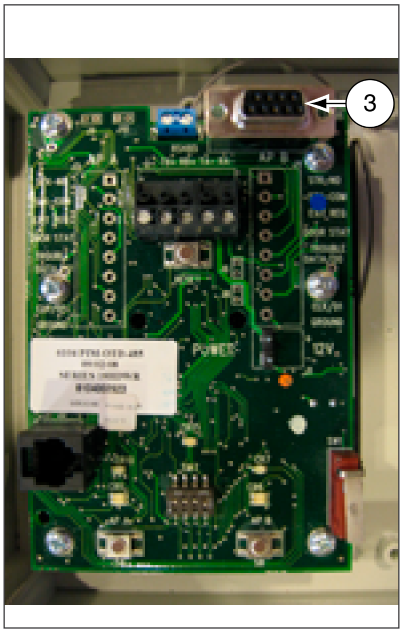
1. Start the Schlage Utility Software.
2. Make sure the HHD is in Serial Connection Mode. See **Connection Type** on page **17** for more information.
3. Connect the serial cable (HH-Serial) to the HHD and the null modem adapter (PIMWA-CV).
4. Connect the null modem adapter to the legacy PIM serial port.
5. Simultaneously press the RESET and the LINK A buttons on the Legacy PIM, then release the RESET button while holding the LINK A button.
6. Continue holding the LINK A button (at least 15 seconds) until communication is established and the device name is displayed on the SUS main screen.



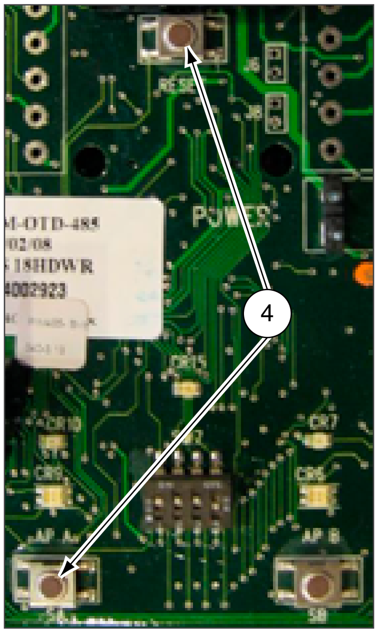
BM-150



BM-170



Legacy PIM



Legacy PIM

AD-Series Locks and Controllers

Supported Locks

All chassis for the following models are supported.

AD-Series Offline

AD-200
AD-201
AD-250

AD-Series Networked

AD-300
AD-301
AD-400
AD-401

Supported Controllers

PIM400 (Panel Interface Module)
WRI400 (Wireless Reader Interface)
WPR400 (Wireless Portable Reader)
PIB300 (Panel Interface Board)
CT5000 Controller

This function works with AD-Series devices only.

Couple HHD to Lock

AD-Series locks can be coupled, or authenticated, with the HHD. This provides enhanced security by ensuring that the lock will only communicate with HHD(s) to which it has been coupled. Once the lock has been coupled, the Coupling Password is passed to the device from the HHD during programming.

The HHD will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See **Coupling Password** on page **18** for more information.

If a device is not in Coupling mode, SUS will display a device specific message with instructions for placing the device into Coupling mode.

➔ HHDs with the same coupling password can program the same devices. Once the HHD and lock are coupled, the coupling password is disabled in the lock and any HHD with the correct coupling password will automatically couple with the lock.

1. Connect the HHD to the lock using the HH-USB cable.

   ➔ The HHD must be in USB mode. See **Connection Type** on page **17** for more information.

2. Press the Schlage button twice. The lock will be displayed on the screen.
3. On the HHD, select **Device Options**.
4. Remove the top inside lock cover.
5. Press and hold the Inside Push button. Then press and release the tamper switch three times.
6. Release the Inside Push button. On the lock, the Inside Push button LED will illuminate.
7. On the HHD, select **Couple HHD to Device**.
8. When Coupling is successful, a message will be displayed on the screen.

This function works with AD-Series devices only.

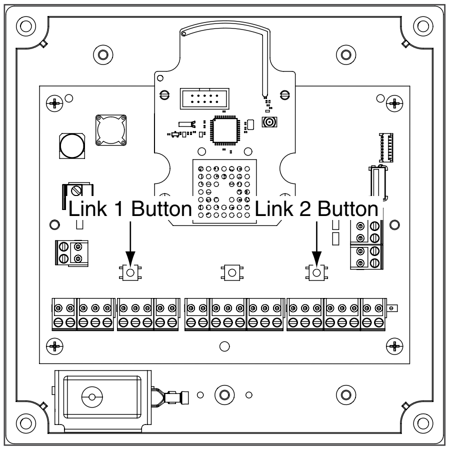
Couple HHD to PIM400 or PIB300

AD-Series devices can be coupled, or authenticated, with the HHD. This provides enhanced security by ensuring that the device will only communicate with HHD(s) to which it has been coupled. Once the device has been coupled, the coupling password is passed to the device from the HHD during programming.

The HHD will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See **Coupling Password** on page **18** for more information.

If a device is not in Coupling mode, SUS will display a device specific message with instructions for placing the device into Coupling mode.

➔ HHDs with the same coupling password can program the same devices. Once the HHD and the device are coupled, the coupling password is disabled in the PIM400 or PIB300 and any HHD with the correct coupling password will automatically couple with the PIM400 (or PIB300).



1 Remove the PIM400 or PIB300 cover.

2 The HHD must be in USB mode. See **Connection Type** on page **17** for more information.

3 Connect the HHD to the PIM400 or PIB300 using the HH-USB cable. The PIM400 or PIB300 will be displayed on the HHD screen.

4 On the HHD, select **Device Options**.

5 On the PIM400 or PIB300, press and hold the LINK 1 button. Then press the LINK 2 button three times.

6 On the HHD, select **Couple HHD to Device**.

7 When Coupling is successful, a message will be displayed on the HHD screen.

This function works with AD-Series devices only.

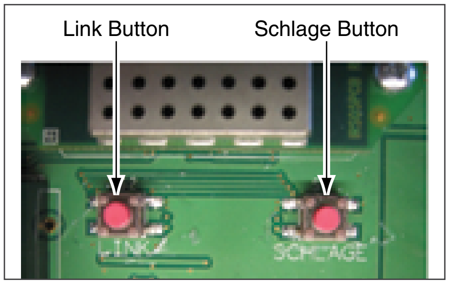
Couple HHD to WRI400/CT5000

The WRI400/CT5000 can be coupled, or authenticated, with the HHD. This provides enhanced security by ensuring that the device will only communicate with HHD(s) to which it has been coupled. Once the device has been coupled, the programming password is passed to the device from the HHD during programming.

The HHD will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See **Coupling Password** on page **18** for more information.

If a device is not in Coupling mode, SUS will display a device specific message with instructions for placing the device into Coupling mode.

➔ HHDs with the same programming password can program the same devices. Once the HHD and the device are coupled, the coupling password is disabled in the WRI400/CT5000 and any HHD with the correct coupling password will automatically couple with the WRI400/CT5000.



1 Remove the device cover.

2 The HHD must be in USB mode. See **Connection Type** on page **17** for more information.

3 Connect the HHD to the device using the HH-USB cable. The name of the device will be displayed on the HHD screen.

4 On the HHD, select **Device Options**.

5 On the WRI400/CT5000, press and hold the Schlage button. Then press the LINK button three times within five (5) seconds. Then release both buttons.

6 On the HHD, select **Couple HHD to Device**.

7 When Coupling is successful, a message will be displayed on the HHD screen.

Program a Lock or Controller

Offline Locks

1 Connect the HHD to the lock or controller and establish communication between the HHD and the device.

2 Select **Device Options**.

3 Select **Program Lock**.

4 Select the door file that should be associated with the lock or controller.

→ Door files are downloaded to the HHD when synchronized with the access control software.

5 Select **OK**.

Online Locks

→ NOTE: This function is not applicable to online locks.

Collect Audits and Update Lock

Collecting audits on the HHD does not delete the audits from a lock.

Collected audits will be transferred from HHD to your Access Control Software the next time they are synchronized.

When Auto Update is enabled, as soon as the Schlage button is pressed twice and the communication with the Schlage Utility Software starts, the lock will automatically:

- update lock's date/time
- collect audits
- update access rights

When Manual Update is enabled, follow the steps below to collect audits and update the lock access rights.

→ See **Update Mode** on page **18** for more information.

Collect Audits when Date/Time and Lock Access Rights are Up-to-Date

1 Confirm HHD is connected to lock.

→ See **Connecting the Handheld Device** on page **20** for more information.

2 Double-click the displayed name of the connected lock.

3 The audit collection will begin.

→ If no previous audit exists, skip to step 7.

4 If a previous audit exists, a message will appear asking to overwrite previous audit. Click **YES** to override audits and skip to step 7.

5 Click **NO** if you do not want to override the audit.

6 Acknowledge the message advising to synchronize the lock with system software. Audit collection will be stopped.

7 A progress indicator will be displayed while the audit is being collected. A message will be displayed once the process is complete.

Collect Audits when Date/Time and Lock Access Rights are Not Up-to-Date

1 Confirm HHD is connected to lock.

➔ See **Connecting the Handheld Device** on page **20** for more information.

2 Double-click the displayed name of the connected lock.

3 When asked to update date and time of the device, click **YES**. A progress indicator will be displayed while date and time is being updated.

4 A message will appear to confirm the successful update.

5 The audit collection will begin. A progress indicator will be displayed while the audit is being collected.

6 The access rights update will begin. A progress indicator will be displayed while lock is being updated.

7 A message will be displayed once the process is complete.

View Properties

1 Connect the HHD to the lock or controller.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 The **View** tab will be displayed.

➔ See **Lock Properties** on page **31** for more information.

Edit Properties

1 Connect the HHD to the device.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 Select the **Edit** tab.

5 Edit the properties as desired.

➔ See **Lock Properties** on page **31** for more information.

6 Select **Save** to update and save the changes.View Reader Properties

1 Connect the HHD to the device.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 Select the **Reader** tab.

➔ See **Lock Properties** on page **31** for more information.

Edit Reader Properties

1 Connect the HHD to the device.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 Select the **Reader** tab.

5 Edit the properties as desired.

6 Select **Save** to update and save the changes.

➔ See **Lock Properties** on page **31** for more information.

Put PIM400 into Link Mode

1. Connect the HHD to the PIM400.
2. Select **Device Options**.
3. Select **PIM Properties** for the connected device.
4. Select the **Link** tab.
5. Select the door number from the drop-down box.
   ➔ See the system administrator for the proper door number selection.
6. The PIM400 will stay in link mode for up to 30 minutes.
7. Put the lock (door) into link mode.
   ➔ See the user guide that came with the lock for more information.
8. The PIM400 will automatically exit link mode once linking is complete.

Put PIM400 into Diagnostics Mode

1. Connect the HHD to the PIM400 and select Device Options.
2. Select Diagnostics and then select the door number from the drop-down box.
   - Card Data box: shows card data from credential when card presented to reader.
   - Unlock on Read: if enabled allows the door to be unlocked upon the reading of a card: the OEM has the ability to disable this feature (grayed out).

Update Firmware

➔ See **AD-Series and CO-Series Device Firmware Update** on page **77** for more information.

Diagnostic Data Log Feature

This new feature provides a simple method for AD-Series customers to quickly gather and save important lock-status information in a file. For details see Appendix E: Diagnostic Data Log.

AD-Series Readers

The Multi-Tech and Multi-Tech + Keypad readers will read both proximity and smart cards. The Proximity, Proximity + Keypad ONLY and Smart Card, Smart Card + Keypad ONLY readers have been discontinued and replaced by the MultiTech, Multi-Tech + Keypad readers that provide all the same functionality as the original Proximity and Smart card readers in a single credential reader.

Multi-Tech

Multi-Tech + Keypad

The MiK and SiK2 readers are both a solution for applications using the HID iClass smart card credential.

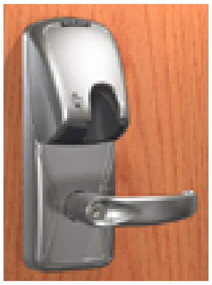
iCLASS® is a proprietary smart card technology developed by HID that operates on ISO 15693. In order to support these requirements, iClass + Multi-Tech + Keypad reader were integrated to create the (MiK) and (SiK2). (SiK2) is not capable of reading Proximity credentials.

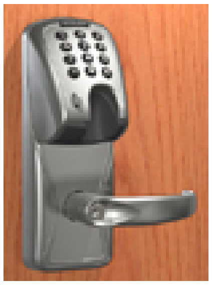
iClass + Multi-Tech

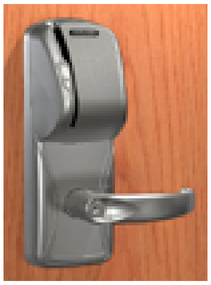
iClass + Multi-Tech + Keypad

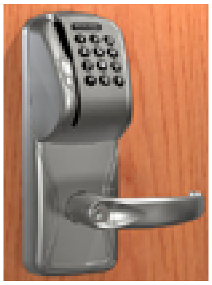
The FMK reader module is for applications which require approval by the U.S. Federal Government under HSPD-12 for FIPS 201 compliance. In order to meet these requirements, FIPS + Multi-Technology + Keypad reader were integrated to create the (FMK).

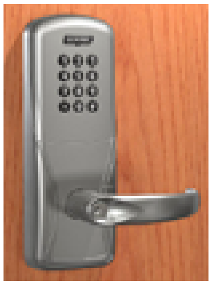
FIPS + Multi-Tech + Keypad


MagInsert


MagInsert + Keypad


MagSwipe


MagSwipe + Keypad


Keypad

Reader Types

Reader Description	Reader Type Shown in SUS
Mag Insert with Keypad	MagInsert + Keypad
Mag Insert without Keypad	MagInsert
Mag Swipe with Keypad	MagSwipe + Keypad
Mag Swipe without Keypad	MagSwipe
Keypad Only	Keypad
Prox with Keypad	Proximity + Keypad
Prox without Keypad	Proximity
Smart with Keypad	Smart Card + Keypad
Smart without Keypad	Smart Card
FMK Reader	FIPS + Multi-Tech + Keypad
MT	Multi-Tech
MTK	Multi-Tech + Keypad
Mi	iClass + Multi-Tech
MiK	iClass + Multi-Tech + Keypad
MT2	Multi-Tech 2
MTK2	Multi-Tech 2 + Keypad
FMK2	FIPS + Multi-Tech 2 + Keypad
KP2	Keypad 2
Si2	iClass + Smart Only 2
SiK2	iClass + Smart Only 2 + Keypad

➔ Note: (Multi-Tech, Multi-Tech + Keypad) and (iClass + Multi-Tech, iClass + Multi-Tech + Keypad) and (FIPS + Multi-Tech +Keypad) and (Keypad) readers are being discontinued (1st half 2016) and replaced by the (Multi-Tech 2, Multi-Tech + Keypad 2) and (FIPS + Multi-Tech +Keypad 2) and (Keypad 2) readers that provide all the same functionality as the original readers.

Lock Properties

- AD-200/250 (Offline Locks): pg 31
- AD-300 (Networked Locks): pg 34
- AD-400 (Networked Locks): pg 38

AD-200/250 (Offline Locks)

VIEW Tab	Property	Description
	Lock Name	The name of the Lock. Set by the door file programmed into the lock.
	Date & Time	Current date and time. Initialized/set by the HHD.
	General Properties	
	Model	Model number of the device connected to the HHD.
	Max Users	Number of Users supported by the lock (AD-200).
	Max Void List	Number of void users supported by the lock (AD-250).
	Power Status	Current voltage level of the AA and Coin Cell batteries. Number of AA batteries connected to the lock.
	Max One Time User	Number of one time use PIN codes supported by the lock (AD-250).
	Main Lock	
	Serial Number	Serial number that uniquely identifies the lock.
	Manufacture Date	Date the lock was manufactured.
	Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when a new firmware version is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Credential Reader	
	Serial Number	Serial number that uniquely identifies the reader.
	Manufacture Date	Date the reader was manufactured.
	Firmware Version	Version of the current firmware file. Automatically updated when a new firmware version is loaded.
	Hardware Version	Current version of the printed circuit credential board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Reader Type	Type of Reader installed: • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
	Custom Key	If the reader supports reporting the status of custom configuration then SUS displays "Custom Key: Installed" or "Custom Key: Not Installed"

AD-200/250 (Offline Locks)

	Property	Description	Default
EDIT Tab	Lock Type	**Classroom:** Unlocks when a credential is presented and then automatically locks after the relock delay has expired. **Office:** Unlocks when a credential is presented and then automatically locks after the relock delay has expired. To keep the door unlocked, push the button on the inside. The button will momentarily illuminate green. To return the lock to the locked state, push the button again or present a credential to the outside. **Privacy:** To initiate the Privacy function, with the door closed, push the button on the inside of the door. This prevents normal credentials from opening the door from the outside. The lock will go back to its normal state when the button is pushed again or when the door position switch indicates that the door has opened. When using a Mortise Deadbolt, extending the deadbolt from the inside lights a red LED on the inside trim and initiates the Privacy function which prevents normal credentials from opening the door from the outside. The lock can always be opened using a Pass-Through credential or mechanical key in case of emergency. **Apartment:** The apartment function lock is normally locked and never relocks automatically, which prevents users from being locked out. To unlock the door from the outside, present a credential. To unlock the door from the inside, push the inside button or, if using the MD chassis, retract the deadbolt. Egress always available from inside. When lever is rotated and door is opened, the request-to-exit switch is used in conjunction with the door position switch to cause the door to return to unlocked condition. To lock the door from the outside, present a credential. To lock the door from the inside, push the inside button or, for MD chassis, extend the deadbolt.	Set by the Factory
	PIN Length (AD-200 only)	Maximum number of digits in the user PIN. Range of 3 to 6 digits.	6
	Allow Privacy Mode Override (AD-250 only)	When enabled, allows cards to override a lock that has been placed in privacy mode. When disabled, only cards specifically assigned to this door will have access.	Disabled
	Ignore Keypad	If checked, key entry codes are ignored.	Disabled
	Record Lock/Unlock	If checked and supported by the system software, will record an audit event when the Inside Push button is pressed.	Disabled
	Enable/Disable Interior LED Status Blinking	Enables or Disables the interior LED's status blinking. When enabled: (enables two options to be checked) • Blink Interior Button LED when locked - The IPB will flash every 15 seconds for the first 10 minutes; it will then flash every 30 seconds for the next 50 minutes; and it will then flash every minute after 1 hour. If a door actuation occurs, then the process is restarted. • Blink Interior LED Rapidly when in Privacy Mode - Interior LED will flash rapidly while privacy mode is enabled.	Disabled (unchecked)
	Battery Fail Mode	Lock state set when battery fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is
	Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential.	3
	ADA Delay	Amount of time before the lock relocks after being unlocked by a user who is flagged as handicapped and presenting a valid credential. Can be changed in the access control system.	30

AD-200/250 (Offline Locks)

	Property	Description	Default
READER Tab	Prox in Use (AD-200 only)	Proximity credential card types allowed. Selections: • HID/Kantech ioProx* • GE/CASI • GE4001 • GE4002* • AWID*	* Default formats
	Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3. Track 1 not configurable for AD-200.	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled
	Smart Cards in Use (AD-200 only)	Smart card(s) to be used with the card reader. • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* **MTK1** • iClass credential formats for Reader Types which support Smart Cards • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE **MTK2** • iClass/Felica credential formats for Reader Types which support Smart Cards • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE	* Default formats
	Beeper	Indicates if the Beeper is on or off.	ON

AD-300 (Networked Locks)

	Property	Description
VIEW Tab	General Properties	
	Model	Model number of the device connected to the HHD.
	Power Status	Shows current auxiliary power status of OFF/ON.
	Main Lock	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Serial Number	Serial number that uniquely identifies the lock.
	Manufacture Date	Date the lock was manufactured.
	Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Credential Reader	
	Serial Number	Serial number that uniquely identifies the reader.
	Manufacture Date	Date the reader was manufactured
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Reader Type	Type of Reader installed: • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
	Custom Key	If the reader supports reporting the status of custom configuration then SUS displays "Custom Key: Installed" or "Custom Key: Not Installed"

AD-300 (Networked Locks)

EDIT Tab	Property	Description	Default
	RS485 Address	Set the RS-485 network address of the lock. 0-255	0
	ACP Timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	3 seconds
	Comm Loss Fail Mode	Lock state set when communication from the ACP fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is
	Power Fail Mode	Lock state set when power to the lock fails. As-Is, Secure/Locked, Unsecure/ Unlocked	As-Is
	Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode. abilities. 0 = cache mode disabled	0
	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	Disable Interior Button LED	If checked, interior button LED blinking is disabled.	LED is Enabled (unchecked)
	Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential.	3 seconds
	Relatch After: Timer/Door Status	Re-latch on: • Timer Only (Lock when timer expires regardless of Door status or Position) • On Door Open or Timer (Lock when the Door opens or Timer expires) • On Door Close or Timer (Lock when the Door closes or Timer expires)	Timer only
	Card + PIN LED mode	Disabled Mode 1: 2 alternating blinks Mode 2: Solid Green/2 red blinks	1
	Communication Link	Direct to Host: Sets RS-485 communication protocol to work directly with an ACP. Through PIB300: Sets RS-485 communication protocol through the PIB300.	Direct to Host

AD-300 (Networked Locks)

	Property	Description	Default
READER Tab	Prox in Use	Proximity credential card types allowed. Selections: • HID/Kantech ioProx* • GE/CASI • GE4001 • GE4002* • AWID*	* Default formats
	Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and having data on track 2, this option will allow longer battery life. (Available only on battery-powered locks.)	Enabled
	Smart Cards in Use	Smart card(s) to be used with the card reader. • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* **MTK1** • iClass credential formats for Reader Types which support Smart Cards • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE **MTK2** • iClass/Felica credential formats for Reader Types which support Smart Cards • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE	* Default formats

AD-300 (Networked Locks)

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	1
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range in 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

AD-400 (Networked Locks)

	Property	Description
VIEW Tab	General Properties	
	Model	Model number of the device connected to the HHD.
	Power Status	Current voltage level and number of AA batteries.
	Main Lock	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Serial Number	Serial number that uniquely identifies the lock.
	Manufacture Date	Date the lock was manufactured.
	Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Credential Reader	
	Serial Number	Serial number that uniquely identifies the reader.
	Manufacture Date	Date the reader was manufactured.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit credential board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Reader Type	Type of Reader installed: • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
	Custom Key	If the reader supports reporting the status of custom configuration then SUS displays "Custom Key: Installed" or "Custom Key: Not Installed"
	Communication	
	Serial Number	Serial number that uniquely identifies the communication module.
	Firmware Version	Version of the communication module firmware.

[1] These properties are view-only when the HHD is connected to the lock. Connect the HHD to the PIM400 to make changes.

AD-400 (Networked Locks)

	Property	Description	Default
EDIT Tab	Heartbeat	The heartbeat is a brief communication from the lock to the PIM400. It allows an idle lock to check for messages. Range: 15 seconds - many hours. The value indicates the time between the heartbeats. Set to a shorter time (lower number) for more frequent communication. Set to a longer time (higher number) for less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.	10 minutes
	Comm Loss Fail Mode	Lock state set when RF communication with the linked PIM400 fails. States: As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	Allow Extended Unlocks (Locks linked to PIM400-TD2 only)	Extended unlock permits the lock to stay in an indefinite unlock state. Enabling the Extended Unlock feature is required to implement a scheduled unlock period from an ACP.	Enabled
	Report RTX for Host to unlock[1]	Determines how an AD-400 will handle a request to exit. If disabled, the AD-400 will only report that a request to exit has occurred. Disable if the access point does not need to be electronically unlocked to provide egress (if equipped with a crash bar) but the access control panel needs to be notified so that a forced door does not occur. If enabled, the AD-400 will report that a request to exit has occurred, and also will query the PIM400 to determine if the AD-400 should be electronically unlocked. Use this mode if the AD-400 needs to be electronically unlocked in order to provide egress.	Disabled
	Relatch After: Timer/Door Status	Re-latch on: • Timer Only (Lock when Timer expires (default 3 seconds) regardless of Door status or Position) • On Door Open or Timer (Lock when the Door opens or Timer expires) • On Door Close or Timer (Lock when the Door closes or Timer expires)	Timer only
	High Low Output (Locks linked to PIM400-TD2 only)	Polarity of the Request-to-Exit (RTX) signal.	Low: RTX
		Polarity of the Request-to-Enter (RTE) signal.	Low: RTE
		Polarity of the On Door Open, (Door Position Switch (DPS)) signal.	High: open
		Polarity of Trouble signal.	Low: trouble
	First, Delay, Retry	**First:** First query a Lock makes to a PIM400 occurs immediately following presentation of a credential. First is the amount of time, in milliseconds, an AD-400 should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance. **Delay:** The idle time between subsequent queries. Shorter delays may reduce latency. Longer delays may enhance battery life. **Retry:** The maximum number of times an access point queries a PIM400 before the Lock goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host. Retrys = [{Max Response Time of Panel- First}/Delay] + 1	First: 300 msec. Delay: 200 msec. Retry: 5
	Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode. abilities. 0 = cache mode disabled	0

[1] These properties are view-only when the HHD is connected to the lock. Connect the HHD to the PIM400 to make changes.

AD-400 (Networked Locks)

Edit Tab (Cont.)	Property	Description	Default
	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by “Full Card” content or just “Facility Code”.	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Card + PIN LED Mode	Disabled Mode 1: 5 left green and right red alternating blinks Mode 2: 5 left green and right red alternating blinks, plus two beeps	1
	Request to Enter	Report Request to Enter signal state to PIM400/401.	Always Enabled
	Wakeup status[1]	Displays the time, in seconds, the lock listens for Wake on Radio broadcasts from its linked PIM400/401.	Disabled
	Disable Interior Button LED	If checked, interior button LED blinking is disabled.	Disabled (unchecked)
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	ACP Timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	10 seconds
	Battery Fail Mode	Lock state set when battery fails. As-Is, Secure/Lock, Unsecure/Unlock	As-Is

[1] These properties are view-only when the HHD is connected to the lock. Connect the HHD to the PIM400 to make changes.

AD-400 (Networked Locks)

	Property	Description	Default
READER Tab	Prox in Use	Proximity credential card types allowed. Selections: • HID/Kantech ioProx* • GE/CASI • GE4001 • GE4002* • AWID*	* Default formats
	Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled
	Smart Cards in Use	Smart card(s) to be used with the card reader. • 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) • 14443 Secure MiFare Classic* • 14443 Secure MiFare Plus* • 14443 EV1 (NOC)* • 15693 UID (CSN)* **MTK1** • iClass credential formats for Reader Types which support Smart Cards • iClass 40-bit UID (CSN) • iClass 64-bit UID (CSN)* • HID iClass Classic* (only appears with Mi/MiK reader attached) • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE **MTK2** • iClass/Felica credential formats for Reader Types which support Smart Cards • iClass/Felica 40-bit UID (CSN) • iClass/Felica 64-bit UID (CSN)* • HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. • PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE	* Default formats

[1] These properties are view-only when the HHD is connected to the lock. Connect the HHD to the PIM400 to make changes.

AD-400 (Networked Locks)

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range is 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

[1] These properties are view-only when the HHD is connected to the lock. Connect the HHD to the PIM400 to make changes.

Controller Properties

- WPR400: pg 43
- PIM400 -TD2, -485, -VBB (PIM PROPERTIES): pg 46
- PIM400 -TD2, -485, -VBB (LOCK PROPERTIES): pg 47
- PIB300: pg 51
- WRI400: pg. **(page 53)**
- CT5000: pg. **(page 55)**

WPR400

	Property	Description
VIEW Tab	General Properties	
	Model	Model of the device connected to the HHD.
	Power Status	Current voltage level and number of AA batteries.
	MAIN LOCK	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Serial Number	Serial number that uniquely identifies the lock.
	Manufacture Date	Date the lock was manufactured
	Days Since Installed	Used for warranty purposes; it marks the beginning of the lock's functional life.
	Firmware Version	Current version of the firmware
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Hardware Version	Current version of the printed circuit board.
	Credential Reader	
	Serial Number	Serial number that uniquely identifies the reader.
	Manufacture Date	Date the reader was manufactured.
	Firmware Version	Current version of the firmware
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Hardware Version	Current version of the printed circuit board.
	Reader Type	Type of Reader installed: • MagInsert • MagInsert + Keypad • MagSwipe • MagSwipe + Keypad • Keypad • Proximity • Proximity + Keypad • Smart Card • Smart Card + Keypad • Multi-Tech • Multi-Tech + Keypad • FIPS + Multi-Tech + Keypad • iClass + Multi-Tech • iClass + Multi-Tech + Keypad • Multi-Tech 2 • Multi-Tech 2 + Keypad • FIPS + Multi-Tech 2 + Keypad • Keypad 2 • iClass + Smart Only 2 • iClass + Smart Only 2 + Keypad
	Custom Key	If the reader supports reporting the status of custom configuration then SUS displays "Custom Key: Installed" or "Custom Key: Not Installed"
	Communication	
	Serial Number	Serial number that uniquely identifies the communication module.
	Firmware Version	Version of the communication module firmware.

WPR400

	Property	Description	Default
EDIT Tab	Relatch After: Timer Length	Amount of time before the lock re-locks after being unlocked by a user presenting a valid credential.	3 seconds
	First, Delay, Retry	**First:** First query a Lock makes to a PIM400 occurs immediately following presentation of a credential. First is the amount of time, in milliseconds, the WPR400 should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance. **Delay:** The idle time between subsequent queries. Shorter delays may reduce latency. Longer delays may enhance battery life. **Retry:** The maximum number of times the WPR400 queries a PIM400 before the Lock goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host. Retrys = [{Max Response Time of Panel- First} / Delay] +1	First: 300 msec. Delay: 200 msec. Retry: 5
	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Card + PIN LED mode	Disabled Mode 1: 2 alternating blinks Mode 2: Solid Green / 2 red right blinks	1
	Wakeup Status	Displays the time, in seconds, the lock listens for Wake on Radio broadcasts from its linked PIM400.	Disabled
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	ACP Timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	10 seconds

WPR400

	Property	Description	Default
READER Tab	Prox in Use	Proximity credential card types allowed. Selections: · HID/Kantech ioProx* · GE/CASI · GE4001 · GE4002* · AWID*	* Default formats
	Mag Track in Use	Magnetic card track that access data is to be read from. Select Track 1, 2 or 3	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled
	Smart Cards in Use	Smart card(s) to be used with the card reader. · 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) · 14443 Secure MiFare Classic* · 14443 Secure MiFare Plus* · 14443 EV1 (NOC)* · 15693 UID (CSN)* **MTK1** · iClass credential formats for Reader Types which support Smart Cards · iClass 40-bit UID (CSN) · iClass 64-bit UID (CSN)* · HID iClass Classic* (only appears with Mi/MiK reader attached) · PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE **MTK2** · iClass/Felica credential formats for Reader Types which support Smart Cards · iClass/Felica 40-bit UID (CSN) · iClass/Felica 64-bit UID (CSN)* · HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. · PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE	* Default formats

WPR400

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	1
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range in 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

PIM400 -TD2, -485, -VBB (PIM PROPERTIES)

	Property	Description
VIEW Tab	General Properties	
	Model	Model number of the device connected to the HHD.
	Source ID	Unique identifier for the PIM400.
	PIM	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Firmware Version	Version of the current firmware file. Automatically updated when a new firmware version is loaded.
	Bootloader version	Version of the current bootloader. Allows new firmware to be loaded.
	Serial No.	Serial number that uniquely identifies the device.
	Manufacture Date	Date the device was manufactured.
	Days since Installed	Used for warranty purposes; marks the beginning of the lock’s functional life.
	Hardware Version	Current version of the printed circuit main board.
	Communication	
	Firmware Version	Version of the communication module firmware.

PIM400 -TD2, -485, -VBB (PIM PROPERTIES)

	Property	Description	Default
EDIT Tab	Unique ID	Set the Unique Identification number of the PIM400. Range: 0 to 65534.	
	Freq Channel	Radio Frequency Channel used for communication with wireless devices. One of ten RF channels can be set.	1
	RS-485 Address	PIM400 -485 and PIM400-VBB ONLY. Set the RS-485 network address of the PIM400/401. Address range 0-254	0
	Low Door	PIM400 -485, -VBB ONLY. Set the Low address for the range of door addresses available for linking. Range: 0 to 255	0
	High Door	PIM400 -485, -VBB ONLY. Set the High address for the range of door addresses available for linking. Range: 0 to 255	15
	Channel Switching	Dynamic Channel Switching is used to improve immunity to RF channel interference. One of three RF channel groups can be set.	Disabled
	Wakeup	When enabled, this feature causes wireless devices linked to the PIM400/401 to respond within seconds to a centralized command from the access control panel. When disabled, the wireless devices will respond only during their heartbeat, which could result in a delay. Range 0 to 10 seconds. 0 = disabled	Disabled
	Output Type (PIM400-TD2 only)	Magnetic, Wiegand or Automatic. Outputs the Credential Card and Keypad data in either Magnetic or Wiegand format. When Automatic is selected, the PIM400-TD2 will detect the Credential Card and Keypad data format and then send the received data in its original data format.	Automatic
LINK Tab (PIM400/401, -485, -VBB only)	**Property**	**Description**	**Default**
	Select Door	Select the door address desired to be linked to the PIM400 -485.	

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

	Property	Description
VIEW Tab	General Properties	
	Model	Model of the device connected to the HHD.
	Door Number	Allows the selection of a door connected to the PIM400 to display its properties.
	Power Status	Current voltage level of the AA batteries.
	PIM	
	Firmware Version	Version of the firmware.
	Communication	
	Firmware Version	Version of the communication module firmware.

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

	Property	Description	Default
EDIT Tab	Heartbeat	The heartbeat is a brief communication from the lock to the PIM400. The heartbeat allows an idle lock to check for messages from the PIM400. By default, this occurs every 10 minutes, but can be adjusted in the range of 15 seconds to many hours. The value indicates the time between the heartbeats. Set the value to a shorter time (lower number) to achieve more frequent communication while the lock is idle. Set the value to a longer time (higher number) to achieve less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.	10 minutes
	Comm Loss Fail Mode	Lock state set when RF communication with the linked PIM400 fails. Selections: As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	Allow Extended Unlocks (PIM400-TD2 only)	Extended unlock is a feature that permits the lock to stay in an indefinite unlock state. Enabling the Extended Unlock feature is required to implement a scheduled unlock period from an ACP.	enabled
	Report RTX for Host to Unlock	This feature determines how a Wireless Access Point (Door) will handle a request to exit. If not checked (disabled), then the access point will only report that a request to exit has occurred. Use this mode if the access point does not need to be electronically unlocked in order to provide egress (for instance, the access point has a crash bar) but the access control panel needs to be notified so that a forced door does not occur. If checked (enabled), then the access point will not only report that a request to exit has occurred, but will query the PIM400 (as in a card swipe) to determine if the access point should be electronically unlocked. Use this mode if the access point needs to be electronically unlocked in order to provide egress.	Enabled
	Relatch After: Timer Length	Amount of time, in seconds, before the lock re-locks after being unlocked by a user presenting a valid credential.	3 seconds
	Relatch After : Timer/ Door Status	Re-latch on: • Timer Only: Lock when timer expires regardless of Door status or Position • On Door Open or Timer: Lock when the Door opens or Timer expires • On Door Close or Timer: Lock when the Door closes or Timer expires	Timer only
	High Low Output (PIM400-TD2 only)	Polarity of the Request-to-Exit (RTX) signal.	Low: RTX
		Polarity of the Request-to-Enter (RTE) signal.	Low: RTE
		Polarity of the On Door Open, (Door Position Switch (DPS)) signal.	High: open
		Polarity of Trouble signal.	Low: trouble
	First, Delay, Retry	First: First query a lock makes to a PIM400 occurs immediately following presentation of a credential. First is the amount of time, in milliseconds, an access point should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance. Delay: The idle time between subsequent queries. Shorter delays may reduce latency. Longer delays may enhance battery life. Retry: The maximum number of times and access point queries a PIM400 before the lock goes back to sleep. The number of retires shoudl be slightly greater than the longest response time from the access control panel or host. Retry = [{ Max Response Time of Panel - First } / Delay] + 1.	First: 300 Delay: 200 Retry: 5
	Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode.abilities. 0 = cache mode disabled	0

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

EDIT Tab (Cont.)	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled
	Degraded (Cache) Mode: PIM485 Card Removal	PIM400 -485, -VBB ONLY. Only displayed when a Legacy PIM is connected. If disabled only time or a full cache will remove an entry from the cache. If enabled only a full cache or receiving a RS−485 Deny Access command will remove an entry from the cache.	Disabled
	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by “Full Card” content or just “Facility Code”.	Full Card
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Card + PIN LED mode	Disabled Mode 1: 5 left green and right red alternating blinks Mode 2: 5 left green and right red alternating blinks, plus two beeps	1
	Request to Enter	Report Request to Enter signal state to PIM400	Disabled
	Wakeup	Displays the time, in seconds, the Wireless Access Point Device listens for Wake on Radio broadcasts from its linked PIM400.	Disabled
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000.	125
	ACP timeout	Time (in seconds) to wait before determining communication from the ACP has failed.	10 seconds
	Power Fail Mode	Lock state set when battery fails. As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	Pin Required	TD2 Only	Disabled (unchecked)
	Disable Interior Button LED	TD2 and 485	Enabled (unchecked)

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

	Property	Description	Default
READER Tab	Prox in Use	Proximity credential card types allowed. Selections: ▪ HID/Kantech ioProx* ▪ GE/CASI ▪ GE4001 ▪ GE4002* ▪ AWID*	* Default formats
	Mag Track in Use	Magnetic card track that access data is to be read from. Select Track 1, 2 or 3	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled
	Smart Cards in Use	Smart card(s) to be used with the card reader. ▪ 14443 UID(CSN) (when selected, disables all other 14443 selections and PIV format) ▪ 14443 Secure MiFare Classic* ▪ 14443 Secure MiFare Plus* ▪ 14443 EV1 (NOC)* ▪ 15693 UID (CSN)* **MTK1** ▪ iClass credential formats for Reader Types which support Smart Cards ▪ iClass 40-bit UID (CSN) ▪ iClass 64-bit UID (CSN)* ▪ HID iClass Classic* (only appears with Mi/MiK reader attached) ▪ PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE **MTK2** ▪ iClass/Felica credential formats for Reader Types which support Smart Cards ▪ iClass/Felica 40-bit UID (CSN) ▪ iClass/Felica 64-bit UID (CSN)* ▪ HID iClass/iClass SE/iClass SEOS (only appears with Si2/SiK2 reader attached). Enabled by default. ▪ PIV credential formats for AD200 reader types which support Smart Cards. Range is 1 to 15. 1. 75 Bit PIV* 2. 58 Bit TWIC/CAC 3. 200 Bit FASC–N 4. 64 Bit (BCD) TWIC/CAC 5. 83 Bit TWIC/CAC 6. 66 Bit (58 Bit Format + TSM) TWIC/CAC 7. 64 Bit (58 Bit Format (no parity) + TSM) TWIC/CAC 8. 91 Bit (83 Bit Format + TSM) TWIC/CAC 9. 40 Bit BCD 10. 40 Bit Reversed BCD 11. 64 Bit BCD 12. 64 Bit Reversed BCD 13. 128 Bit BCD 14. 128 Bit Reversed BCD 15. 58 Bit HSE	* Default formats

PIM400 -TD2, -485, -VBB (LOCK PROPERTIES)

READER Tab	Beeper	Indicates if the Beeper is On or Off.	ON
	Keypad: Output Type	Wiegand or Magnetic output type.	Wiegand
	Keypad: Facility Code	A facility or site code is encoded into each card to increase security. A number from 0 to 255 on a 26-bit format card.	1
	Keypad: Keys Buffered	Fixed number of key presses to buffer. Range in 1 to 11. Active only in keypad output modes that support buffered key presses. See Output formats 4, 6, 9 and 10 below.	4
	Keypad: Output Format	Sets the keypad data length and format mode. Range is 0 to 12. 0. Disable Keypad output 1. Mode 1: 4 Data Bits per Key without Parity (high nibble) 2. Mode 2: 4 Data Bits per Key with Parity 3. Mode 3: 8 Data Bits per Key without Parity 4. Mode 4: 8 Data Bits per Key with Parity 5. Mode 5: 4 Data Bits per Key, Buffered Key Presses without Parity 6. Mode 6: 4 Data Bits per Key, Buffered Key Presses with Parity 7. Mode 7: 26 Bit Wiegand Emulation 8. Mode 8: 4 Data Bits per Key without Parity (low nibble) 9. Mode 9: IR, 4 Data Bits per Key, Buffered Key Presses without Parity 10. Mode 10: IR, 4 Data Bits per Key, Buffered Key Presses with Parity 11. Mode 11: 8 Data Bits per Key, ASCII with parity 12. Mode 12: 32 Bit Wiegand Emulation	1

PIB300

	Property	Description
VIEW Tab	General Properties	
	Model	Model of the device connected to the HHD.
	PIB	
	Firmware Version	Version of the firmware file. Automatically updated when a new firmware file is loaded.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Serial No.	Serial number that uniquely identifies the device.
	Manufacture Date	Date the device was manufactured.
	Days since Installed	Used for warranty purposes; marks the beginning of the lock's functional life.
	Hardware Version	Current version of the printed circuit main board.

PIB300

	Property	Description	Default
EDIT Tab	Standard / Legacy VIP	RS-485 network communication format: Standard (Schlage RSI RS-485 protocol) or Legacy VIP Protocol.	Standard
	Number of doors	Number of doors connected to the RS-485 network.	2
	Lock 1 Address	RS-485 address for Lock 1, Range: 0 to 254	0
	Lock 2 Address	RS-485 address for Lock 2, Range: 0 to 254	1
	Output Type	Magnetic, Wiegand or Automatic. Outputs the Credential Card and Keypad data in either Magnetic or Wiegand format. When Automatic is selected, the PIB300 will detect the Credential Card and Keypad data format and then send the received data in its original data format.	Automatic
	Host Control: LED Control	Off= two-line led control of lock led indication On=single-line led control of lock led indication	Unchecked
	Host Control: LED Standard	Off=led standard (active low signal from access control panel) On=led invert (active high signal from access control panel.)	Unchecked
	Host Control: LED Style	Off=led style std. (For use on two led system.) On=special case. If panel tries to light both leds (at the same time) neither of them lights. Beeper is not controlled by panel with this switch on. S1-1 must be set to off when this switch is set to on.	Unchecked
	Host Control: Lock Control from ACP	Off=normally open lock control from panel On=normally closed lock control from panel	Unchecked
	Host Control: Beep Std/ Inverted	Off=beep standard (active low signal from access control panel) On=beep inverted (active high signal from access control panel)	Unchecked
	Output Reporting: Door Status	Off=normally open door status output (when door closed) On=normally closed door status output (when door closed)	Unchecked
	Output Reporting: Request to Exit (RTX)	Off=normally open RTX output when lever not depressed On=normally closed RTX output when lever not depressed	Unchecked
	Output Reporting: Spare	Off=normally open spare output (normal = key not used/latch extended, locked position) On=normally closed spare output (normal = key not used/latch extended, locked position)	Unchecked
	Output Reporting: Spare Status	Off=spare output provides status of key use (rta) - if lock is equipped w/option On=spare output provides status of latch bolt monitor (lbm) - if lock is equipped w/ option	Unchecked
	Output Reporting: Spare Provides	Off=spare output does not provide troubles status. Selection on 9 is used On=spare output provides troubles status. Selection on 9 is ignored	Unchecked

WRI400

VIEW Tab	Property	Description
	General Properties	
	Model	Model number of the device connected to the HHD.
	Main Lock	
	RS485 Partner ID	Identifies the participating OEM software partner.
	Serial Number	Serial number that uniquely identifies the WRI400.
	Manufacture Date	Date the WRI400 was manufactured.
	Days Since Installed	Used for warranty purposes; marks the beginning of the WRI400 functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Communication	
	Serial Number	Serial number that uniquely identifies the communication module.
	Firmware Version	Version of the communication module firmware.

EDIT Tab	Property	Description	Default
	Heartbeat	The heartbeat is a brief communication from the WRI400 to the PIM400. It allows the WRI400 to check for messages. Range: 1 s. – 65535 s. The value indicates the time between the heartbeats. Set to a shorter time (lower number) for more frequent communication. Set to a longer time (higher number) for less frequent communication. A smaller value will decrease battery life. A larger value will increase battery life.	10 minutes
	Comm Loss Fail Mode	WRI400 state set when the RF communication with the linked PIM400 fails. States: As-Is, Secure/Lock, Unsecure/Unlock	As-Is
	Allow Extended Unlocks	Extended unlock permits the WRI400 to stay in an indefinite unlock state (available only in a PIM400-TD2). Enabling the Extended Unlock feature is required to implement a scheduled unlock period from an Access Control Panel.	Enabled
	Report RTX for Host to unlock	Determines how the WRI400 handles a request to exit. If disabled, the WRI400 will only report that a request to exit has occurred. Disable if the WRI400 does not need to be electronically unlocked to provide egress (if equipped with a crash bar) but the access control panel needs to be notified so that a forced door does not occur. If enabled, the WRI400 will report that a request to exit has occurred, and also will query the PIM400 to determine if it should be electronically unlocked. Use this mode if the WRI400 needs to be electronically unlocked in order to provide egress.	Enabled
	Relatch After	Amount of time before the WRI400 re-locks after being unlocked by a user presenting a valid credential. The value set in the HHD is only used if the Access Control Panel (ACP) responds with a "Momentary Unlock" command. When the Access Control Panel sends the number of seconds to unlock the WRI400 then the relatch after value set in the HHD is ignored.	3 seconds
	Relatch After: Timer/ Door Status	Timer Only: Locks the WRI400 when timer expires regardless of its status or position. On Door Open or Timer: Locks WRI400 when it opens or Timer expires. On Door Close or Timer: Locks WRI400 when it closes or Timer expires.	Timer Only

WRI400

EDIT Tab (cont.)	Output (PIM400-TD2) On Door Open	Signaled through the PIM400-TD2 to the Access Control Panel, it sets the polarity of the Request to Enter (RTE) signal.	Active High
	Output (PIM400-TD2) On Request to Exit: Active High/Active Low	Signaled through the PIM400-TD2 to the Access Control Panel, it sets the polarity of the Request to Exit (RTX) signal.	Active Low
	Output (PIM400-TD2) On Trouble: Active High/Active Low	Signaled through the PIM400-TD2 to the Access Control Panel, this sets the polarity of the Trouble signal.	Active Low
	WRI400 - Input Request to Enter: Active Open/Active Close	This sets the polarity of the Request To Enter signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Request to Enter.	Active Close
	WRI400 - Input Request to Exit: Active Open/Active Close	This sets the polarity of the Request To Exit signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Request to Exit.	Active Close
	Reader 1 Tamper: Active Open/Active Closed	This sets the polarity of the Reader 1 Tamper signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Reader 1 Tamper.	Active Close
	Reader 2 Tamper: Active Open/Active Closed	This sets the polarity of the Reader 2 Tamper signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports a Reader 2 Tamper.	Active Close
	Door Position Switch (DPS): Active Open/ Active Closed	This sets the polarity of the Door Position Switch (DPS) signal into the WRI400. Default is when the switch is closed and the WRI400 reads and reports the door closed.	Active close
	First, Delay, Retry	**First**: First query the WRI400 makes to a PIM400 occurs immediately following presentation of a credential. This parameter is the amount of time, in milliseconds a WRI400 should wait before making its second query to a PIM400. This setting should be slightly greater than the fastest response time from the access control panel or host to any message originated by the WRI400. This optimizes battery life and system performance. **Delay**: The idle time between subsequent queries. Shorter delays may reduce latency, but also decrease battery life. Longer delays may enhance battery life. **Retry**: The maximum number of times the WRI400 queries a PIM400 before it goes back to sleep. The number of retries should be slightly greater than the longest response time from the access control panel or host. Retries = [{Max Response Time of Panel - First } / Delay] +1	First: 300 msec. Delay: 200 msec. Retry: 5 times
	Degraded (Cache) Mode: Card Bit Format	Enter the number of bits on the cards being used to enable degraded mode.abilities. 0 = cache mode disabled	0
	Degraded (Cache) Mode: Full Card Number or Facility Code	Use the full card number or the facility codes of previously approved credentials in the Degraded (Cache) mode. Granting access is determined by "Full Card" content or just "Facility Code".	Full Card
	Degraded (Cache) Mode: Purge unused after 5 days	When enabled, deletes the cache entry after 5 days of non-use. If enabled, cards that have not accessed the lock within 5 days will be removed.	Disabled

WRI400

EDIT Tab (cont.)	Degraded (Cache) Mode: PIM485 Card Removal	PIM400 -485, -VBB ONLY Only displayed when a PIM400–485 is connected. If disabled, both ACP's refusing access (no access grant) and ACP's explicit deny access (Deny Access Command) will remove an entry. If enabled, only ACP's explicit deny access command will remove an entry from the cache.	Disabled
	Degraded (Cache) Mode: Clear Cache	Deletes all valid user credentials from the Degraded (cache) memory. Allows you to manually clear cache memory.	n/a
	Max Entries Stored	Number of credential cards or facility codes maintained in the cache. Minimum of 5, Maximum of 1000	125
	ACP Timeout	Time (in seconds) to wait before determining communication from the access control panel has failed.	10 seconds
	Wakeup Status	Displays the time, in seconds, the WRI400 listens for Wakeup on Radio broadcasts from its linked PIM400.	Disabled
	Strike Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (Needs to read a valid credential before changing the relay polarity.)	Normally Closed (Secure)
	Aux Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (The auxiliary relay polarity will change as soon as saved, a credential is not required.)	Normally Closed (Secure)
	Keys Buffered		4
	Reader 1 Facility Code		1
	Reader2 Facility Code		1

CT5000

	Property	**Description**
VIEW Tab	Lock Name	The name of the CT5000. Set by the door file programmed into the CT5000.
	Date & Time	Current date and time. Initialized/set by the HHD.
	General Properties	
	Model	Model number of the CT5000 connected to the HHD.
	Max Users	Number of Users supported by the CT5000.
	Max Audits	Number of audits supported by the CT5000.
	Power Status	Current voltage level of the Coin Cell battery.
	CT5000	
	Serial Number	Serial number that uniquely identifies the CT5000.
	Manufacture Date	Date the CT5000 was manufactured.
	Days Since Installed	Used for warranty purposes; marks the beginning of the CT5000 functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.

CT5000

	Property	Description	Default
EDIT Tab	Lock Type	Classroom: Unlocks when a credential is presented and then automatically locks after the relock delay has expired. The CT5000 can only be Classroom Type.	Classroom
	PIN Length	Maximum number of digits in the user PIN. Range of 3 to 6 digits.	6
	Ignore Keypad	If checked, key entry codes are ignored.	Disabled
	Relock Delay	Amount of time before the CT5000 relocks after being unlocked by a user presenting a valid credential or the Request to Exit being released.	3 seconds
	CT5000-Input Request to Exit: Active Open/Active Closed	This sets the polarity of the Request To Exit signal into the CT5000. Default is when the switch is closed and the CT5000 reads and reports a Request to Exit.	Active close
	CT5000-Input Reader Tamper 1: Active Open/Active Closed	This sets the polarity of the Reader 1 Tamper signal into the CT5000. Default is when the switch is closed and the CT5000 reads and reports a Reader 1 Tamper.	Active close
	CT5000-Input Reader Tamper 2: Active Open/Active Closed	This sets the polarity of the Reader 2 Tamper signal into the CT5000. Default is when the switch is closed and the CT5000 reads and reports a Reader 2 Tamper.	Active close
	Door Position Switch (DPS): Installed	If unchecked, the Door Position Switch (DPS) is disabled and the Door Prop Delay, Anti-Tailgate, Request to Exit Clears Alarm, and Alarm are also disabled. By default, the CT5000 assumes there is no Door Position Switch (DPS) connected.	Disabled
	Door Position Switch (DPS): Active Open/ Active Closed	This sets the polarity of the Door Position Switch (DPS) signal into the CT5000 (Open or Closed). Default is when the switch is closed and the CT5000 reads and reports the door closed.	Active Open
	Door Prop Delay	The Prop Delay setting is the time to allow the door to be held open before the alarm relay triggers the alarm.	30 seconds
	Door Prop Delay: Enabled/Disabled	When enabled, the alarm relay will activate after the door has been open more time than the number of seconds specified in the Door Prop Delay time.	Disabled
	Anti-Tailgate	Anti-Tailgate is designed to automatically relock the door when the door re-closes, no matter how much time is left on the relock delay (requires a Door Position Switch).	Disabled
	Request to Exit Clears Alarm	During an alarm event, enabling request to exit disables the alarm.	Disabled
	Alarm Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (The alarm relay polarity will change as soon as saved, a credential is not required.)	Normally Closed (Secure)
	Aux Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (The auxiliary relay polarity will change as soon as saved, a credential is not required.)	Normally Closed (Secure)
	Strike Relay: Normally Open (Secure) Normally Closed (Secure)	When Normally-closed (Secure), the normally-closed side of the relay is the secure side. (Needs to read a valid credential before changing the relay polarity.)	Normally Closed (Secure)
	Coin Cell Nuisance Delay		Enabled (checked)

CO-Series Locks

Supported Locks

All chassis for the following models are supported.

CO-Series Locks		
CO-200	CO-220	CO-250

Couple HHD to Lock

This function works with CO-Series devices only.

CO-Series locks can be coupled, or authenticated, with the HHD. This provides enhanced security by ensuring that the lock will only communicate with HHD to which it has been coupled. Once the lock has been coupled, the coupling password is passed to the device from the HHD during programming. Each lock will retain only one coupling password; therefore, only one HHD can be coupled with the lock.

The HHD will use a default Coupling Password (123456) when coupling with a device. The Coupling Password should be changed to provide increased security for your locks. See **Coupling Password** on page **18** for more information.

If a device is not in Coupling mode, SUS will display a device specific message with instructions for placing the device into Coupling mode.

➔ HHDs with the same coupling password can program the same devices. Each HHD with a different coupling password must be coupled with each device it will program.

1. Connect the HHD to the lock using the HH-USB cable.
2. Insert the mechanical key into the lock. Then rotate and hold the key.
3. Continue holding the key and press the Schlage button three (3) times. Then release the key.
4. On the HHD, select **Device Options**.
5. On the HHD, select **Couple HHD to Device**.
6. When Coupling is successful, a message will be displayed on the screen.

Program a Lock

1. Connect the HHD to the lock or controller and establish communication between the HHD and the device.
2. Select **Device Options**.
3. Select **Program Lock**.
4. Select the door file that should be associated with the lock or controller.

   ➔ Door files are downloaded to the HHD when synchronized with the access control software.
5. Select **OK**.

Collect Audits

Collecting audits on the HHD does not delete the audits from a lock.

Collected audits will be transferred from HHD to your Access Control Software the next time they are synchronized.

When Auto Update is enabled, as soon as the Schlage button is pressed twice and the communication with the Schlage Utility Software starts, the lock will automatically:

- update lock's date/time
- collect audits
- update access rights

When Manual Update is enabled, follow the steps below to collect audits and update the lock access rights.

➔ See **Update Mode** on page **18** for more information.

Collect Audits when Date/Time and Lock Access Rights are Up-to-Date

1 Confirm HHD is connected to lock.

➔ See **Connect the Handheld Device to the PC** on page **13** for more information.

2 Double-click the displayed name of the connected lock.

3 The audit collection will begin.

➔ If no previous audit exists, skip to step 7.

4 If a previous audit exists, a message will appear asking to overwrite previous audit. Click **YES** to override audits and skip to step 7.

5 Click **NO** if you do not want to override the audit.

6 Acknowledge the message advising to synchronize the lock with system software. Audit collection will be stopped.

7 A progress indicator will be displayed while the audit is being collected.
A message will be displayed once the process is complete.

Collect Audits when Date/Time and Lock Access Rights are Not Up-to-Date

1 Confirm HHD is connected to lock.

➔ See **Connect the Handheld Device to the PC** on page **13** for more information.

2 Double-click the displayed name of the connected lock.

3 When asked to update date and time of the device, click **YES**. A progress indicator will be displayed while date and time is being updated.

4 A message will appear to confirm the successful update.

5 The audit collection will begin. A progress indicator will be displayed while the audit is being collected.

6 The access rights update will begin. A progress indicator will be displayed while lock is being updated.

7 A message will be displayed once the process is complete.

View Properties

1 Connect the HHD to the lock or controller.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 The **View** tab will be displayed.

➔ See **Lock Properties** on page **60** for more information.

Edit Properties

1. Connect the HHD to the device.
2. Select **Device Options**.
3. Select **Properties** for the connected device.
4. Select the **Edit** tab.
5. Edit the properties as desired.
   ➔ See **Lock Properties** on page **60** for more information.
6. Select **Save** before exiting the tab.

View Reader Properties

1. Connect the HHD to the device.
2. Select **Device Options**.
3. Select **Properties** for the connected device.
4. Select the **Reader** tab.
   ➔ See **Lock Properties** on page **60** for more information.

Edit Reader Properties

1. Connect the HHD to the device.
2. Select **Device Options**.
3. Select **Properties** for the connected device.
4. Select the **Reader** tab.
5. Edit the properties as desired.
6. Select **Save** before exiting the tab.
   ➔ See **Lock Properties** on page **60** for more information.

Update Firmware

➔ See **AD-Series and CO-Series Device Firmware Update** on page **77** for more information.

Lock Properties

CO-200/220/250

	Property	Description
VIEW Tab	Lock Name	The name of the Lock. Set by the door file programmed into the lock.
	Date & Time	Current date and time. Initialized/set by the HHD.
	General Properties	
	Model	Model number of the device connected to the HHD.
	Max Users	Number of Users supported by the lock (CO-200/220)
	Max Void List	Number of void users supported by the lock (CO-250)
	Max Audits	Number of Audits supported by the lock.
	Power Status	Current voltage level of the AA and Coin Cell batteries.
	Main Lock	
	Serial Number	Serial number that uniquely identifies the lock.
	Manufacture Date	Date the lock was manufactured.
	Days since Installed	Used for warranty purposes; marks the beginning of the lock's functional life.
	Firmware Version	Version of the current firmware file. Automatically updated when new firmware file is loaded.
	Hardware Version	Current version of the printed circuit main board.
	Bootloader Version	Version of the current bootloader. Allows new firmware to be loaded.
	Credential Reader	
	Reader Type	Type of Reader installed: Keypad, MagInsert, MagSwipe, Proximity, and Keypad Variations

CO-200/220/250

	Property	Description	Default
EDIT Tab	Lock Type	**Classroom Security (CO-220 Only):** Allows lock to be placed into secure lockdown by the a paired fob. Once in lockdown, only a Passthrough credential can be used to gain access. **Office:** Unlocks when a credential is presented and then automatically locks after the relock delay has expired. To keep the door unlocked, push the button on the inside. The button will momentarily illuminate green. To return the lock to the locked state, push the button again or present a credential to the outside. **Privacy:** To initiate the Privacy function, with the door closed, push the button on the inside of the door. This prevents normal credentials from opening the door from the outside. The lock will go back to its normal state when the button is pushed again or when the door position switch indicates that the door has opened. When using a Mortise Deadbolt, extending the deadbolt from the inside lights a red LED on the inside trim and initiates the Privacy function which prevents normal credentials from opening the door from the outside. The lock can always be opened using a Pass-Through credential or mechanical key in case of emergency. **Storeroom:** Lockset is normally secure. Inside lever always allows free egress. Valid Toggle credentials may be used to alternate (toggle) the state of the lock between passage (unlocked) and secured (locked). Unlocks when a normal credential is presented and then automatically locks after the relock delay has expired.	Set by the Factory
	PIN Length (CO-200/220 only)	Maximum number of digits in the user PIN. Range of 3 to 6 digits.	6
	Allow Privacy Mode Override (CO-250 only)	When enabled, allows cards override a lock that has been placed in privacy mode. When disabled, only cards specifically assigned to this door will have access.	Disabled
	Ignore Keypad	If checked, key entry codes are ignored.	Disabled
	Record Lock/Unlock[1]	If checked and supported by the system software, will record an audit event when the Inside Push button is pressed.	
	Disable Interior Button LED[1]	If checked, interior button LED blinking is disabled.	Enabled (checked)
	Battery Fail Mode	Lock state set when battery fails. As-Is, Secure/Locked, Unsecure/Unlocked	As-Is
	Coin Cell Battery Nuisance Delay	Lock state set after coin cell battery replacement. If unchecked, nuisance delay is disabled.	Disabled (unchecked)
	Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential.	3
	ADA Delay (CO-250)	Amount of time before the lock relocks after being unlocked by a user who is flagged as handicapped and presenting a valid credential. Can be changed in the access control system.	30
READER Tab	**Property**	**Description**	**Default**
	Prox in Use	Proximity credential card types allowed. Selections: HID/KantechIO, GE/CACY, AWID	ALL selected
	Mag Track in Use	Magnetic card track that access data is to be read from. Track 1, 2 or 3 (Track 1 not configurable for CO-200)	Track 2
	Enable Low Power Wake-Up	Active when Mag Track 1 or 3 is selected in "Mag Track in Use". By enabling Low Power Wake-Up and recording data on track 2, this option will allow longer battery life.	Enabled
	Beeper	Indicates if the Beeper is on or off.	ON

[1] This feature is not available on the CO-220 Safe School Lock.

Legacy Locks and Controllers

Supported Legacy Locks		Supported Controllers	
KC2	BE367	Legacy PIM WRI* WPR* WPR2* WSM*	CT500/1000 Controller CL Campus Lock Controller
CM			
CL			

* These devices cannot be configured directly. They are configured through the Legacy PIM.

Program a Lock or Controller

All legacy devices use the serial connection type. Be sure to change the connection type option when connecting to a legacy device. See **Connection Type** on page **17** for more information.

See **Start the Schlage Utility Software** on page **15** and **Connecting the Handheld Device on page 20** for more information.

1. Connect the HHD to the lock using the HH-Serial Cable and CIP if using the BM150. Both the BM-150 and BM-170 can also use the HH-2PIN Serial Cable.
   ➔ See **Connecting the Handheld Device** on page **20** for more information.
2. Select **Device Options**.
3. Select **Program Lock**.
4. Select the door file that should be associated with the lock.
   ➔ Door files are downloaded to the HHD when synchronized with the access control software.
5. Select **OK**.
6. Wait for the screen asking for the programming credential. Then present the programming credential to the lock.
   ➔ The lock will flash red and green alternating several times, indicating it has entered programming mode.
   ➔ Consult the lock user guide that came with your lock for more information about programming mode.
7. Select **OK**. Lock programming will begin.

Collect Audits and Update a Lock

When Auto Update is enabled, as soon as the Schlage button is pressed twice and the communication with the Schlage Utility Software starts, the lock will automatically update lock's date/time, collect audits and update access rights.

When Manual Update is enabled, follow the steps below to collect audits and update the lock access rights.

➔ **See Update Mode on page 18 for more information.**

All legacy devices use the serial connection type. Be sure to change the connection type option when connecting to a legacy device. See **Connection Type** on page **17** for more information.

Collecting audits on the HHD does not delete the audits from a lock.

Collected audits will be transferred from HHD to your Access Control Software the next time they are synchronized.

Collect Audits when Date/Time and Lock Access Rights are Up-to-Date

1 Connect the HHD to the lock using the HH-Serial cable, CIP and serial connection type, if using the BM150.

2 Both the BM-150 and BM-170 can also use the HH-2PIN Serial Cable.

➔ **See Connecting the Handheld Device on page 20 for more information.**

3 Double-click the displayed name of the connected lock.

4 The audit collection will begin.

➔ If no previous audit exists, skip to step 7.

5 If a previous audit exists, a message will appear asking to overwrite previous audit. Click **YES** to override audits and skip to step 7.

6 Click **NO** if you do not want to override the audit.

7 Acknowledge the message advising to synchronize the lock with system software. Audit collection will be stopped.

8 A progress indicator will be displayed while the audit is being collected.
A message will be displayed once the process is complete.

Collect Audits when Date/Time and Lock Access Rights are Not Up-to-Date

1 Confirm HHD is connected to lock.

➔ **See Connecting the Handheld Device on page 20 for more information.**

2 Double-click the displayed name of the connected lock.

3 When asked to update date and time of the device, click **YES**.

4 When asked for a valid programming credential, present the credential and then click **OK**. A progress indicator will be displayed while date and time is being updated.

5 A message will appear to confirm the successful update.

6 When asked for a valid programming credential (second time), present the credential and then click **OK**. The audit collection will begin. A progress indicator will be displayed while the audit is being collected.

7 The access rights update will begin. A progress indicator will be displayed while lock is being updated.

8 A message will be displayed once the process is complete.

All legacy devices use the serial connection type. See **Connection Type** on page **17** for more information.

All legacy locks require the CIP if using the BM150. Both the BM-150 and BM-170 can also use the HH-2PIN Serial Cable. See **Connecting the Handheld Device** on page **20** for more information.

All non-lock legacy controllers require the null converter (PIMWA-CV). See **Connecting the Handheld Device** on page **20** for more information.

View Properties

1 Connect the HHD to the lock or controller.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 The **View** tab will be displayed.

➔ See **Lock Properties** on page **65** for more information.

Edit Properties

1 Connect the HHD to the lock or controller.

➔ See **Connecting the Handheld Device** on page **20** for more information.

2 Select **Device Options**.

3 Select **Properties** for the connected device.

4 Select the **Edit** tab.

5 Edit the properties as desired.

➔ See **Lock Properties** on page **65** for more information.

6 Select **Save**.

7 Wait for the screen asking for the programming credential. Then present the programming credential to the lock.

➔ The lock will flash red and green alternating several times, indicating it has entered programming mode.

➔ Consult the lock user guide that came with your lock for more information about programming mode.

8 Select **OK**. Lock properties will be saved.

Update Firmware

Consult the directions that came with your lock for information about entering programming mode.

1 Connect the HHD to the device you want to update.

➔ See **Connecting the Handheld Device** on page **20** for more information.

2 Select **Device Options**.

3 Select **Firmware Update**.

4 Select the desired firmware file from the list.

➔ Firmware updates are available at www.schlage.com/support to be downloaded to the computer that synchronizes with the HHD. See **Appendix B: Device Firmware Update on page 77** for details on how to obtain firmware files online and update to the HHD.

5 Select **OK** at the bottom of the screen.

6 Wait for the screen asking for the programming credential. Then present the programming credential to the device.

➔ The lock will flash red and green alternating several times, indicating it has entered programming mode.

➔ Consult the lock user guide that came with your lock for more information about programming mode.

7 Select **OK** to proceed when prompted.

8 A progress indicator will be displayed during the firmware update. A message will be displayed briefly once the firmware update is complete.

➔ Updating Lock firmware will require the user to reset the lock before proceeding. See **Appendix C: Change Lock Class** on page **85** for more information.

Link a Door to a Legacy PIM

1 Connect the HHD to the Legacy PIM. Both the BM150 and the BM-170 with HH-Serial Cable and with the null converter (PIMWA-CV) attached can be used.

➔ See **Connecting the Handheld Device** on page **20** for more information.

2 Select **Device Options**.

3 Select the **PIM Properties** button.

4 Select the **Link** tab.

5 Select the door you want to link from the **Door** drop-down list.

6 Select the **Link** button.

➔ Perform the necessary steps to place the appropriate wireless lock or controller into linking mode. See the user guide that came with the device for more information.

Diagnostics

Test Mode can be used for troubleshooting.

1 Connect the HHD to the controller.

➔ See **Connecting the Handheld Device** on page **20** for more information.

2 Select **Device Options**.

3 Select **Diagnostics**.

Lock Properties

Property	**Description**	**Editable?**
Lock Name	Name of the Lock Can be edited in the access control system.	No
Firmware Version	Version of the current firmware file Automatically updated when a new firmware version is loaded.	No
Date & Time	Current date and time Lock setting	Yes
Relock Delay	Amount of time before the lock relocks after being unlocked by a user presenting a valid credential	Yes
Prop Delay	Amount of time a door can be open before the prop delay alarm is activated	Yes

Troubleshooting

General Troubleshooting

If you are having trouble with the SUS and/or the handheld device, please check the following before contacting customer support:

Battery:

1 Make sure the handheld device has been charged.

2 Make sure the batteries in the lock are not depleted.

Cable:

3 The programming cable must be properly connected to the lock and the handheld device.

4 Make sure you are using the programming cable that came with the handheld device.

5 When programming a legacy device using the CIP, the CIP must be inserted in the correct orientation. See **Connecting the Handheld Device** on page **20** for more information.

Handheld Device (HHD):

6 Make sure you are using the correct connection type. See **Connection Type** on page **17** for more information. Both the BM-150 and the BM-170 can use serial communications with locks and controllers using the HH-Serial Cable and with the null converter (PIMWA-CV) attached with the Legacy PIM.

7 If the HHD is not responding to button presses or screen taps, be sure that the HOLD slider switch on the left side of the HHD (BM-150 ONLY), is not in the HOLD position.

8 If the HHD is not responding to screen taps, check to see if the Unlock selection is available at the bottom of the START screen. If the Unlock selection is present, tap on it to unlock the

9 If the HHD or SUS application appears to be hung up and not operating properly, RESET the (BM-150) HHD by removing the battery compartment cover and carefully press the RESET button in the lower right-hand corner. To RESET the (BM-170) press the RESET button located on the lower right-hand corner of the case.

PC and HHD:

10 If the HHD will not connect and synchronize with the PC, be sure the SUS application is not running and the PCs USB port is not in use by other applications.

11 If synchronizing with your PC takes a long time, be sure that the My Document folder does not have large files in it.

12 If you do not have firmware files available in the **Update Firmware** menu, be sure the files have been copied to the HHD root directory My Device.

System:

13 If the SUS is not running properly or is intermittent, be sure the HHD has adequate memory available.

14 Communication between PIM400 and Access Control Panel will not occur if the HHD is connected to either the AD-400 or the PIM400.

➔ Disconnect the HHD from hardware prior to testing system.

15 If the BM-170 goes to sleep while connected to a CO Lock, wake the device up and press the Schlage button four (4) times to resume communication.

Error Codes

No.	Error	Solution
E100	Enter a valid password	No password was entered. Enter the correct password.
E101	Incorrect password	The password entered was incorrect. Enter the correct password.
E102	Incorrect password entered three times. Wait for 30 seconds before next retry	An incorrect password was entered three times. Wait thirty (30) seconds. Then enter the correct password.
E103	The old password is incorrect	When attempting to change the password, the old password entered was incorrect.
E104	Password field cannot be left blank	When attempting to change the password, no password was entered.
E105	Password must be at least 4 characters	When attempting to change the password, the password entered was too short.
E106	Passwords do not match	When attempting to change the password, the second password entered did not match the first password entered.
E107	Old password and new password are identical	When attempting to change the password, both passwords are the same. The new password must be different.
	No Device Connected	The Options menu was tapped when no lock was connected to the HHD. Connect the HHD to a device and try again.
E201	This device is not connected	A device name, other than the device to which the HHD is currently connected, was selected and then the Options menu item was tapped. Options can be viewed only for the lock that is currently connected.
E202	Unrecognized device connected or incompatible SUS version. Please visit **www.schlage.com/support** to download the latest SUS version and try again	SUS is unable to recognize this device. The version of SUS on the handheld is currently incompatible with this device. Please visit **www.schlage.com/support** to download the latest SUS version and try again.
E300	Collecting audit failed	The HHD was disconnected from the lock before audit collection was complete. The HHD must remain connected to the lock until collection is complete.
E301	Synchronizing lock data failed	The HHD was disconnected from the lock before synchronization was complete. The HHD must remain connected to the device until synchronization is complete. OR No valid programming credential was presented to the lock. A valid programming credential must be presented before the device can be programmed.
E302	Updating lock's date and time failed	The HHD was disconnected from the lock before date/time update was complete. The HHD must remain connected to the device until date/time update is complete. OR No valid programming credential was presented to the lock. A valid programming credential must be presented before the date/time can be updated.
E303	Your HHD is not authenticated to perform this action. Couple HHD with the device to authenticate	This message appears when the device is not coupled with the HHD and an action requiring authentication was performed (feature change, firmware update, lock synchronization, etc.).

Error Codes

No.	Error	Solution
E304	Retrieving lock properties failed	The HHD was disconnected from the lock before the Retrieving Properties process was complete. The HHD must remain connected to the lock until the process is complete.
E305	Retrieving PIB properties failed	The HHD was disconnected from the PIB300 before the Retrieving Properties process was complete. The HHD must remain connected to the PIB300 until the process is complete.
E306	Retrieving PIM properties failed	The HHD was disconnected from the PIM400/401 or Legacy PIM before the Retrieving Properties process was complete. The HHD must remain connected to the PIM400/401 or Legacy PIM until the process is complete.
E307	Retrieving door properties failed	The HHD was disconnected from the Door before the Retrieving Properties process was complete. The HHD must remain connected to the Door until the process is complete.
E400	Data files for French language are missing	When attempting to change the language to French, the French language files cannot be found. Contact customer support.
E401	Data files for Spanish language are missing	When attempting to change the language to Spanish, the Spanish language files cannot be found. Contact customer support.
E500	Please set the Relock delay and Prop delay	The relock delay and prop delay must be greater than zero (0). Change the delay(s) to a value greater than zero (0).
	Lock1 and Lock2 address cannot be identical	The Save menu item was tapped but no values were changed. Change at least one value, or tap back to cancel.
E502	Saving properties failed	The HHD was disconnected from the lock before the saving properties function was complete. The HHD must remain connected to the lock until the saving properties process is complete. OR No valid programming credential was presented to the lock. A valid programming credential must be presented before the properties can be saved.
E503	The Unique ID should be in range 0 - 65535	The PIM400 or Legacy PIM address entered was greater than 65535. Enter a value less than 65535 and try again.
E504	The Unique ID should be in range 1-65534	The PIM400 or Legacy PIM address is incorrect. Enter a value less than 65535 and try again.
E505	The RS485 address should be in range 0- 254	The RS485 address entered was greater than 254. Enter a value less than 254 and try again.
E506	The Relock Delay value should be in range 0- 255	The Relock Delay entered was greater than 255. Enter a value less than 255 and try again.
E507	Reserved address 170 cannot not be used for RS485 address	The RS485 address entered is incorrect. Enter a value less than 254 and different than 170.
E508	Difference between high door and low door cannot be equal or greater than 16	While setting the addresses of the Low and High doors make sure that the difference between both is less than 16.
E509	High door cannot be lesser than low address	The address of the High door MUST be greater than the Low door.

Error Codes

No.	Error	Solution
E510	The ADA Delay value should be in range 0- 255	The ADA Delay entered was greater than 255. Enter a value less than 255 and try again.
E600	Please select the firmware file	No firmware file was selected before the OK menu item was tapped when attempting to update the lock's firmware. Select a firmware file and try again.
E601	Updating firmware failed	The HHD was disconnected from the lock before the firmware update was complete. The HHD must remain connected to the lock until the firmware update is complete.
		No valid programming credential was presented to the lock. A valid programming credential must be presented before the firmware update can be done.
		SUS may need to be updated in order to perform firmware updates to this device. Please check www.schlage.com/support for the latest version.
E602	No files to select	The HHD does not have any files to select from or they were put in the incorrect folder.
E603	File integrity check failed	While updating Firmware or Programming a lock, the SUS software detected that the file being used is corrupted. Download/Create the file again and upload it into the HHD.
E604	Cannot open file	
E605	Cannot read file	
E606	Invalid file	
E607	Please select the lock class file	While attempting to change a lock class, inside the Firmware Package Screen – no selections were made. Select a lock class and try again.
E700	Please select the door	While attempting to program a lock, no door was selected. Select a door and try again.
E701	Programming lock failed	The HHD was disconnected from the lock before the lock setup was complete. The HHD must remain connected to the lock until the lock setup is complete.
		No valid programming credential was presented to the lock. A valid programming credential must be presented before the lock can be set up.
E702	The door file is invalid due to incorrect data present; for example, blank lines. This can occur for multiple reasons, including manually editing the door file.	Use SMS to regenerate the door file & load the new door file into the SUS. Then retry programming.
E703	Door file contains invalid data for the AD200 lock model. Verify the correct lock and door files are selected or regenerate the door file and try again. Click OK to continue.	The Doorfile used contains IButton Data. This data is not valid for an AD200 Lock. Ensure the correct door/doorfile is selected or regenerate the doorfile.
E704	The selected Door file contains format errors. Click OK to Continue or Cancel to exit and try again using a new door file.	The doorfile contains errors that may interfere with normal operation. Programming is allowed to proceed if OK is selected. It is recommended that the doorfile be generated again by the access software in order to ensure the expected function of the lock.

Error Codes

No.	Error	Solution
E800	Device is not in coupling mode	AD series: Hold down the Interior Push Button and press the Tamper switch (sw1) 3 times. PIM400/PIB300 devices: Hold down LINK1 switch (s2) and press LINK2 switch (s3) 3 times. CO Series: Rotate mechanical key and hold while pressing Schlage button 3 times. WRI400/CT5000 devices: Hold down the SCHLAGE switch (s1) and press the LINK switch (s2) 3 times. WPR400: Hold down the IPB switch (s2) and press the TMP switch (s3) 3 times. While trying to couple the HHD with the device, the message pops up when the connected device was not in coupling mode. Follow the instructions to put the connected device in coupling mode and try again.
E801	Lock not responding correctly	Verify cable is properly connected to lock. If trying to program, verify Program Mode has been entered properly. If programming a KC-2 Deadbolt for the first time be sure the latch bolt is retracted. While communicating with the lock, the SUS has detected some problems, follow the presented instructions to correct the problem.
E802	Device does not support this action	
E810	Saving from device failed.	Please try again.
E900	Cannot open or read file	SUS was not able to read this file. If this was a firmware package, SUS is currently incompatible with this firmware package. Please visit www.schlage.com/support to download the latest SUS version and try again.

Remove the Schlage Utility Software

This process will remove the Schlage Utility Software from the handheld device.

1. On your handheld device, tab the **Start** menu.
2. Select **Settings**.
3. Select the **System** tab.
4. Select the **Remove Programs** icon.
5. Select to select the **Schlage Universal Software** in the list.
6. Select the **Remove** button.
7. Select the **Yes** button.

   ➔ To reinstall the SUS, see **Install/Update Schlage Utility Software on page 13.**

Glossary

BCD

Acronym for Binary Coded Decimal, an encoding method for representing decimal numbers where each digit is represented by four bits.

CAC

Acronym for Common Access Card, a U.S. Department of Defense smart card issued as standard identification, and for access to computers, networks and some facilities.

Cache Mode

How the reader will handle stored card information if there is loss of communication to its controller.

Card Conversion

Card data filters and converters that provide data that can be accepted by the access control system.

CM Lock

A Computer Managed offline lock, for example the Schlage CM 5500 series.

CSN

Acronym for the Card Serial Number, a unique, unencrypted identification number contained on the integrated chip in each smart card.

DCS

Acronym for Dynamic channel switching - can be selected to decrease the chance of interference but will decrease battery life.

Delay

The idle time between subsequent queries. - Shorter delays may reduce latency. - Longer delays may enhance battery life.

Door Prop Delay

The time allowed between opening a Door and closing it. If the Door is open longer then the Door prop delay an alarm is released. The delay can be set individually for each Door and is programmed through the program files.

Extend Unlock

This setting is required to respond to scheduled unlocks from an access control panel.

Fail Safe/Secure

The condition of a lock or latch when a loss of RF communications occurs between the PIM400/401 or Legacy and an access point.

FASC-N

Acronym for Federal Agency Smart Credential Number, an identifier used on all government issued credentials.

FC Mode

Allows access by Facility (Site) code.

First

The first query an access point makes to a PIM400/401 or Legacy PIM occurs immediately following a card swipe. - "First" is the amount of time, in milliseconds, an access point should wait before making its second query to a PIM400/401 or Legacy. This setting should be slightly greater than the fastest response time from the access control panel or host. This optimizes battery life and system performance.

GUI

Acronym for Graphical User Interface.

Heartbeat

The time interval that access points communicate to PIM400/401 or Legacy PIM when there is no activity. Affects battery life.

Hi Lo Output

These settings control the PIM400/401-TD2 open collector outputs sent to an access control panel on detection of Request-to-Exit (RTX), Door Position Switch (DPS), and Trouble. The WPIM switches these signals between an open collector and ground state.

Latch Type

Configuration of an access point depending on lock or latch type issued or used.

Mode

Configuration of an access point for standard operation or for factory testing.

No Purge

Reader will remember the first 20 cards swiped for degraded mode access.

PIM

Acronym for Panel Interface Module.

PIV

Acronym for Personal Identification Verification, refers to control and security standards set by the National Institute of Standards and Technology (NIST) for Federal employees and long-term contractors.

Relatch Time

The interval between the unlocking and relocking of an access point. Controlled by the access point, not the host system.

Relock delay

The time span from unlocking a lock after presenting a Credential until relocking. The relock delay can be set for each Door individually between 1 and 254 seconds. The relock delay setting is transferred to the lock through the program file.

TSA

Acronym for Transportation Security Administration.

TSM

Acronym for Transaction Status Message.

TWIC

Acronym for Transportation Worker Indentification Credential.

Request to Exit

Whenever a Door is opened from the safe side a request to exit is required. In the simplest version this means operating a mechanism that unlocks the door (for example turning the doorknob). Most electronic locks use a switch to detect a request to exit. This can be a passive infrared sensor, a push button, an electronic exit bar, or the doorknob contact itself. This switch has either a normally open or a normally closed contact. Based on this configuration the system has to be set up correctly, otherwise a request is permanently reported unless someone activates the switch.

Retry

The maximum number of times an access point queries a PIM400/401 or Legacy PIM before the access point goes back to sleep The number of retries should be slightly greater than the longest response time from the access control panel or host.

Rxt

Determines whether the access point module queries for unlock authorization on a Request to Exit activation.

Rxt Sift

Determines whether a WA56XX or WA993 reports Request to Exit activations in unlocked state.

UID

Acronym for the Unique Identifier, a unique, unencrypted identification number contained on the integrated chip in each smart card. (May also be referred to as CSN.)

WAPM

Acronym for Wireless Access Point Module.

Appendix A: SUS Update Guide

Follow the steps listed on this guide to update your SUS software to the latest version provided.

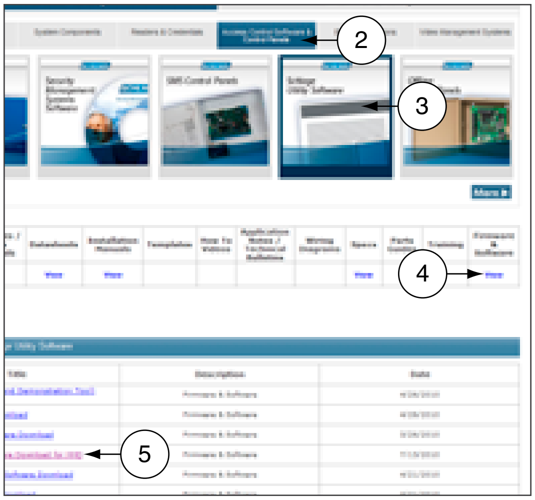
1 Browse to **www.schlage.com/support**.

2 Click the **Access Control Software & Control Panels** tab.

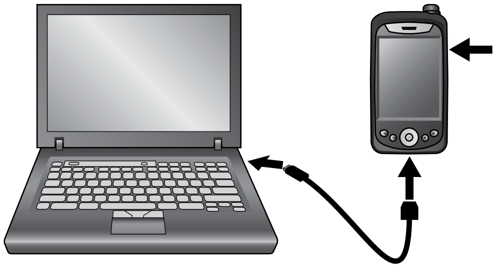
3 Click **Schlage Utility Software**.

4 Click **View** under the **Firmware & Software** column

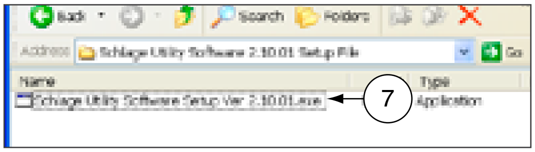
5 Click **Schlage Utility Software Download for HHD** and save the “Schlage Utility Software Setup File.zip” file to your computer.



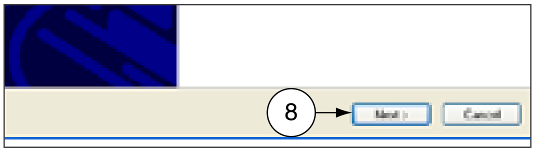
6 Turn ON the Hand Held Device (HHD) and connect it to the computer.



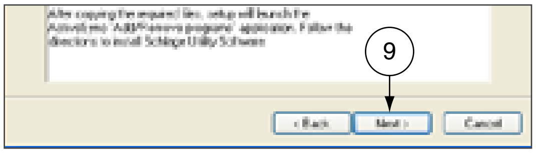
7 Open “Schlage Utility Software Setup File.zip” (see step 5) and double-click **Schlage Utility Software Setup Ver X.X.X.exe** (version number may vary). Then click **Run**.


Back
Search
Folders
Address
Schlage Utility Software 2.10.01 Setup File
Go
Name
Type
Schlage Utility Software Setup Ver 2.10.01.exe
Application
7

8 Click the **Next** button when the welcome screen appears.

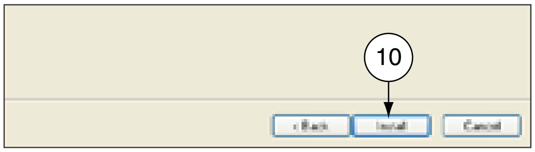


9 Click the **Next** button after reading the information screen.

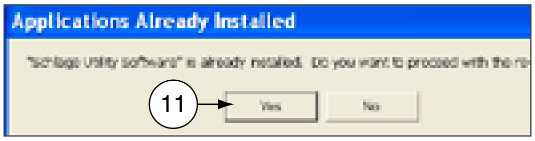


After copying the required files, setup will launch the ActiveSync 'Add/Remove programs' application. Follow the directions to install Schlage Utility Software

10 Click the **Install** button to start installation.



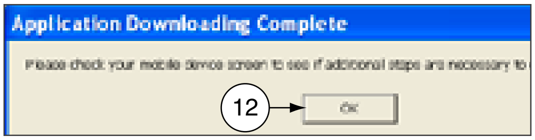
11 If the SUS is already installed a message will warn you about the upgrade, click the **Yes** button to continue. The installation will start.



Applications Already Installed

"Schlage Utility Software" is already installed. Do you want to proceed with the re

12 Click the **OK** button, when prompted to check your Hand Held Device (HHD).

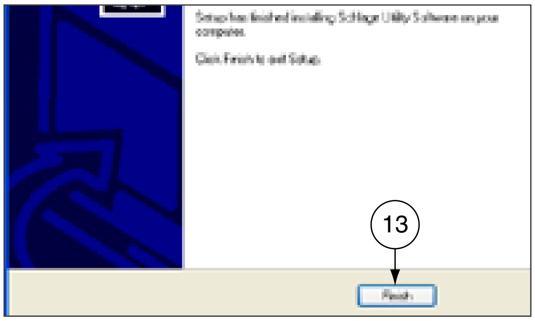


Application Downloading Complete

Please check your mobile device screen to see if additional steps are necessary to

13 Click the **Finish** button to complete the first stage, and then check the HHD for the final steps.

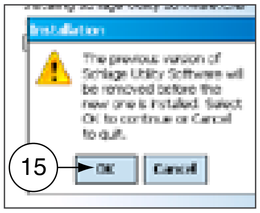
14 On the Hand Held Device (HHD) check if you received a message stating that the software is from an unknown publisher, click the **Yes** button to continue the installation or jump to the next step if you don't receive the message.



Setup has finished installing Schlage Utility Software on your computer.

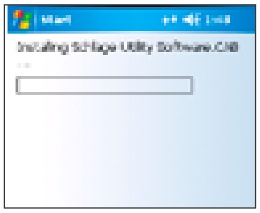
Click Finish to exit Setup.

15 On the Hand Held Device (HHD) a prompt message will appear asking if you'd like to remove the previous version, click the **OK** button to continue. The installation will start on the Hand Held Device (HHD)



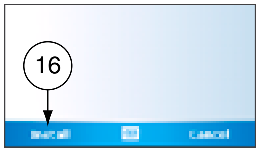
Installation

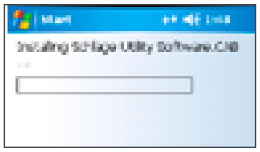
The previous version of Schlage Utility Software will be removed before the new one is installed. Select OK to continue or Cancel to quit.



Installing Schlage Utility Software.CAB

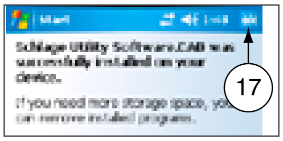
16 A screen prompting for the correct location to install the software will appear; Select: **\ProgramStore** and click **Install**. The installation will continue.





Installing Schlage Utility Software.CAB

17 Click the <**OK**> button on the right top of the screen to close the successfully installed message.

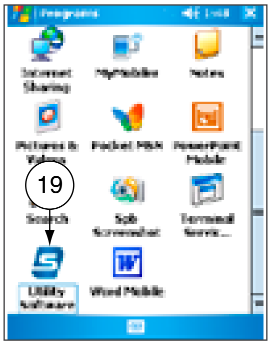


Schlage Utility Software.CAB was successfully installed on your device.

If you need more storage space, you can remove installed programs.

18 Before launching the Schlage Utility Software on the HHD disconnect it from the computer.

19 On the HHD Go to **Start -> Programs** and double click on the <**Utility Software**> icon to start the Schlage Utility Software (SUS). You'll see a welcoming screen with the actual software version.



➔ Important note: The SUS and the HHD pairing passwords are back to their default values (123456). If your pairing password was different than the default, you would need to change it before trying to reconnect to your device.

20 Change the Coupling Password.

➔ See **Coupling Password** on page **18** for more information.

Appendix B: Device Firmware Update

AD-Series On-Line Devices: Over Network Reprogramming (ONR).

Supported Products

PIM400-485-RSI, PIM400-485-VBB, AD-300/301 when wired by RS-485 to the ACP, AD-400/401 when linked to a PIM400-485. Devices must have been updated to A.D.A.60 or later for ONR to be available.

This feature must be provided by the Access Control Software Partner. Talk to your Access Control Provider for more details.

AD-Series and CO-Series Device Firmware Update

Windows XP

Prerequisites

- ActiveSync should be installed on your PC.

  ➔ See **Synchronization Software** on page **9** for more information.

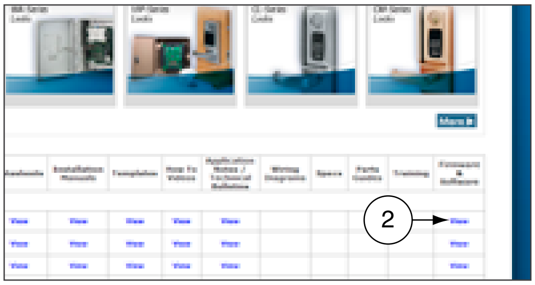
- HHD should have a partnership with ActiveSync.
- HHD should be already coupled with AD-Series device to be updated.

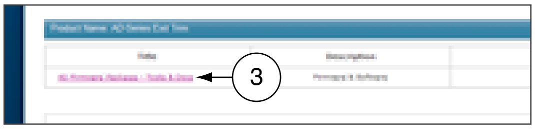
  ➔ See **"Couple HHD to Lock"** or **"Couple HHD to PIM400 or PIB300"** for more information.

1 Browse to **www.schlage.com/support**.

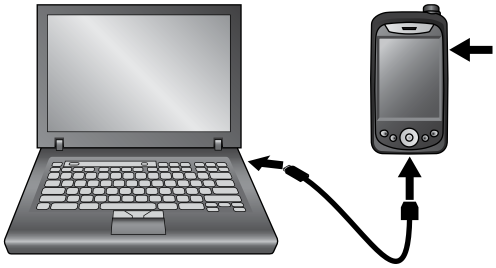
2 Click **View** under the **Firmware & Software** column

3 Click **AD Firmware Package - Tools & Docs** and save the "AD Firmware Pkg.zip" file to your computer.

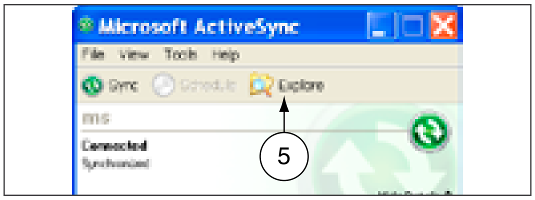




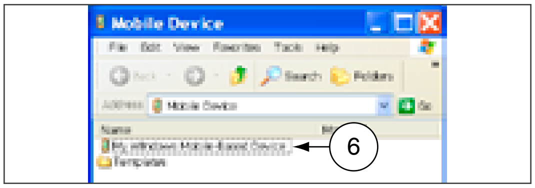
4 Turn on the HHD and connect it to the computer. The Microsoft ActiveSync window will automatically appear.



5 In the Microsoft ActiveSync window, click on the **Explore** button to open the HHD **Mobile Device** folder.



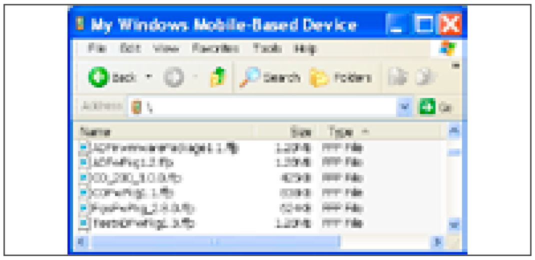
6 Double click on **My windows Mobile-Based Device** to go to the root directory of the HHD.



7 Copy the ".ffp" firmware file available inside the "AD firmware Pkg.zip" file (see step 3) and paste it inside the root folder **<My Windows Mobile-Based Device>**.

8 Wait for the HHD to synchronize.

9 Disconnect the HHD from computer.


My Windows Mobile-Based Device
File Edit View Favorites Tools Help
Back Search Folders
Address \
Go
Name Size Type

10 Go to the device and connect the HHD.

➔ See **Connecting the Handheld Device** on page **20** for more information.

11 Start the Schlage Utility software.

➔ See **Start the Schlage Utility Software** on page **15** for more information.

12 Login as a Manager.

➔ See **Log in as a Manager** on page **16** for more information.

13 Click **Device Options** at the bottom of the screen.

14 Click **Firmware Update**.

15 Select the firmware package you would like to use and click **OK**.

16 A message asking for confirmation to start programming the firmware will appear. Click **YES**.

17 The updating process will begin. The device will then restart. After a few minutes, a message indicating the firmware update was successful will appear.

18 Click **OK**.

➔ If the credential reader was changed, a factory default reset is recommended. See the user manual that came with the device for more information. WARNING: A factory default reset will delete all door information from the lock.

Windows 10, Windows 8, Windows 7 and Windows Vista

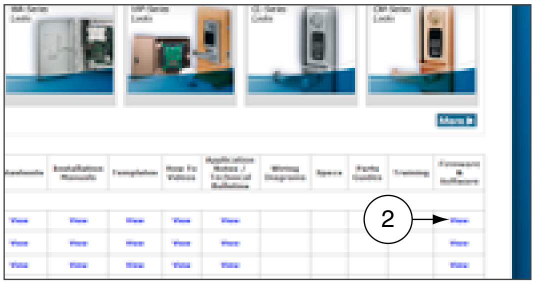
Prerequisites

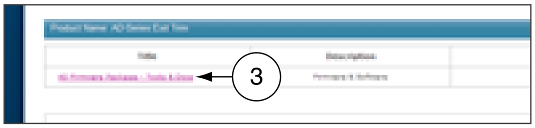
- Microsoft Windows Mobile Device Center should be installed on your PC.
  - ➔ See **Synchronization Software** on page **9** for more information.
- HHD should have a partnership with Windows Mobile Device Center.
- HHD should be already coupled with AD-Series device to be updated.
  - ➔ See **"Couple HHD to Lock"** or **"Couple HHD to PIM400 or PIB300"** for more information.

1 Browse to **www.schlage.com/support**.

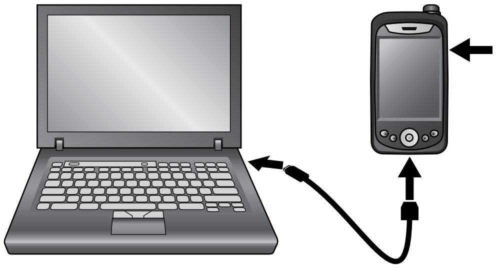
2 Click **View** under the **Firmware & Software** column.

3 Click **AD Firmware Package - Tools & Docs** and save the "AD Firmware Pkg.zip" file to your computer.

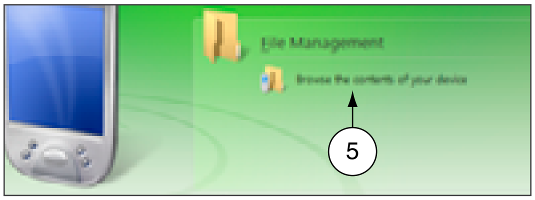




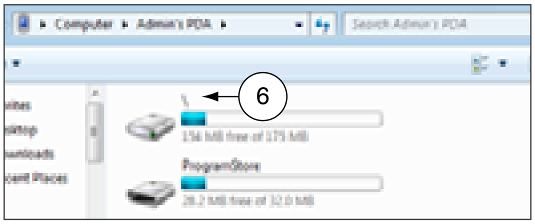
4 Turn on the HHD and connect it to the computer. The Microsoft Windows Mobile Device Center window will automatically appear.



5 In the Microsoft Windows Mobile Device Center window, click on **File Management** and then **Browse the contents of your device** to open the HHD device contents.



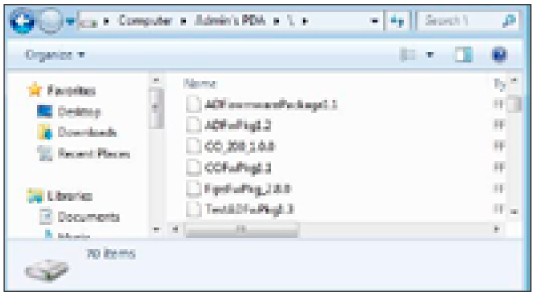
6 Double click on **** to go to the root directory of the HHD.



7 Copy the ".ffp" firmware file available inside the "AD firmware Pkg.zip" file (see step 3) and paste it inside the root folder (****).

8 Wait for the HHD to synchronize.

9 Disconnect the HHD from computer.



➔ NOTE: The SUS will prevent a user from reprogramming a device if batteries are too low and give the warning saying, "The voltage level to complete the firmware update is too low, you must replace the AA batteries and try again." The battery threshold requirements are as follows:

CO locks	All locks	4.7V
AD locks running firmware older than AD.A.50	8 battery locks	8V
	4 battery locks	5.5V
AD locks running firmware AD.A.50 or greater	8 battery locks	7.2V
	4 battery locks	4.7V

10 Go to the device and connect the HHD.

➔ See **Connecting the Handheld Device** on page **20** for more information.

11 Start the Schlage Utility software.

➔ See **Start the Schlage Utility Software** on page **15** for more information.

12 Login as a Manager.

➔ See **Log in as a Manager** on page **16** for more information.

13 Click **Device Options** at the bottom of the screen.

14 Click **Firmware Update**.

15 Select the firmware package you would like to use and click **OK**.

16 A message asking for confirmation to start programming the firmware will appear. Click **YES**.

17 The updating process will begin. The device will then restart. After a few minutes, a message indicating the firmware update was successful will appear.

18 Click **OK**.

➔ If the credential reader was changed, a factory default reset is recommended. See the user manual that came with the device for more information. WARNING: A factory default reset will delete all door information from the lock.

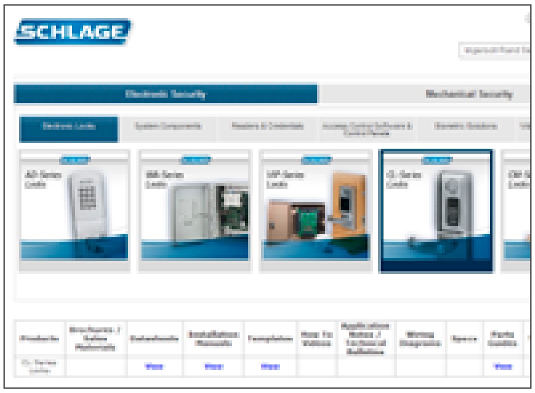
Legacy Device Firmware Update

Windows XP

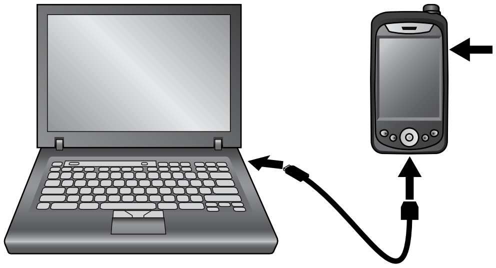
Prerequisites

- ActiveSync should be installed on your PC.
  ➔ See **Synchronization Software** on page **9** for more information.
- HHD should have a partnership with ActiveSync.

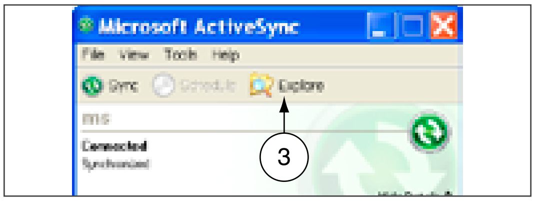
1 Browse to **www.schlage.com/support**. Select the legacy product and click **View** under the **Firmware & Software** column. Download the latest firmware to your computer.



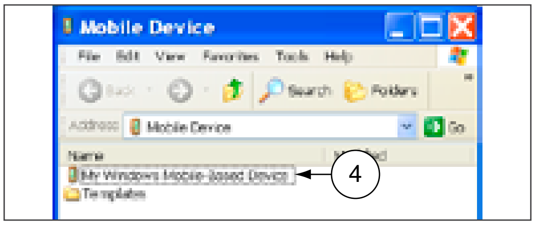
2 Turn on the HHD and connect it to the computer. The Microsoft ActiveSync window will automatically appear.



3 In the Microsoft ActiveSync window click on the **Explore** button to open the HHD **My Documents** folder.



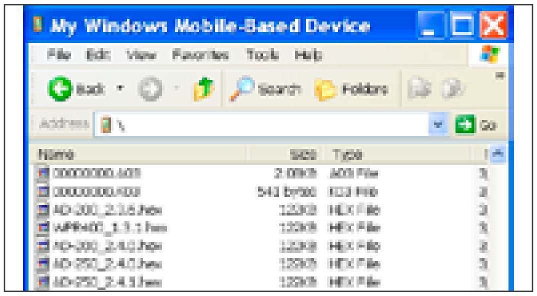
4 Double click on **My windows Mobile-Based Device** link to go to the root directory of the HHD.



5 Copy the ".s19" firmware file available inside the .zip file (see step 1) and paste it inside the **My Windows Mobile-Based Device** folder.

6 Wait for HHD to synchronize.

7 Disconnect the HHD from computer.


My Windows Mobile-Based Device
File Edit View Favorites Tools Help
Back
Search
Folders
Address
\
Go

Name	Size	Type
00000000.A01	2.00KB	A01 File
00000000.K03	541 bytes	K03 File
AD-200_2.3.6.hex	122KB	HEX File
WPR400_1.1.1.hex	122KB	HEX File
AD-200_2.4.0.hex	122KB	HEX File
AD-250_2.4.0.hex	122KB	HEX File
AD-250_2.4.1.hex	122KB	HEX File

8 Go to the device and connect the HHD.

➔ See **Connecting the Handheld Device** on page **20** for more information.

9 Start the Schlage Utility software.

➔ See **Start the Schlage Utility Software** on page **15** for more information.

10 Login as a Manager.

➔ See **Log in as a Manager** on page **16** for more information.

11 Click **Device Options** at the bottom of the screen.

12 Click **Firmware Update**.

13 Select the firmware file you would like to use and click **OK**.

14 Present a valid programming credential to the device and click **OK**.

15 The updating process will begin. The device will then restart. After a few seconds, a message indicating the firmware update was successful will appear.

16 Click **OK**.

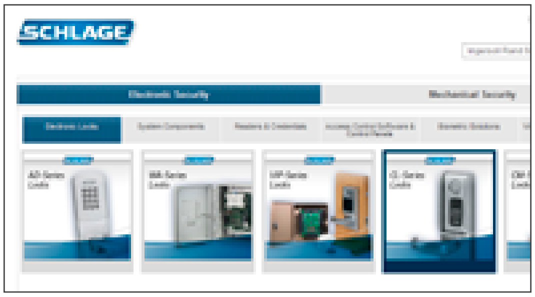
17 Reset the device to factory defaults before any additional programming. See the user manual that came with the device for more information.

Windows 10, Windows 8, Windows 7 and Windows Vista

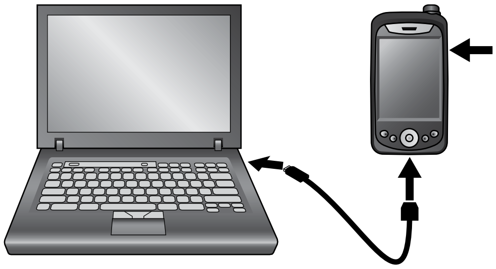
Prerequisites

- Microsoft Windows Mobile Device Center should be installed on your PC.
  ➔ See **Synchronization Software** on page **9** for more information.
- HHD should have a partnership with Windows Mobile Device Center.

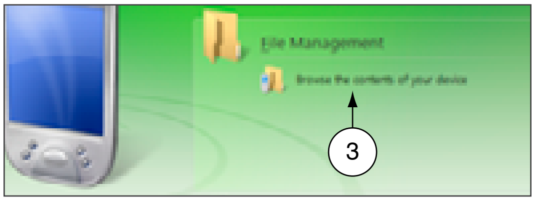
1 Browse to **www.schlage.com/support**. Select the legacy product and click **View** under the **Firmware & Software** column. Download the latest firmware to your computer.



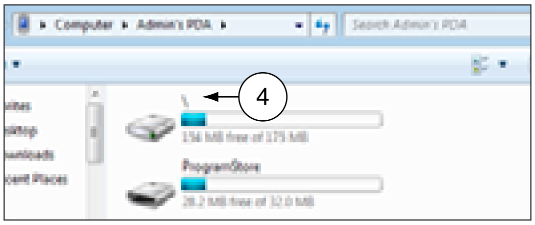
2 Turn on the HHD and connect it to the computer. The Microsoft Windows Mobile Device Center window will automatically appear.



3 In the Microsoft Windows Mobile Device Center window click on **File Management** and then **Browse the contents of your device**.



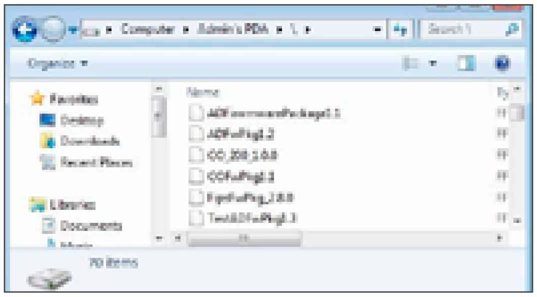
4 Double click on \ link to go to the root directory of the HHD.



5 Copy the ".s19" firmware file available inside the .zip file (see step 1) and paste it inside the root folder (\).

6 Wait for HHD to synchronize.

7 Disconnect the HHD from computer.



8 Go to the device and connect the HHD.

➔ See **Connecting the Handheld Device** on page **20** for more information.

9 Start the Schlage Utility software.

➔ See **Start the Schlage Utility Software** on page **15** for more information.

10 Login as a Manager.

➔ See **Log in as a Manager** on page **16** for more information.

11 Click **Device Options** at the bottom of the screen.

12 Click **Firmware Update**.

13 Select the firmware file you would like to use and click **OK**.

14 Present a valid programming credential to the device and click **OK**.

15 The updating process will begin. The device will then restart. After a few seconds, a message indicating the firmware update was successful will appear.

16 Click **OK**.

17 Reset the device to factory defaults before any additional programming. See the user manual that came with the device for more information.

Appendix C: Change Lock Class

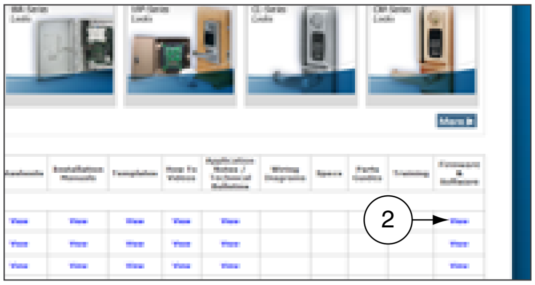
AD-Series Locks

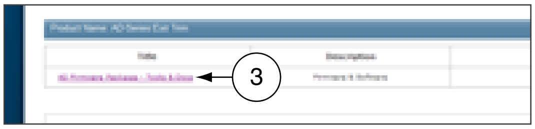
Windows XP

Prerequisites

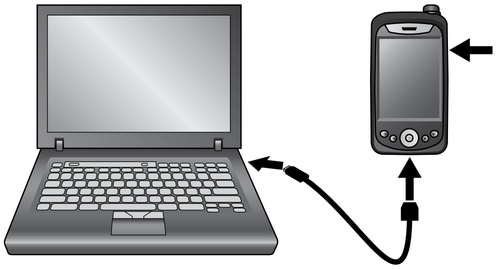
- ActiveSync should be installed on your PC.
  ➔ See **Synchronization Software** on page **9** for more information.
- HHD should have a partnership with ActiveSync.
- HHD should be already coupled with AD-Series device to be updated.
  ➔ See **"Couple HHD to Lock"** for more information.

1. Browse to **www.schlage.com/support**.
2. Click **View** under the **Firmware & Software** column.
3. Click **AD Firmware Package - Tools & Docs** and save the "AD Firmware Pkg.zip" file to your computer.

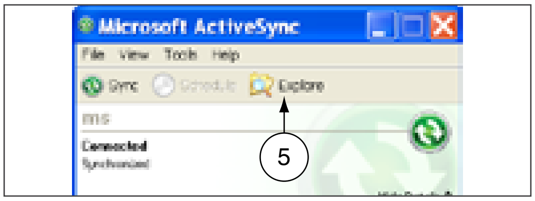


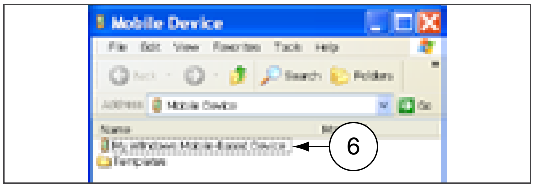


4. Turn on the HHD and connect it to the computer. The Microsoft ActiveSync window will automatically appear.

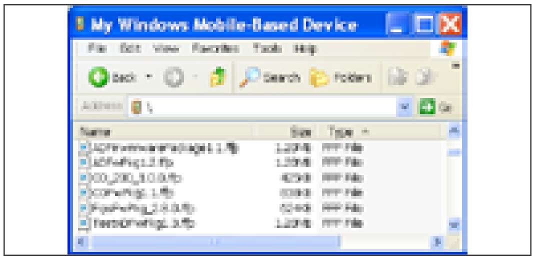


5. In the Microsoft ActiveSync window, click on the **Explore** button to open the HHD **Mobile Device** folder.





6 Double click on **My windows Mobile-Based Device** to go to the root directory of the HHD.


My Windows Mobile-Based Device
File Edit View Favorites Tools Help
Back Search Folders
Address \ Go
Name Size Type

7 Copy the ".ffp" firmware file available inside the "AD firmware Pkg.zip" file (see step 3) and paste it inside the root folder **<My Windows Mobile-Based Device>**.

8 Wait for the HHD to synchronize.

9 Disconnect the HHD from computer.

10 Go to the lock and connect the HHD.

➔ See **Connecting the Handheld Device** on page **20** for more information.

11 Start the Schlage Utility software.

➔ See **Start the Schlage Utility Software** on page **15** for more information.

12 Login as a Manager.

➔ See **Log in as a Manager** on page **16** for more information.

13 Click **Device Options** at the bottom of the screen.

14 Click **Change Lock Class**.

15 Select the firmware package you would like to use and click **Next**.

16 All available lock classes are displayed on the screen. Select the appropriate lock class and then click **OK**.

➔ Only locks with a magnetic reader can be changed to AD-250.

17 A message asking for confirmation to change the lock class will appear. Click **Yes**.

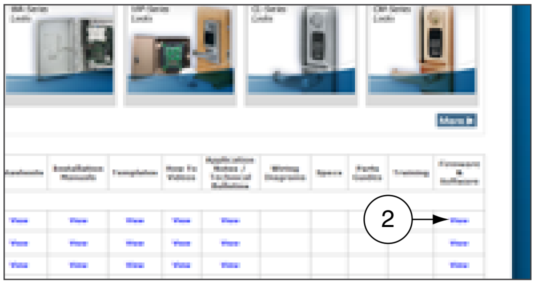
18 The change process will begin. Wait for the lock to restart. Once the confirmation message appears, the process is complete. Click **OK**.

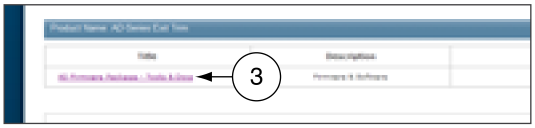
Windows 10, Windows 8, Windows 7 and Windows Vista

Prerequisites

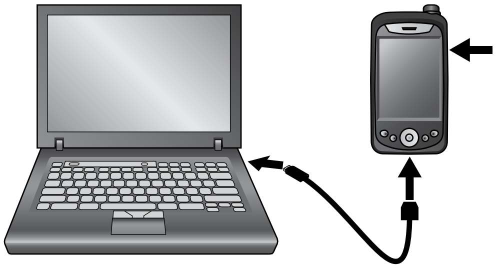
- Microsoft Windows Mobile Device Center should be installed on your PC.
  ➔ See **Synchronization Software** on page **9** for more information.
- HHD should have a partnership with Windows Mobile Device Center.
- HHD should be already coupled with AD-Series device to be updated.
  ➔ See **"Couple HHD to Lock"** or **"Couple HHD to PIM400 or PIB300"** for more information.

1. Browse to **www.schlage.com/support**.
2. Click **View** under the **Firmware & Software** column.
3. Click **AD Firmware Package - Tools & Docs** and save the "AD Firmware Pkg.zip" file to your computer.

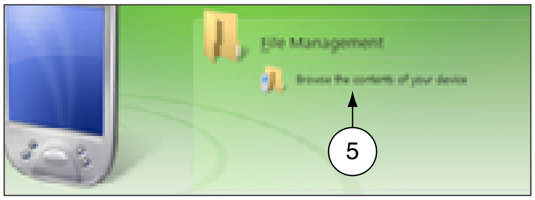




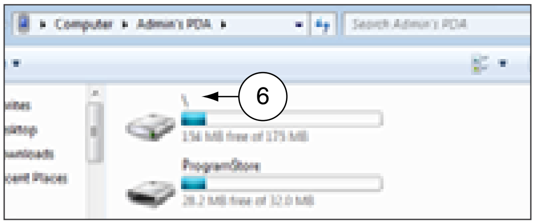
4. Turn on the HHD and connect it to the computer. The Microsoft Windows Mobile Device Center window will automatically appear.



5. In the Microsoft Windows Mobile Device Center window, click on **File Management** and then **Browse the contents of your device** to open the HHD device contents.



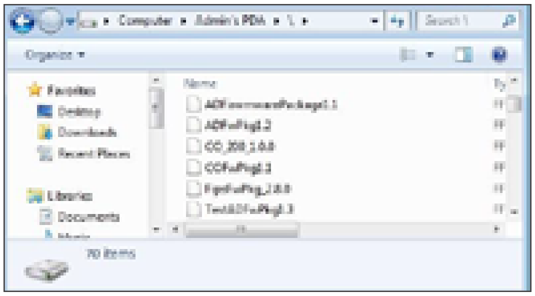
6. Double click on \ to go to the root directory of the HHD.



7 Copy the ".ffp" firmware file available inside the "AD firmware Pkg.zip" file (see step 3) and paste it inside the root folder (****).

8 Wait for the HHD to synchronize.

9 Disconnect the HHD from computer.



10 Go to the lock and connect the HHD.

➔ See **Connecting the Handheld Device** on page **20** for more information.

11 Start the Schlage Utility software.

➔ See **Start the Schlage Utility Software** on page **15** for more information.

12 Login as a Manager.

➔ See **Log in as a Manager** on page **16** for more information.

13 Click **Device Options** at the bottom of the screen.

14 Click **Change Lock Class**.

15 Select the firmware package you would like to use and click **Next**.

16 All available lock classes are displayed on the screen. Select the appropriate lock class and then click **OK**.

➔ Only locks with a magnetic reader can be changed to AD-250.

17 A message asking for confirmation to change the lock class will appear. Click **Yes**.

18 The change process will begin. Wait for the lock to restart. Once the confirmation message appears, the process is complete. Click **OK**.

19 Perform a Factory Default Reset of the lock before further use or programming.

➔ See the user manual that came with the device for more information.

Appendix D: Device Template

About Device Template Feature

The Schlage Utility Software (SUS) version 4.10.2 (or higher) includes the Device Template feature.

Users may quickly change and copy "Device Properties" settings across multiple devices so that a group of devices may have the exact same settings applied.

A Device Template file may be initiated from and copied to locks and devices, saved on the HHD, transferred to another HHD, and saved to a computer or network drive.

Supported Locks and Controllers

AD-200

AD-250

AD-300

AD-400

WRI400

WPR400

CT5000

PIB300

PIM400-TD2

PIM400-485

CO-200

CO-220

CO-250

Prerequisites

- The HHD used must be coupled before the Device Template file may be saved or retrieved. See **Couple HHD to Lock** on page **24** for more information.
- The "source" lock or device must be installed and working as desired with all property settings configured as required by the user.
- The Device Template file can be saved and restored for a **specific hardware class only.** For example:
  - ➔ A Device Template created from an AD-200 Mag Swipe lock will not be available when the SUS is communicating with an AD-200 Prox lock.
  - ➔ A Device Template created from an AD-200 Prox lock will not be available with an AD-300 Prox lock.

Saving a Device Template will also capture the following device status parameters:

- Lock Firmware Version
- Reader Firmware Version
- Lock Serial number
- Reader Serial number
- Boot Loader Version
- Days Since Installed
- AA Battery Pack Type
- AA Battery Voltage
- Coin Cell Voltage

This information is saved within the Device Template file, and can be viewed with any text viewer by the user.

When naming the Device Template, use normal Windows OS naming conventions.

Create a Device Template

1 Connect the HHD to the device with desired properties.

➔ If the device properties have not been programmed, configure the device properties as desired. Refer to AD-Series **Lock Properties** on page **31**, or CO-Series **Lock Properties** on page **60**.

2 Select **Device Options**.

3 Select **Lock Properties** for the connected device.

4 Select the **Edit** or **Reader** tab.

5 Select **Device Template** at the bottom of the screen.

6 Select **Save From Device** to create a Device Template file from the properties of this device.

7 Enter a name for the Device Template file.

➔ The name should describe the device configuration this Template is intended to work with and clearly identify the hardware configuration. (Example: AD200-PRK main entrances.)

8 Tap **OK** to save. The SUS will display the location of the saved Template file.

Before copying, a Device Template file must be saved to the SUS, /My Documents/ and must be a hardware configuration match with the receiving device.

The device template file (.dtf) can be shared among devices by copying it from the my documents folder of one of the handhelds, saving it to a computer, and then copying it to the my documents folder of any handhelds that need the template.

Copy a Saved Device Template

1 Connect the HHD to the device that will receive the saved properties settings.

➔ Be sure that the receiving device is of the same hardware configuration as that of the source of the Device Template. (**See Prerequisites on page 89 for more information.)**

2 Select **Device Options**.

3 Select **Lock Properties** for the connected device.

4 Select the **Edit** or **Reader** tab.

5 Select **Device Template** at the bottom of the screen.

6 Select **Save To Device** to copy and save a Device Template file to the connected device.

7 Select the Device Template file name.

➔ If the Device Template name is not available, check to be sure that the receiving device is of the same hardware configuration as that of the source of the Device Template. (**See Prerequisites on page 89 for more information.)**

8 Tap **OK** to save.

9 Tap **YES** on the confirmation window, then tap **OK** again to finish.

➔ Saving a Device Template file to a PIM or PIB will require re-linking of all previously linked devices

Appendix E: Diagnostic Data Log

About Diagnostic Data Log Feature

The Schlage Utility Software (SUS) version 6.2.1 (or higher) includes the Diagnostic Data Log feature. This new feature provides a simple method for AD-Series customers to quickly gather and save important lockset information in a file. This Diagnostic Data file can then be shared with Technical Services for setup and configuration review and for analysis of issues from the field.

Supported Locks

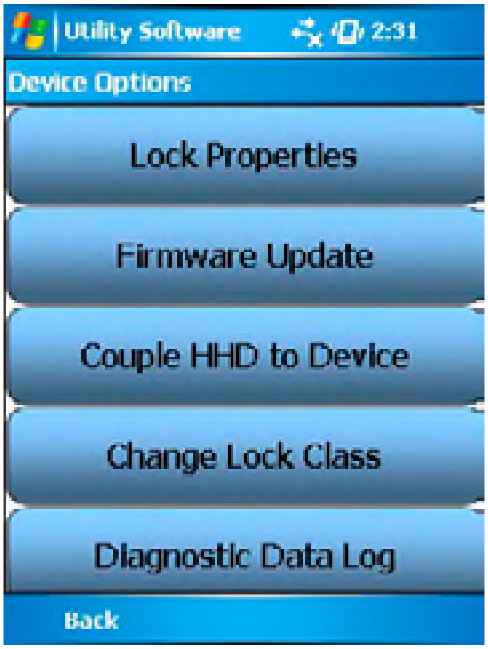
AD-Series locksets (ONLY) - AD200, AD250, AD300, AD400

Prerequisites

- The HHD used must be coupled before the Diagnostic Data Log file may be saved. See **Couple HHD to Lock** on page **24** for more information.

Diagnostic Data Log Menu

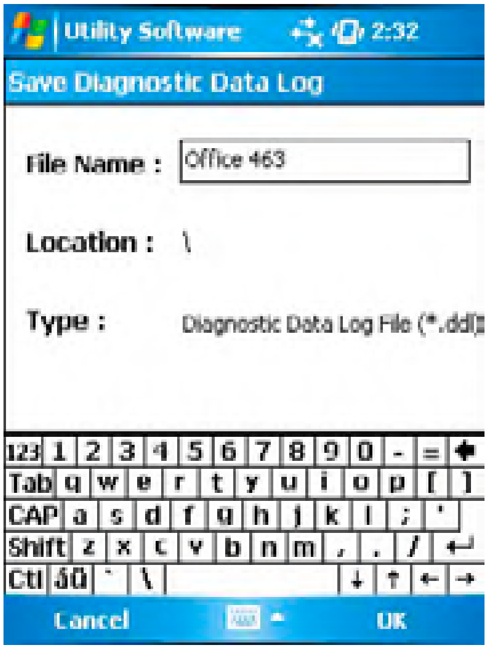
Schlage Utility Software (SUS) version 6.2.1 (or higher) provides a new **Device Options** menu. This new **Diagnostic Data Log** menu will be available when the SUS is connected and communicating with AD-Series locksets. See **Diagnostic Data Log Menu**.



Diagnostic Data Log Menu

When the Diagnostic Data log menu is selected, the customer must then provide a name for the file and then select “OK” to continue. See **Enter a descriptive name**.

➔ NOTE: Be sure to provide a sufficiently descriptive name for the file so that you and others will know which AD-Series device and location the file pertains to.



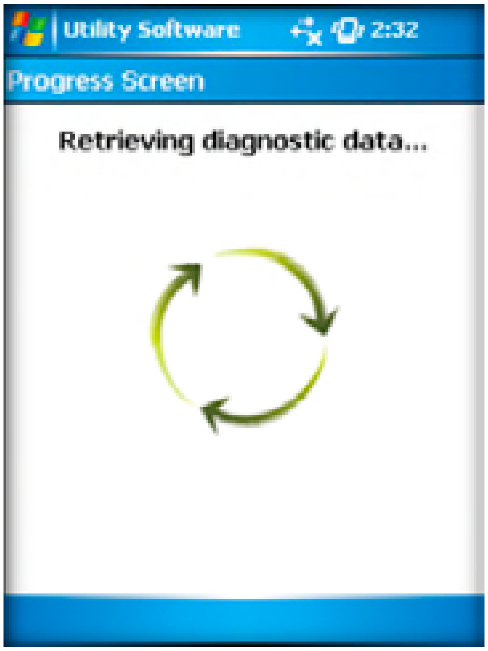
File Name : Office 463

Location : \

Type : Diagnostic Data Log File (*.ddl)

Enter a descriptive name

Next, the SUS will request all data from the AD-Series device and save the file. See **Retrieving device data** screen shot.

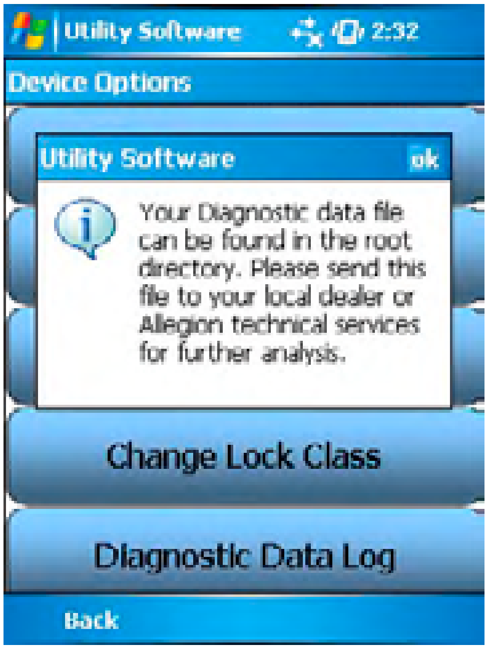


Retrieving diagnostic data...

Retrieving device data

Once the file is generated, the customer should copy and forward the Diagnostic Data file to Technical Services for detailed analysis. See **File ready for analysis** screen shot.

➔ NOTE: CO-Series products and non-lock AD-Series products do not support the Diagnostic Data Log feature



Your Diagnostic data file can be found in the root directory. Please send this file to your local dealer or Allegion technical services for further analysis.

File ready for analysis

Index

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit **www.allegion.com**.

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

SUS User Guide, Rev. 01/18-6.5.3
www.allegion.com

ALLEGION™