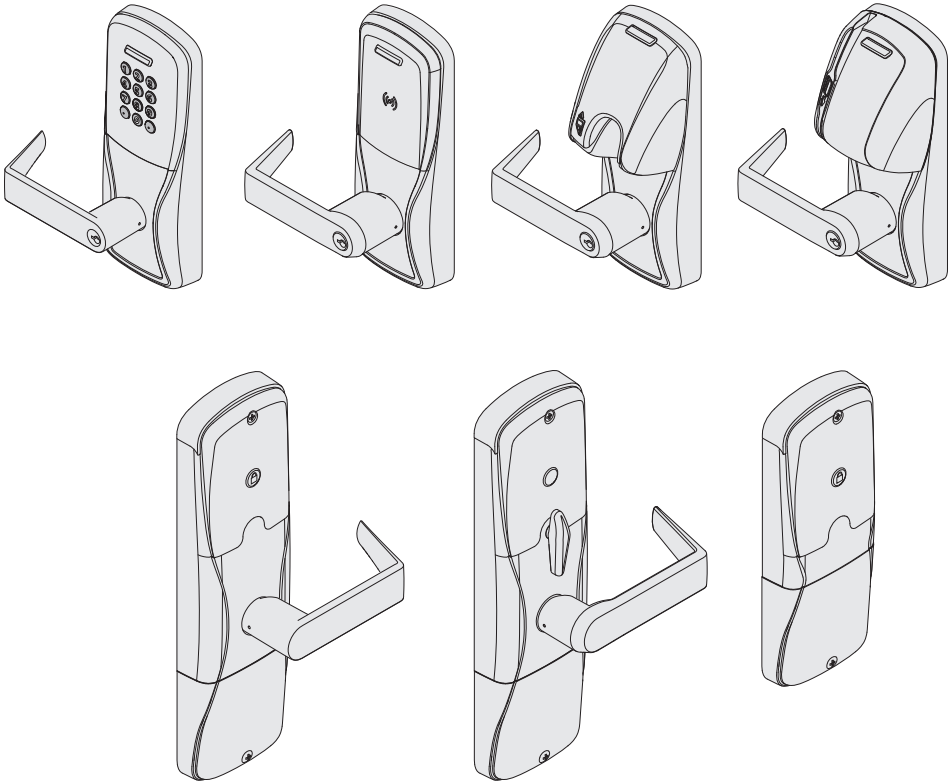
P516-128

AD-300
AD-302

Networked hardwired lock user guide

Instructions for adaptable series networked hardwired 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.

UL294 Access Control Levels tested to: Destructive Attack - Level 1; Line Security - Level 1; Endurance - Level 4; Standby Power - Level 1.

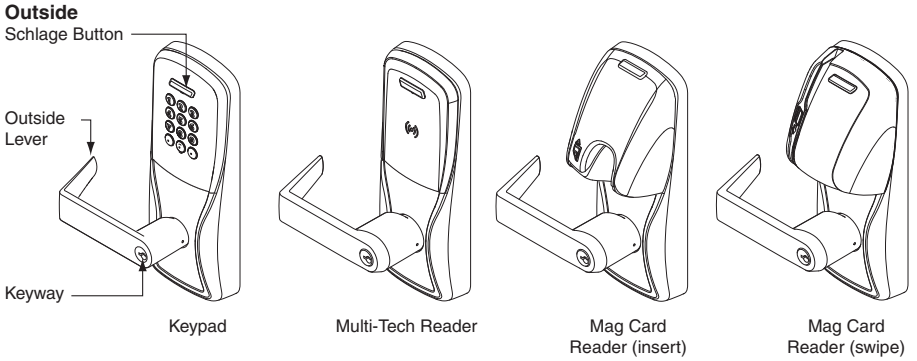
Overview

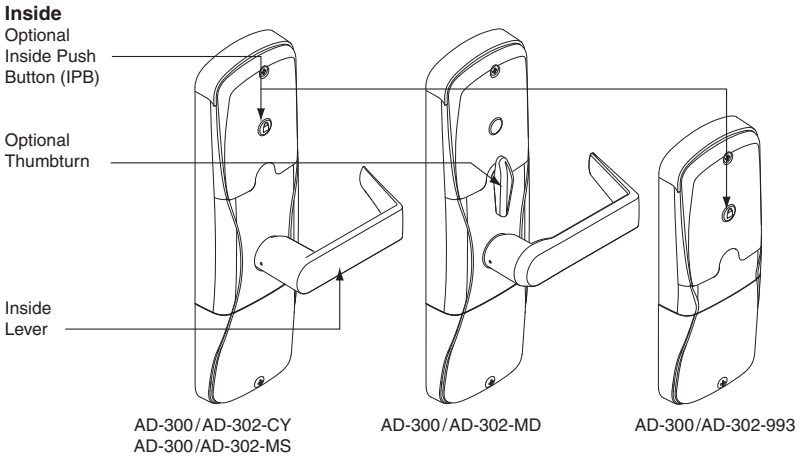
The Schlage AD-300/AD-302 is an open architecture product designed to interface with access control panels (ACPs) which use the RSI RS485 protocol.

When using an access control panel that does not use the RSI RS485 protocol, the addition of a Schlage PIB300 is required to provide a Wiegand or clock & data communications protocol.

The Schlage AD-302 is a FIPS-201-2 certified product.

- Powered by external power using a UL294 or ULC S318/ULC S319 listed power supply capable of sourcing at least 250 mA @ 12 or 24 VDC.
- The outside lever is normally locked.
- The inside lever always allows egress.
- The AD-300/AD-302 normally operates in networked mode. Information contained in the user credential is passed to an ACP, which controls lock functions. The ACP maintains the audit trail.





Additional AD-300 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 functionality as the original Proximity and Smart card readers in a single credential reader.

The AD-302 reader is a FIPS-201-2 certified Multi-Tech + Keypad (FM2) reader.

Getting started

Follow these steps to set up a new lock.

1. Install the lock. See the installation guide that came with the lock, or visit www.allegion.com/us for more information.
2. Make sure the power supply is properly connected. See *Connect to an access control panel* on page 9 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 system.
4. Test the lock for proper mechanical and electronic operation. See *Test lock operation* on page 11 for more information.
5. Connect the lock to the Access Control Panel (ACP). See *Connect to an access control panel* on page 9 for more information.
6. Consult the SUS user guide for information about configuration of the lock.
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 PIB300, and to set the RS485 address.

The SUS is used for programming lock characteristics and setup only. Access rights for the AD-300/AD-302 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 IPB state is communicated to the control panel through the RS485 connection. 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. Activity may only be reported to control systems connected by a RS485 connection.

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.

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 12 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 default settings* on page 12 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.

Lock address setup

Manually set the RS485 address

ⓘ **The lock MUST NOT be connected to RS485 communication during this procedure.**

1. Make sure that 12 or 24 VDC power is connected properly, and RS485 is not connected.

ⓘ **The Schlage button will blink red to indicate no communication with the access control panel.**

2. Open the door.
3. Create a request-to-exit condition by holding down the inside lever or crash bar. Continue to hold the inside lever or crash bar through step 5.

ⓘ **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.**

4. Press and release the Schlage button on the lock. Wait for the Schlage button to flash green.
   The lock address is now set to zero (0).
5. Repeat step 4 until the number of times you have pressed the Schlage button corresponds with the desired RS485 address.

ⓘ **Two (2) total presses sets the address to one, three (3) total presses sets the address to two, etc.**

ⓘ **Manual RS485 addresses may be assigned up to address "15" (16 total presses).[1] To assign addresses 16 - 255, use the SUS (lock properties, edit menu). For further information, refer to the SUS user guide.**

6. Release the inside lever or crash bar. The Schlage button will blink green, and the beeper will beep to indicate confirmation.

ⓘ **The number of green blinks and beeps indicates the RS485 address.**

7. After the confirmation blinks and beeps are completed, the Schlage button will again blink red to indicate no communication with the access control panel.

Set the RS485 address with Schlage utility software (SUS)

The RS485 address may be set using the SUS. Please refer to the Schlage utility software user guide for details.

1 Check your ACP to determine how the address assignments run. Most access control systems run 1 - 16, however some systems run 0 - 15 (true RS485).

Connect to an access control panel

- The two data wires from the panel (Data-A(-) and Data-B(+)) must be a shielded twisted pair.
- In case of power outage, the lock will enter the configured power failure mode. See *Power failure* on page 13 for more information.
- The AD-300/AD-302 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).
- For compliance with UL 294, product must be used with a UL 294 Listed access control panel or unit. For compliance with CAN/ULC-S319, product must be used with a CAN/ULC-S319 Listed access control panel or unit.
- The power supply may be connected to either: a) Auxiliary Power Inputs on the main board or, b) VIN (PWR) and GND connectors on the RS485 communication board.

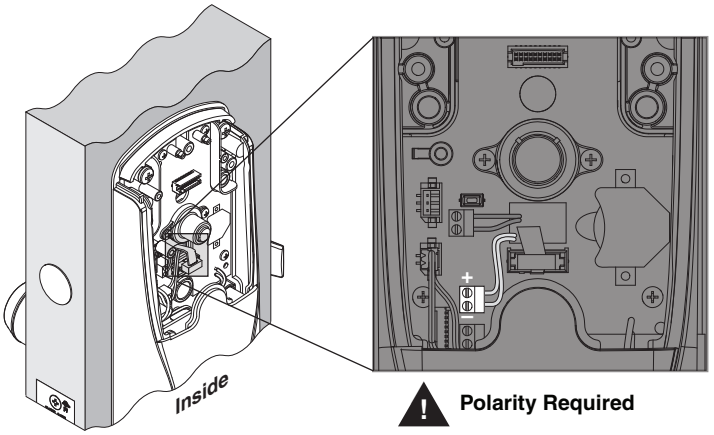
ⓘ **The EIA RS485 Specification labels the data wires as "A" and "B" but many RS485 products label their wires "+" and "-." Some products associate the "+" signal with "A", some with "B". The bottom line is that the "+" should always be connected to the "+" and the "-" to the "-" , however it is designated. Reversing the polarity will not damage either RS485 device, it will only fail to communicate. Attempt to connect "+" to "+" and "-" to "-" . If it does not work, switch them.**

WARNING: DO NOT attach power to A/B data terminals!

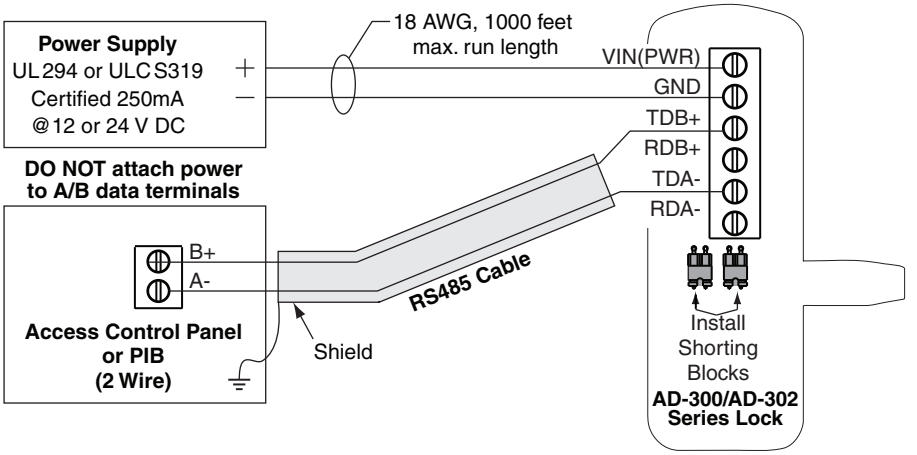
Cable/wire specifications

Application	Part number	AWG	Description	Max run length
Dc power input	Belden 8760 or equivalent	18	2 Conductor	1000 feet
RS485	Belden 9841 or 9842 or equivalent	24	3 Conductor shielded	4000 feet[1]

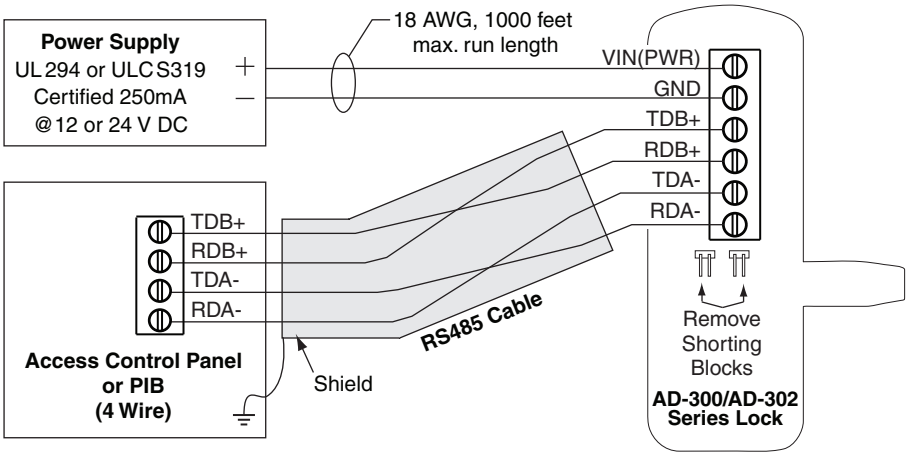
1 RS485 has 4,000 foot (1,219 meter) maximum run length. Consult the ACP supplier for maximum run directly to the ACP.



2 Wire


Power Supply
UL 294 or ULC S319
Certified 250mA
@ 12 or 24 V DC
+
—
18 AWG, 1000 feet
max. run length
VIN(PWR)
GND
TDB+
RDB+
TDA-
RDA-
DO NOT attach power
to A/B data terminals
B+
A-
RS485 Cable
Shield
Access Control Panel
or PIB
(2 Wire)
Install
Shorting
Blocks
AD-300/AD-302
Series Lock

4 Wire


Power Supply
UL 294 or ULC S319
Certified 250mA
@ 12 or 24 V DC
+
—
18 AWG, 1000 feet
max. run length
VIN(PWR)
GND
TDB+
RDB+
TDA-
RDA-
TDB+
RDB+
TDA-
RDA-
RS485 Cable
Shield
Access Control Panel
or PIB
(4 Wire)
Remove
Shorting
Blocks
AD-300/AD-302
Series Lock

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-300/AD-302 in factory default mode

1. Press any number key. The lock should beep.
2. Press the Schlage button. The keypad should light blue for a few seconds.
3. Enter the default PIN (**13579** and "**#**"). The lock should unlock momentarily and relock after the default relock delay (3 seconds).
4. 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 and RS485 is not connected, no credentials are accepted.

Test the AD-300/AD-302 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 one time. See *Construction access mode* on page 6 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.

Test with the AD-300/AD-302 linked to an access control panel

1. Present a valid credential to the lock. 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.
2. 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 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. Lock settings that will be deleted include functions, failure mode, and re-lock delays.**

ⓘ **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: credential format, magstripe reader track and beeper default.**

ⓘ **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

If communication fails between the AD-300/AD-302 and the ACP, the lock will go into communication failure mode. If the ACP loses power, the lock can lock, unlock, remain as-is, or allow valid access without communication to the ACP. This mode can be configured using the SUS. See the SUS User Guide for more information.

Cache mode is not applicable on AD-302 locks.

Network mode	When the lock is communicating with the ACP, information contained in the user credential is passed to the ACP, which controls lock functions. The ACP should maintain the audit trail.
Cache mode	Applicable only to AD-300. Upon communication failure, access may be enabled for facility codes or recent valid users. See the SUS user guide for details on the configuration of this setting.

Communication failure

If communication fails between the AD-300/AD-302 and the ACP or the PIB300, the lock will go into communication failure mode. 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 AD-300 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.

Power failure

ⓘ **Power failure does not affect any programmed data. Use the SUS to configure power failure mode. The default power failure mode is “as-Is”.**

When power failure is detected, the lock will instantly switch to the configured mode. Credentials will no longer allow access.

- If the power failure mode is “fail secure locked”, then the mechanical override key must be used to gain access (when equipped).
- If the power failure mode is “fail secure locked” or “fail unsecure unlocked”, the AD-300 will recharge for two (2) minutes after power is restored. During this two-minute recharge, the AD-300 will remain in power failure mode and the Schlage button will blink alternating green on the left and red on the right.

Power Failure Modes

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

LED and beep reference

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

Schlage button LED

Action	Lights	Beeps
Extended (Toggle) unlock	Solid green	0
Card presented and not read	None	0
Card presented and read	None	1
Access denied	Controlled by ACP via PIB300	
Access granted, momentary unlock (motor runs)	1 green	1
Relock (motor runs)	1 red	0
Keypad button press	None	1
RS485 address was manually set successfully	See page 8 for LED and beep response	
Communication from the ACP is not received by lock	Slow (1 second) flashing red continuously	4 beeps on initial communication loss

ⓘ **Note: The access control panel may have some control over the Schlage button lights, and the actual response may vary.**

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 wired power may be improperly connected.	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 wired power is connected correctly. Refer to the installation instructions that came with the lock, or this user guide for details on the above mentioned procedures.
The AD-300/ AD-302 is not communicating with the access control panel. When a valid credential is presented, the Schlage button blinks red one time and/or the IPB LED blinks red four (4) times with rapid beeps.	The RS485 Communication Module is not properly installed. Data transmission to the access control panel is not successful.	Check that the RS485 Communication Module is installed and fully seated, and that there are no bent pins on the connector. Check that the lock is wired to the access control panel. Check that the access control panel software has the AD-300/AD-302 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.
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 door ribbon cable is not pinched and is seated properly. Change the Smart card format using the SUS. Select AD-300/AD-302 “Lock Properties”, “Reader” tab, and “Smart cards in use”. Use the SUS to change “Mag Track in Use”. Select AD-300/AD-302 “Lock Properties”, “Reader” tab, and “MAG Card Track selection”. Refer to the installation instructions that came with the lock, or the SUS user guide for details on the above mentioned procedures.
The AD-300/ AD-302 does not grant access immediately.	The time to grant access is an operation of the access control panel.	Check the access control panel configuration.

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

Printed in U.S.A.
P516-128 Rev. 06/18-m