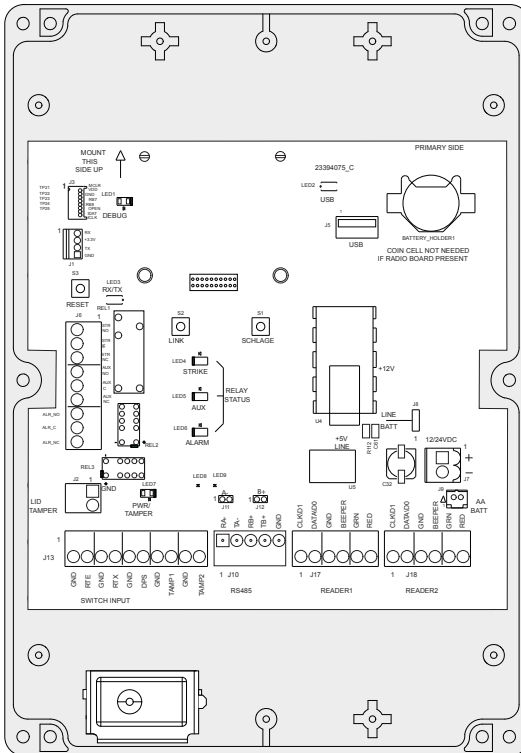# CT5000

Offline controller user guide

Instructions for Adaptable Series offline controller

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.

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

Overview

The Schlage CT5000 is an off-line access controller in the AD-Series product line.
- The CT5000 is intended for use on one (1) single opening.
- May be used with up to two (2) credential reader interfaces that use Wiegand and/or Clock & Data outputs.
- Externally powered using a UL 294 power supply for UL installations and a ULC S318/ULC S319 listed Class 2 power supply for cUL installations (not included) capable of sourcing at least 500 mA @ 12 or 24 VDC (example: Schlage models PS902, PS904, PS906).
- Capable of storing credentials for up to 5000 users.
- Maintains an audit trail of up to 5000 events.
- Intended for indoor use only. Ambient temperature range -35C to +66C (-31F to +151F).
- The CT5000 is configured using the Handheld Device (HHD). See *Handheld Device (HHD)* on page 14 for more information.
- Any installation involving an opening which is considered an emergency exit or a fire rated opening must conform to all local and national safety and building codes.
- Access equipment manufactured and/or sold by Allegion is not rated for, or intended for use in life safety installations. UL listed panic hardware must be used to allow emergency exit from the protected area.
- **Before installing the CT5000 controller, read all documentation for all products in the installation**.
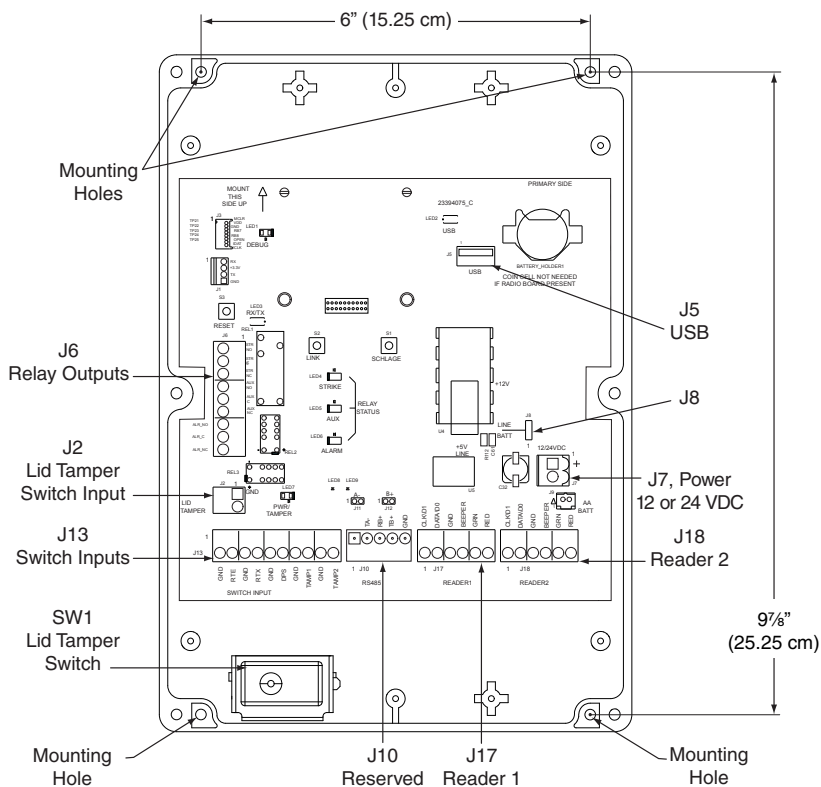
Before installing the CT5000, read all documentation for all products in the installation.

1. Determine the location of each component in the access control system. **The CT5000 must be installed indoors.**
2. To operate at optimum efficiency, cable runs should be kept as short as possible.
3. Consult the National Electrical Code (NEC) and local electrical codes for information regarding wire run lengths and minimum required wire gauge.
4. Install the UL listed reader(s) as specified in the control unit installation instructions.

ⓘ **The CT5000 may not control or configure the reader's beeper or LED settings. Consult the reader's user guide for more information on configuring the reader's beeper or LED patterns.**

5. Install the UL listed electrified locking hardware. See the manufacturer's installation guide that came with the hardware. For installation instructions and information for Schlage electrified locks, visit the Schlage website at www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library).
6. Install the CT5000. **A U.S. single gang electrical box (not included) is required for the remote USB connection**. See *Remote USB connection* on page 13.
7. Install a UL294 or ULCS318/ULCS319 listed power supply (example: Schlage PS900 Series) for the CT5000 and the readers. The power supply must be compatible with all components and must have the capacity to power the CT5000 **and** the readers. (The CT5000 requires a power supply capable of sourcing at least 500 mA @ 12 or 24 VDC.)

ⓘ **If preferred, separate UL294 or ULCS318/ULCS319 listed power sources for the CT5000 and the readers is an acceptable alternative.**

8. Make sure power is properly connected to all components in the system.
9. After power is applied, remove the mylar strip from the coin cell battery.
10. Make all wiring connections.
11. Configure and program the CT5000. See *CT5000 manual programming* on page 16.
12. Test the operation of the CT5000 with the electrified locking hardware. See *Test* on page 21.

Save this user guide for future reference.
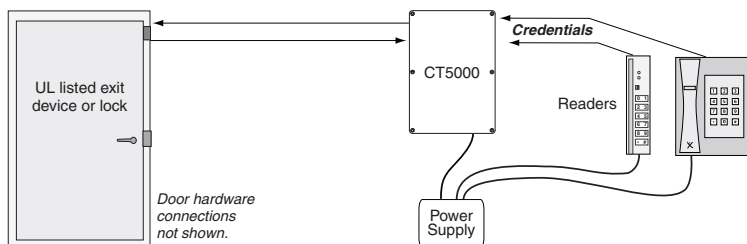
Typical installation

Compatible credential reader output formats:
- Wiegand and Clock & Data formats are compatible with the CT5000.
- Keypad formats compatible with the CT5000 are: ASCII with leading parity, 4-bit, 8-bit and 26-bit Wiegand. (Note: Manual programming and card plus pin are not supported in 26-bit Wiegand.)

Mount the CT5000

Follow these steps to permanently attach the CT5000 enclosure to its desired location.

1. Drill four holes, ⁹⁄₃₂" diameter drill bit, 1¾" (44 mm) deep, located to match the mounting holes as shown on page 3.
2. If the location does not adequately support the CT5000, mounting anchors should be used (not included).
3. Mount the CT5000 using appropriate #8 mounting hardware (not included).

CT5000 wiring connections

Wiring the CT5000 to access control peripherals

The CT5000 will interface with two (2) UL listed credential readers and supports three (3) output relays – strike, auxiliary and alarm and four (4) optional inputs – reader 1 tamper, reader 2 tamper, request to exit and door position switch.

Request to enter is not supported on the CT5000.

Use cable entry/exit connectors that comply with local electrical codes (i.e. conduit, etc.)

Drill hole(s) in the CT5000 enclosure to accommodate the size and number of entry/exit connectors to be used (refer to diagram).

To avoid damage to electronics inside the enclosure when drilling, use light pressure so that the bit does not penetrate very far when it breaks through the enclosure, or remove electronics from the enclosure before drilling.

Drill access hole(s) in this area.
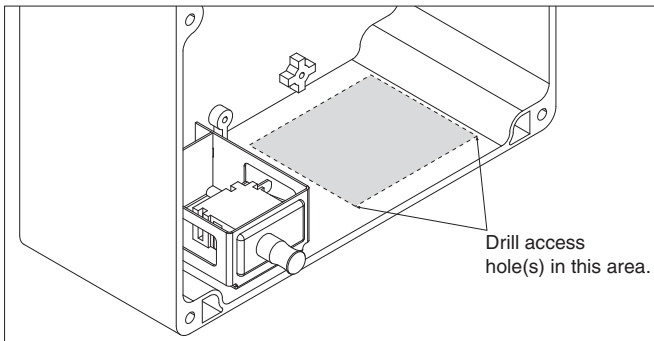
CT5000 cable/wire specifications
- Wiring methods should be in accordance with the National Electric Code (ANSI/ NFPA70), local electric codes and the authorities having jurisdiction.
- Cabling and wire must be UL listed and recognized wire suitable for the application.
- Use only stranded, multi-conductor wire without splices.
- Refer to *Cable/Wire Table 1 - Typical Installation* for wire specifications for a typical configuration.
- Refer to *Cable/Wire Table 2* for wire specifications for other wiring configurations.

Cable/wire table 1 –Typical Installation

Application	Part number	AWG	Description	Length of wire run
DC power input	Belden 8760	18	2 conductor	100 feet (30.5 meters)
Door position switch	Belden 8760	18	2 conductor shielded	500 feet (152.5 meters)
Request to exit	Belden 8760	18*		
Strike relay output	Belden 8760	18*		
Auxiliary relay output	Belden 8760	18*		
Alarm relay output	Belden 8760	18*		
Credential reader tamper	Belden 8760	18*		
Credential reader 1	Alpha 1296C	22	6 conductor shielded	
	Alpha 1298C	22	8 conductor shielded	
Credential reader 2	Alpha 1296C	22	6 conductor shielded	
	Alpha 1298C	22	8 conductor shielded	

* Typical application. See *Cable/wire table 2* for load/power wire runs.

Cable/wire table 2

Total length of one wire run	Load current @ 12 VDC				Load current @ 24 VDC			
	1/4 A	1/2 A	3/4 A	1 A	1/4 A	1/2 A	3/4 A	1 A
100 feet (30.5 meters)	24	18	16	14	24	20	18	18
200 feet (61 meters)	16	14	12	12	20	18	16	14
300 feet (91.5 meters)	16	12	12	10	18	16	14	12
400 feet (122 meters)	14	12	10	–	18	14	12	12
500 feet (152.5 meters)	14	10	10	–	16	14	12	10

Power

The J7 input power connection is mandatory. An external, UL 294 or ULC S318/ULC S319 listed power supply capable of sourcing at least 500 mA @ 12 or 24 VDC must be provided.

RS-485

J10 RS-485 connection is reserved for future expansion.

Tamper input

SW1 lid tamper switch monitors the state of the CT5000 enclosure lid and generates a tamper trouble signal when the lid is open. When terminals J2-1 and J2-2 are shorted, a tamper audit is recorded.

Switch inputs

Request to exit and door position switch are designed to be dry contact switches tied to ground when the switch is closed.

Reader 1 tamper and reader 2 tamper are designed to be dry contact switches tied to ground when the switch is closed, **OR** a signal level input for 5V logic. Any voltage greater than 5V may cause damage to either the CT5000 or the reader(s).

Connect the shield of the electrified locking hardware input cables to the appropriate CT5000 GND terminal.

ⓘ **The switch input may be changed from the default condition using the Schlage Utility Software (SUS) on the HHD.**

Switch input terminal			Description	Default condition
GND	J13-1	Ground	Not currently used in the CT5000.	
RTE	J13-2	Request to enter		
GND	J13-3	Ground	Electrical ground (common) for the CT5000.	
RTX	J13-4	Request to exit	When the switch opens or closes, the CT5000 will change the state of the strike relay.	Switch closed (GND) = Request to exit
GND	J13-5	Ground	Electrical ground (common) for the CT5000.	
DPS	J13-6	Door position switch	By default, the CT5000 assumes there is no DPS connected. To install DPS, a Handheld Device (HHD) with Schlage Utility Software (sold separately) is necessary to change the configuration of the system to indicate that a DPS is installed. When DPS is installed and enabled, the CT5000 will trigger an alarm if configured in this manner with the HHD.	Switch open = door closed
GND	J13-7	Ground	Electrical ground (common) for the CT5000.	
TAMP1	J13-8	Reader 1 tamper	When a signal level input is used, connect the wire to TAMP1 OR When a dry contact switch is used, connect one wire to TAMP1 and the other to pin 7 (GND).	Signal low or switch closed (GND) = reader 1 tamper
GND	J13-9	Ground	Electrical ground (common) for the CT5000.	
TAMP2	J13-10	Reader 2 tamper	When a signal level input is used, connect the wire to TAMP2 OR When a dry contact switch is used, connect one wire to TAMP2 and the other to pin 9 (GND).	Signal low or switch closed (GND) = reader 2 tamper

Relay outputs

The three (3) relay outputs consist of strike, auxiliary and alarm outputs. These are Form C type relay outputs with normally open, common and normally closed contacts.

The factory default configuration of the strike relay is as follows:
- When the strike relay is de-energized, the opening is assumed to be secure.
- When the strike relay is energized, the opening is assumed to be unsecure.

Accordingly, **the appropriate side of the relay contact (normally open/normally closed) must be used to ensure that when the relay is de-energized the opening is locked, and when the relay is energized the opening is unlocked.** The aux and alarm relays are de-energized by default.

The strike, auxiliary and alarm relay outputs can be individually configured by the SUS on the HHD.

Refer to *Wiring Diagrams* on page 10, page 11, and page 12.

Relay output terminal			Description
STR_NO	J6-1	Strike normally open	The strike relay is capable of switching up to a 6 amp resistive load at 24 VDC, 6 amp at 120 VAC, or 3 amp at 240 VAC.
STR_C	J6-2	Strike common	
STR_NC	J6-3	Strike normally closed	
AUX_NO	J6-4	Auxiliary normally open	The aux relay is capable of switching up to a 2 amp resistive load at 24 VDC or 0.5 amp at 120 VAC.
AUX_C	J6-5	Auxiliary common	
AUX_NC	J6-6	Auxiliary normally closed	
ALR_NO	J6-7	Alarm normally open	The alarm relay is capable of switching up to a 2 amp resistive load at 24 VDC or 0.5 amp at 120 VAC. Note: The CT5000 alarm operates only when a DPS is installed and the CT5000 is properly configured with the HHD.
ALR_C	J6-8	Alarm common	By default, the CT5000 assumes there is no DPS connected. To install DPS, a Handheld Device (HHD) with Schlage Utility Software (sold separately) is necessary to change the configuration of the system to indicate that a DPS is installed.
ALR_NC	J6-9	Alarm normally closed	

A transient suppressor must be installed with every electrical device switched through a relay output contact.

Refer to the *Relay output suppression diagram* below. Follow the UL listed electrified lock/load manufacturer's recommendation for suppression of magnetic/inductive loads. Use a properly rated transient voltage suppression (TVS) diode (or silicon avalanche diode). Install the suppressor within 18 inches (46 cm) of the switched electrical load.

ⓘ **Relay outputs must utilize a dedicated shielded cable to prevent transient contamination of other CT5000 signal wiring. Do not run relay output wires in the same cable or conduit as any other CT5000 wiring. Connect the shield of the relay output cables to the appropriate earth ground terminal of the electrified lock/load or auxiliary load power supply. The shield should NOT be connected at the CT5000.**
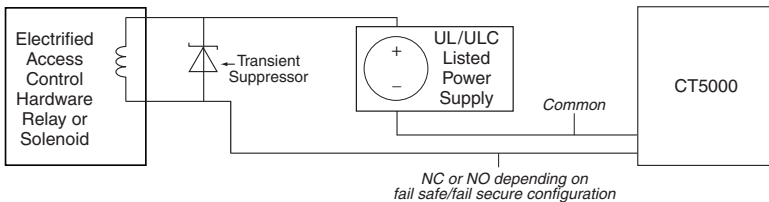
Relay output suppression diagram

Credential readers

An input device with either Wiegand (Data1/Data0) or Magnetic (Clock and Data) bit stream can be used with the CT5000. The CT5000 provides two (2) separate credential reader interfaces for control of one (1) opening.

The following readers are UL 294 listed for use with the CT5000:
- Essex Electronics model KTP-162
- Mercury Security models MR-5 and MR-20, and XceedID models XF-1050, XF-1100, XF-1500, XF-1550 and XF-2100

The following readers are UL C S319 listed for use with the CT5000:
- XceedID models PR10, SM10, MT11, MT11-485, MT15, MT15-485, MTK15 and MTK15-485.

Connect the shield of the reader 1 cable to the CT5000 J17-3 terminal (GND). Connect the shield of the reader 2 cable to the CT5000 J18-3 terminal (GND). Do not connect the cable shield at the credential reader.
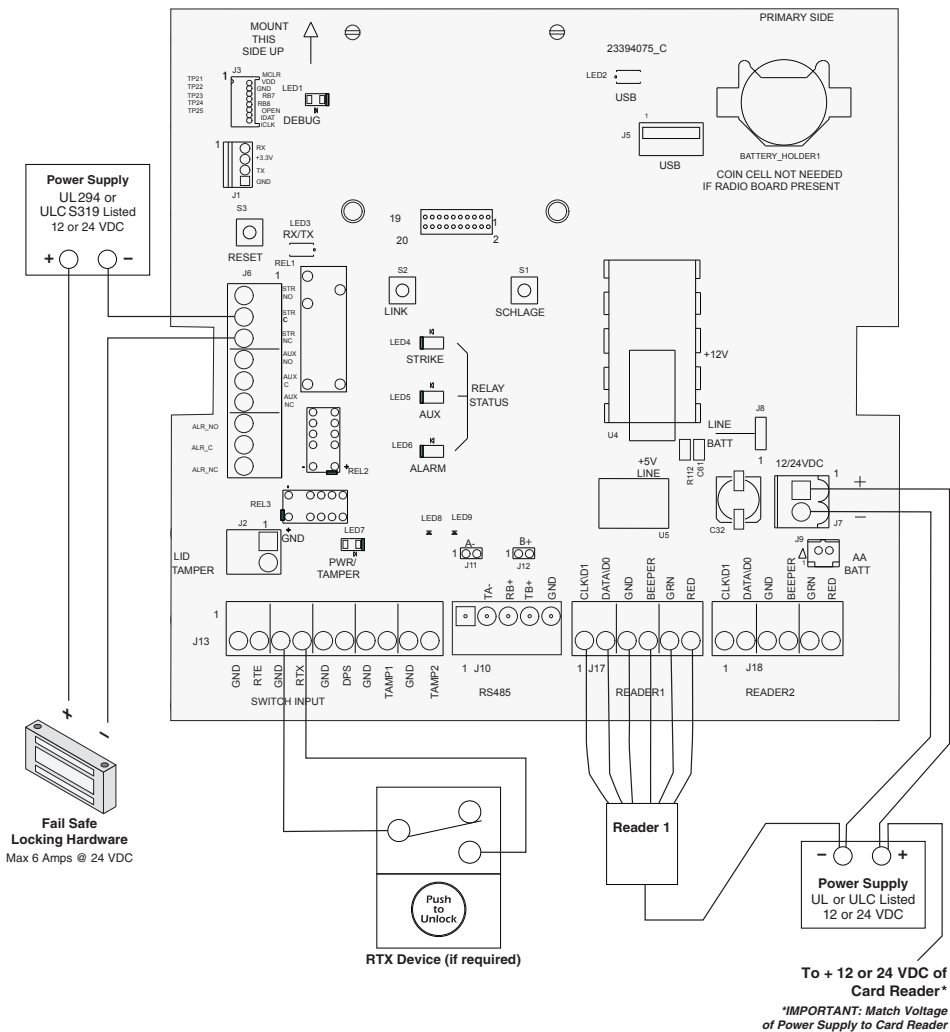
ⓘ **Reader input ports are designed for 5V logic. Any voltage greater than 5V may cause damage to either the CT5000 or the reader(s).**

The CT5000 does not provide power to the reader(s). Power must be provided to the reader(s) separately by a UL listed power supply. Refer to *Wiring Diagram* examples on page 10, page 11, and page 12.
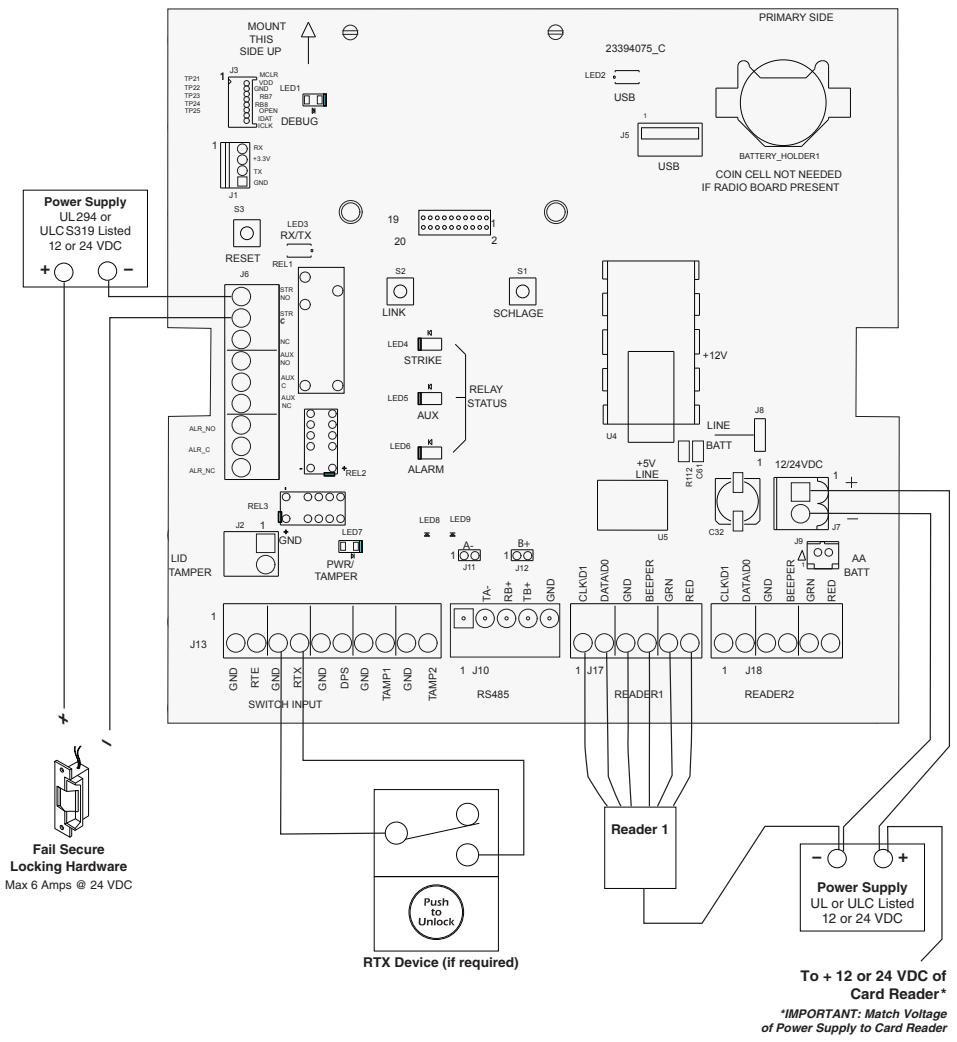
The CT5000 may not provide complete control of the reader's beeper or LEDs. Please consult the reader's manufacturer for instruction on reader configuration.

Make sure your reader is configured with the LEDs and beeper OFF for best compatibility.

	Reader 1 terminal	Reader 2 terminal	Description
CLK/D1	J17-1	J18-1	Credential reader inputs: Each input line is pulled to GND through a 12V transient suppressor and a 2 mega-ohm resistor.
DATA/D0	J17-2	J18-2	
			Wiegand or magnetic format is automatically detected.
GND	J17-3	J18-3	The signal ground of the CT5000 must be tied to the signal ground at the reader.
BEEPER	J17-4	J18-4	Beeper signal line connection to the reader.
			This is an "open collector" style output, and has a 12V transient suppressor to GND.
			The output is switched to GND through a 100 ohm resistor to activate the beeper on the reader.
			Note: Most readers beep independently, and beeper performance depends on the specific reader model.
GRN	J17-5	J18-5	Green LED signal line connection to the reader.
			This is an "open collector" style output, and has a 12V transient suppressor to GND.
			The output is switched to GND through a 100 ohm resistor to activate the green LED on the reader.
RED	J17-6	J18-6	Red LED signal line connection to the reader.
			This is an "Open Collector" style output, and has a 12V transient suppressor to GND.
			The output is switched to GND through a 100 Ohm resistor to activate the red LED on the reader.

Wiring diagram CT5000 x magnetic lock

PRIMARY SIDE

MOUNT
THIS
SIDE UP

23394075_C

LED2
USB

J5
USB

BATTERY_HOLDER1

COIN CELL NOT NEEDED
IF RADIO BOARD PRESENT

TP21
TP22
TP23
TP24
TP25

J3
MCLR
VDD
GND
RB7
RB8
OPEN
IDAT
ICLK

LED1

DEBUG

1
RX
+3.3V
TX
GND
J1

Power Supply
UL 294 or
ULCS319 Listed
12 or 24 VDC

+   −

S3

RESET

LED3
RX/TX

REL1

J6
STR
NO
STR
C

NC

AUX
NO

AUX
C

AUX
NC

ALR_NO

ALR_C

ALR_NC

19

20

2

S2

LINK

S1

SCHLAGE

LED4
STRIKE

LED5
AUX

LED6
ALARM

RELAY
STATUS

+12V

U4

LINE

BATT

J8

1

12/24VDC

1
+

J7
−

+5V
LINE

R112

C61

C32

U5

J9

AA
BATT

REL2

−   +

REL3

J2 1

GND

LID
TAMPER

LED7
PWR/
TAMPER

LED8 LED9

A-
J11

B+
J12

TA-
RB+
TB+
GND

CLK/D1
DATA0
GND
BEEPER
GRN
RED

CLK/D1
DATA0
GND
BEEPER
GRN
RED

J13

1

GND
RTE
GND
RTX
GND
DPS
GND
TAMP1
GND
TAMP2

SWITCH INPUT

1 J10

RS485

1 J17

READER1

1 J18

READER2

**Fail Secure
Locking Hardware**
Max 6 Amps @ 24 VDC

Reader 1

Push
to
Unlock

RTX Device (if required)

−   +

Power Supply
UL or ULC Listed
12 or 24 VDC

**To + 12 or 24 VDC of
Card Reader**
*IMPORTANT: Match Voltage
of Power Supply to Card Reader*

Wiring diagram CT5000 x electric strike
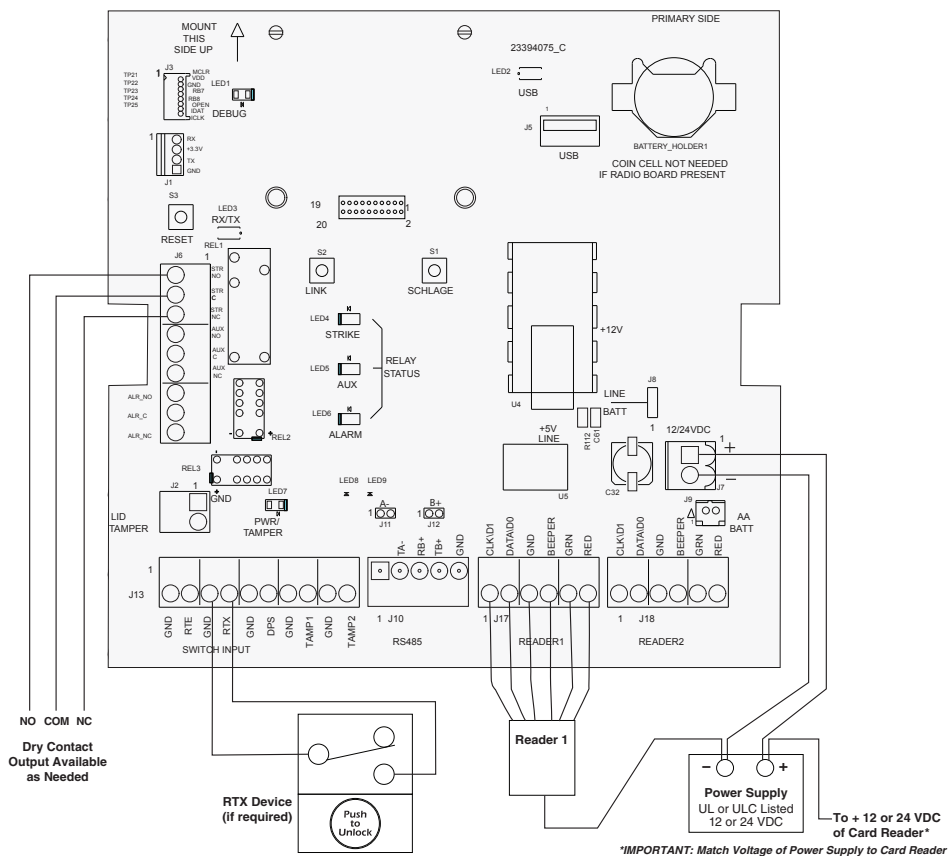
Wiring diagram CT5000 x dry contact relay

Power failure modes

The CT5000 strike relay can be configured to fail safe (fail unlocked) or fail secure (fail locked) using SUS on the HHD. The default state of the strike relay is fail secure or "normally closed (secure)" on the HHD. Auxiliary and alarm relays can also be configured. Please use the chart below as a recommended wiring guideline with various types of electronic locking hardware.

To maximize security, a valid credential must be presented before any configuration change to the strike relay can take effect.

- For **fail secure**, UL listed panic hardware must be used to allow emergency exit from the protected area.
- UL listed electronic locking devices may need a UL listed access control or burglar power supply **with** battery backup for the CT5000 to control their power failure mode (example: Schlage models PS902, PS904, PS906). The battery backup time must be the same or greater than the CT5000 battery backup time.

Locking hardware	Failure state	Strike relay wiring	SUS strike relay configuration	Battery backup for locking hardware?
Fail safe locking hardware	Fail secure	NC-C	Normally closed	Yes
	Fail safe	NC-C	Normally closed	No
Fail secure locking hardware	Fail secure	NO-C	Normally closed	No
	Fail safe	NC-C	Normally open	Yes

Programming may be performed locally at the CT5000, or remotely up to 15 cable feet away using the furnished cable, panel mount cable and wall plate (shown below). A remote USB connection will allow the Handheld Device (HHD) to communicate with the CT5000 without removing the CT5000 enclosure lid.
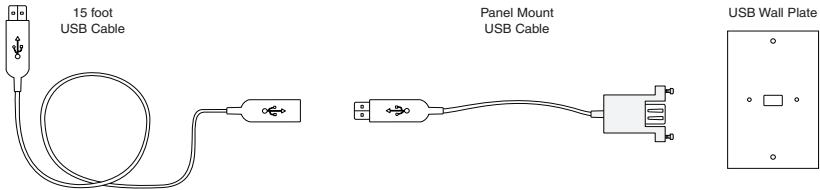

ⓘ **Programming may be remotely performed up to 125 cable feet away using a USB extender kit, part number 23745565 (sold separately).**

Follow these steps to install the 15 foot USB cable, panel mount USB cable, and USB wall plate (see diagram below):
1. Route the 15 foot USB cable through the hole in the CT5000 enclosure (see *CT5000 wiring connections* on page 5 for more detail). Verify proper USB mating end is run into the CT5000. **DO NOT connect the USB cable to the CT5000 USB port (J5) yet.**
2. Route the 15 foot USB cable from the CT5000 to where a U.S. single gang electrical box (not included) will be installed. Install the single gang box at this location.
3. Connect the panel mount USB cable to the USB wall plate using the included hardware.
4. Route the 15 foot USB cable through the single gang electrical box and connect it to the panel mount USB cable.
5. Attach the USB wall plate to the single gang electrical box using the included hardware.
6. Connect the USB cable to the CT5000.

The CT5000 can now be configured and programmed with the HHD through the USB wall plate.

ⓘ **The lid must be taken off of the CT5000 enclosure in order to couple an HHD to the CT5000 for the first time.**
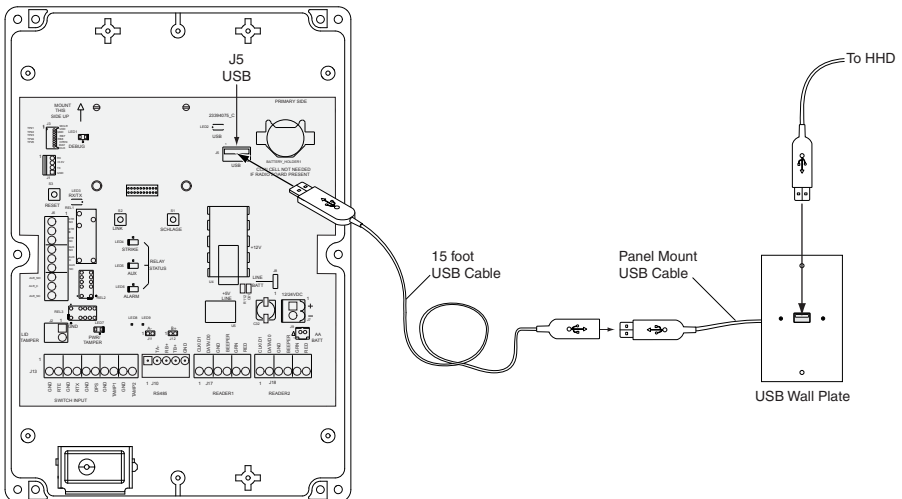
The Handheld Device is used for programming and setup only.

The HHD is used to configure the CT5000. This includes transferring data files between the access control software and the CT5000. Refer to the SUS user guide for more information about the HHD.

To connect the HHD to the CT5000:

ⓘ **If a remote USB connection is being used, begin at step 3.**

1. Loosen the 6 screws and remove the CT5000 lid. The POWER LED should blink green when the lid is off.
2. Verify power is connected to the CT5000.
3. Log in to the SUS software. See the SUS User Guide at www.allegion.com/us (see Support>Schlage Electronics>Electronic Locks Technical Library).

ⓘ **Make sure the HHD connection type is set to "USB Connection".**

4. Connect the HHD to J5 USB port, or to the USB wall plate if a remote USB connection is used. The CT5000's USB LED will blink green.

   The CT5000 is communicating with the HHD when the USB LED blinks green and the HHD display indicates "new lock", "no door data available" or the name of the door file. ***The SUS is now ready to view the CT5000 settings.***

5. To Edit Settings or Update Firmware on the CT5000, the SUS software and the CT5000 must be coupled.To couple the CT5000 and the HHD:
   - On the CT5000, press and hold the SCHLAGE button while pressing the LINK button three (3) times within 5 seconds.
   - The USB LED will blink red and green. On the SUS, select the option "Couple HHD to Device". SUS will report when coupling is successful.
   - Successful coupling will be indicated on the CT5000 with a blinking green USB LED.
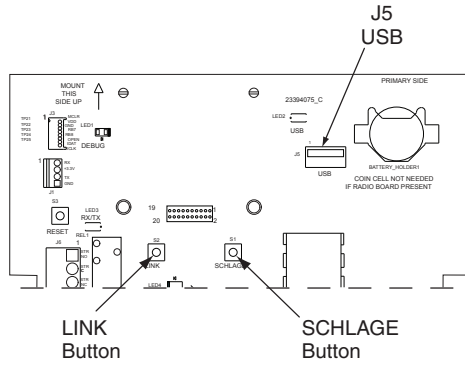
Construction access mode

Construction access mode is used to allow access before the CT5000 controller has been programmed, and for testing purposes.
- Enabled by default.
- The CT5000 controller will remain in construction access mode until the mode is cancelled as described below.
- No audits are captured while the CT5000 controller is in construction access mode.

CT5000 controller with readers
1. Remove the CT5000 lid.
2. Press and hold the Schlage button.
3. Present a credential to the reader within 5 seconds of pressing the Schlage button.
4. The DEBUG LED and the reader's LED will blink green five (5) times.
5. This credential becomes the master construction credential.

ⓘ **If the credential is not presented within 5 seconds, timeout will occur. Repeat steps 2-5 above.**

To program construction access mode user credentials:

ⓘ **The master construction credential must be programmed before programming construction access mode user credentials.**
1. Present the master construction credential to the reader.
2. The DEBUG LED and the reader's LED will light green for 20 seconds.
3. Present the credential to be programmed within 20 seconds.
4. The DEBUG LED and the reader's LED will blink green five (5) times.

Cancel construction access mode

Do one of the following:
- Program the lock with the HHD. See the SUS User Guide for more information.
- Reset the lock to factory settings. See *Reset to factory defaults* on page 15 for information.

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

> **TIPS**
>
> Use the same master construction credential for all the controllers in the facility.
>
> If you present the first card with a new controller to create the master construction credential and the card is not accepted, the controller has either been programmed or already has a master construction credential.
>
> If the master construction credential cannot be located, or to put the controller back into construction access mode, reset the controller to factory settings. See *Reset To Factory Defaults* below for more information.

Reset to factory defaults

All information in the CT5000 will be deleted and reset to factory defaults!
1. Remove the CT5000 lid.
2. Press and hold both the SCHLAGE and LINK buttons for approximately three (3) seconds.
3. When the POWER/TAMPER LED turns off, release the buttons.
4. After a 15 second delay, the CT5000 DEBUG LED and the reader's LED will blink green for one second, and the reader will beep for one second.
5. Replace the lid.

CT5000 manual programming

ⓘ **Manual programming applies only to a CT5000 installed with a keypad credential reader.**

ⓘ **Keypad credential readers with ASCII with leading parity, 4-bit and 8-bit formats allow manual programming.**

When adding a card credential, **the 3-6 digit code (PIN) entered prior to presenting the card becomes the** <u>Credential Reference Number</u>. This number can be used to delete a card without physically having the card. Keep a log of all issued Credential Reference Numbers and codes for future reference.

> **TIPS**
>
> The default programming code is 97531 and "*".
>
> The default normal use code is 13579 and "#".

Credential types

Credential type	Function	Description
Programming (code or card)	Used to program the CT5000 controller. Does not unlock the lock.	Five-digit code and "*" OR card
Normal use	Unlocks the lock (activates main relay), for the time of the relock delay.	PIN (3 - 6 digits) OR card
Normal use +PIN		PIN (3 - 6 digits) AND card
Toggle	Changes the state of the CT5000 controller from locked to unlocked, or vice versa, unless in a Freeze state.	PIN (3 - 6 digits) OR card
Toggle +PIN		PIN (3 - 6 digits) AND card
Freeze	Freezes the lock in the current state. CT5000 controller remains frozen until Freeze credential is presented again.	PIN (3 - 6 digits) OR card
Freeze +PIN		PIN (3 - 6 digits) AND card
Pass-Through	Unlocks a lock momentarily, regardless of state. Overrides a CT5000 controller in Freeze state.	PIN (3 - 6 digits) OR card
Pass-through +PIN		PIN (3 - 6 digits) AND card
Aux only	Used to activate the auxiliary relay, for the time of the relock delay.	PIN (3 - 6 digits) OR card
Aux toggle	Changes the state of the auxiliary relay from locked to unlocked, or vice versa, unless in a Freeze state.	PIN (3 - 6 digits) OR card
Main + aux normal use	Used to activate the main and auxiliary relays together for time of the relock delay.	PIN (3 - 6 digits) OR card
Main + aux pass thru	Unlocks both the main and auxiliary relays regardless of state, for the time of the relock delay.	PIN (3 - 6 digits) OR card
Main + aux toggle	Changes the state of both the main and auxiliary relays from locked to unlocked, or vice versa, unless in a Freeze state.	PIN (3 - 6 digits) OR card

Programming legend

Symbol	Description
[Programming code]	Five-digit code, identical to programming credential code listed in the credential types table.
Programming Card	Programming card, identical to programming credential card listed in the credential types table.
[CODE]	An identifier assigned to a specific function of the electrified locking hardware.
[PIN]	Three- to six-digit code (default PIN length is six digits). A PIN can be any of the PIN code types listed in the Credential Types table. A PIN entered before a card credential becomes the Credential Reference Number.
✱	Asterisk key on the keypad
⓪ - ⑨	Number keys on the keypad

Manual programming commands

ⓘ **Keep a log of programmed credentials and users, with functions and PIN numbers.**

ⓘ **Commands are confirmed by five blinks of the green DEBUG LED and the reader's green LED will blink.**

ⓘ **The reader's red LED will blink to indicate an incorrect entry. To interpret blink patterns, refer to page 20.**

Function	Press/Present	Confirmation[1]
Change [Programming Code]	[Programming Code] ✱ OR Programming Card ⑦ ✱ New [Programming Code] ✱ New [Programming Code] ✱	Wait for green LED to stop blinking between each step.
Change Programming Card	[Programming Code] ✱ OR Programming Card ⑦ ✱ New Programming Card	Wait for green LED to stop blinking between each step.
Add Normal Use Credential	[Programming Code] ✱ OR Programming Card ③ ✱ ••••••••••••••••►New [PIN] ✱ ✱ (for PIN only) OR New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Add Normal Use +PIN Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ③ ① ① ✱ ••••••••••••••••►New [PIN] ✱ New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.

1 Other lights may show before the final confirmation. Wait for the final confirmation before continuing to the next step.

Function	Press/Present	Confirmation[1]
Add Toggle Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ① ⑨ ① ✱ ▶New [PIN] ✱ ✱ (for PIN only) OR New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Add Toggle +PIN Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ③ ⑨ ① ✱ ▶New [PIN] ✱ New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Add Freeze Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ① ① ⑤ ✱ ▶New [PIN] ✱ ✱ (for PIN only) OR New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Add Freeze +PIN Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ③ ① ⑤ ✱ ▶New [PIN] ✱ New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Add Pass Through Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ① ① ⑨ ✱ ▶New [PIN] ✱ ✱ (for PIN only) OR New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Add Pass Through +PIN Credential	[Programming Code] ✱ OR Programming Card ③ ③ ✱ ③ ① ⑨ ✱ ▶New [PIN] ✱ New Card add another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.
Delete Credential	[Programming Code] ✱ OR Programming Card ⑤ ✱ ▶Credential [PIN] ✱ delete another credential OR ✱ to finish	Wait for green LED to stop blinking between each step.

1 Other lights may show before the final confirmation. Wait for the final confirmation before continuing to the next step.

Function	Press/Present	Confirmation[1]
Aux Only	[Programming Code] ✱　OR　Programming Card ③ ③ ✱ ⑦ ① ① ✱ ·····················► New [CODE] ✱ ✱ (for CODE only)　OR　New Card add another credential　OR　✱ to finish	Wait for green LED to stop blinking between each step.
Aux Toggle	[Programming Code] ✱　OR　Programming Card ③ ③ ✱ ⑦ ⑨ ① ✱ ·····················► New [CODE] ✱ ✱ (for CODE only)　OR　New Card add another credential　OR　✱ to finish	Wait for green LED to stop blinking between each step.
Main + Aux Normal	[Programming Code] ✱　OR　Programming Card ③ ③ ✱ ⑨ ① ① ✱ ·····················► New [CODE] ✱ ✱ (for CODE only)　OR　New Card add another credential　OR　✱ to finish	Wait for green LED to stop blinking between each step.
Main + Aux Pass Thru	[Programming Code] ✱　OR　Programming Card ③ ③ ✱ ⑨ ① ⑨ ✱ ·····················► New [CODE] ✱ ✱ (for CODE only)　OR　New Card add another credential　OR　✱ to finish	Wait for green LED to stop blinking between each step.
Main + Aux Toggle	[Programming Code] ✱　OR　Programming Card ③ ③ ✱ ⑨ ⑨ ① ✱ ·····················► New [CODE] ✱ ✱ (for CODE only)　OR　New Card add another credential　OR　✱ to finish	Wait for green LED to stop blinking between each step.
Change Relock Delay	[Programming Code] ✱　OR　Programming Card ⑨ ⑨ ✱ ① ✱ Each button press adds to the total delay time Example: ① + ⑨ adds a 10 second delay ✱ to finish	Wait for green LED to stop blinking between each step.
Change PIN Length	[Programming Code] ✱　OR　Programming Card ⑨ ⑨ ✱ ④ ✱ Press ③, ④, ⑤, OR ⑥ for desired PIN length ✱ to finish	Wait for green LED to stop blinking between each step.

1 Other lights may show before the final confirmation. Wait for the final confirmation before continuing to the next step.

Manual programming error codes

ⓘ **Error codes are indicated at the reader by a blinking red LED. The number of red blinks indicates the error code.**

ⓘ **The CT5000 may not provide complete control of the reader's beeper or LEDs. Please consult the reader's manufacturer for instruction on reader configuration.**

Number of red blinks	Error code description
1	Computer programming error (not complete).
2	Too long user/master code entered. Master code length must be five (5) digits. User code length cannot exceed 6 digits.
3	Memory full, too many codes. Delete some codes.
4	Master code cannot be deleted, only changed.
5	Master code entries do not match. Master code not changed.
6	Invalid command. Invalid function code entered.
7	Code not found.
8	Code too short. Master 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.

Using the CT5000 controller

After credentials have been programmed, present credentials to operate the CT5000 controller as follows:

Credential type	Action
Credential	Present credential to reader ➔ Green blink and access granted
+ PIN Credential	Present credential to reader ➔ Press PIN ➔[1] Green blink and access granted

1 The default PIN length is six digits. The "#" key must be used as an ENTER key for PINs with fewer than six digits. PIN length can be manually configured (refer to *Change PIN Length* on page 19).

Reader LED reference

The CT5000 supports independent reader LED and beeper operation. The credential reader being used may or may not allow independent control of the reader's LEDs. Please consult the credential reader's manufacturer for instruction on reader configuration.

The table below represents the operation of most available credential readers. LED feedback during manual programming may differ depending on the reader configuration used.

Reader condition	Reader LED
Access denied	2 red blinks
Access denied, user outside time zone	4 red blinks
Factory default reset	No LED indicator while clearing memory, then a one-second solid green and one beep when complete
Waiting for PIN (Card + PIN)	5 alternating red and green blinks
Low battery indicator, coin cell battery	1 green and 3 red blinks before valid access
Momentary unsecured access	Solid green while unlocked

Reader condition	Reader LED
Toggle unsecured	Solid green while unlocked
Toggle secure (relocking)	Solid red
Access denied, frozen secured or holiday restricted secured	12 red blinks

CT5000 coin cell battery

When installing the CT5000, after power is applied, remove the mylar strip from the coin cell battery.

When the coin cell battery is low, the CT5000 will provide a delay after acceptance of a valid credential, and the POWER/TAMPER LED (LED7) will blink rapidly. The reader's LED will indicate low battery with one green blink and three red blinks before allowing access.

ⓘ **Replace the CT5000's coin cell battery with Panasonic CR-2025 only. Use of another battery may present a risk of fire or explosion.**

CAUTION! Risk of fire, explosion, and burns. Do not recharge, disassemble, heat above 100°C or incinerate.

Test

Test the CT5000 with power applied
1. The POWER/TAMPER LED will blink green when the CT5000 lid is removed, and will light solid green when the lid tamper switch is pressed.
2. Most readers are designed to function independently of the CT5000. If the reader's LED and beeper performance is irregular or unexpected, refer to the instructions that came with the reader.

Schlage button test
ⓘ **Performing the Schlage button test will not result in the loss of any CT5000 settings or programming changes.**
1. While holding the SCHLAGE button, press and release the RESET button.
2. All relays, on-board LEDs, reader LEDs and reader beeper will be active while the SCHLAGE button is pressed.

CT5000 in construction mode
1. After programming a Construction Credential (refer to page 15), present a valid Construction Credential to the reader.
2. The CT5000 Strike relay will activate for the length of the default relock delay. The Auxiliary relay will not activate.

CT5000 and door file test
1. Present a valid credential to the reader.
2. The CT5000's STRIKE relay and STRIKE LED will activate for the relock delay, and the reader's green LED will blink. **A valid credential will not activate the AUX relay unless the door file has given the credential authorization to do so.**
3. If the credential is not accepted, the reader's red LED will blink twice.

The audit file is capable of indicating the status for *Anti-Tamper Switch Activated*, and *Door Propped Open* or *Door Forced Open*. For *Door Propped Open* or *Door Forced Open,* the Door Position Switch must be configured using the HHD.

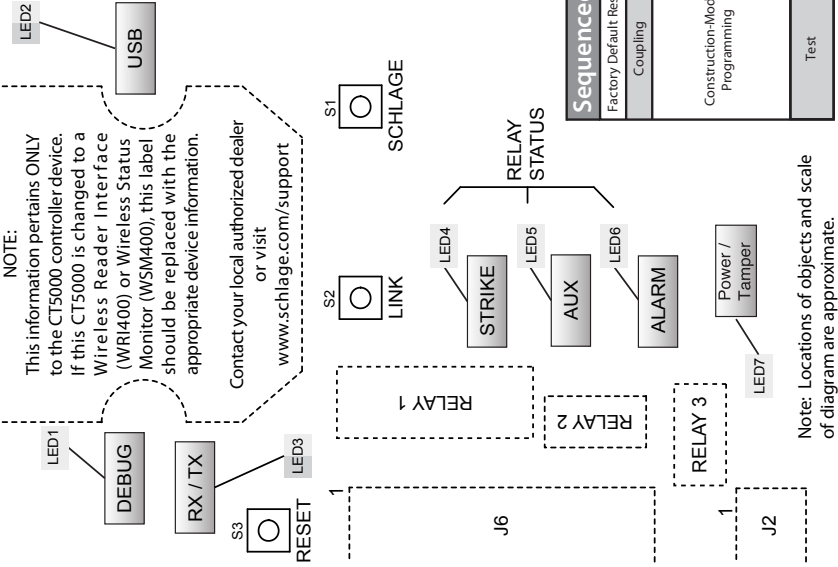| Problem	Problem indication	Solution
CT5000 is not operating	No blink from PWR/TAMPER LED	Confirm connection to external power supply. See *Wiring diagram CT5000 x magnetic lock* on page 10, page 11 and page 12.
		The PWR/TAMPER LED should flash green when the CT5000 is powered and the lid is removed.
		Confirm the J8 jumper is in LINE position.
The credential reader is not operating properly	The CT5000 STRIKE Relay/LED is not activated when a card or keypad credential is presented	Confirm that the four (4) connections required for basic operation readers are properly connected: Power, Ground, CLK/D1 and DATA/D0.
		Confirm that CLK/D1 and DATA/D0 wiring is not reversed.
		Consult the reader's user guide and confirm that the reader has specified power.
	The reader's beeper and/or LED is not functioning as expected	The CT5000 does not configure and may not control the reader's beeper or LED settings.
		Consult the reader's user guide for more information on configuring the reader's beeper or LED patterns.
HHD is not communicating with the CT5000	No USB LED	Make sure the USB connector is properly connected. The USB LED will blink green.
	HHD display reads "No Device Connected"	Set the HHD connection type to "USB". See *Handheld Device (HHD)* on page 14.
Unable to configure settings with HHD	HHD display reads "Your HHD is not authenticated to perform this action"	Check that the HHD is properly coupled to the CT5000. See *Handheld Device (HHD)* on page 14.

Important things to know before calling technical service:
- The CT5000 may not provide complete control of the reader's beeper or LEDs. Please consult the reader's manufacturer for instruction on reader configuration.
- The two reader inputs on the CT5000 are independent inputs. Both have the same access control rights.
- AUX relay action is assigned by the door programming. A credential must have AUX relay rights before the CT5000 will activate the AUX relay. The AUX relay will activate **only when the CT5000 is in normal operating mode**.
- When the CT5000 is operating in construction mode, only the strike relay will activate for access.

CT5000 LED reference

LED	Condition	CT5000
STRIKE (LED4)	Solid GREEN	Relay energized
	OFF	Relay de-energized
AUX (LED5)	Solid GREEN	Relay energized
	OFF	Relay de-energized
ALARM (LED6)	Solid GREEN	Relay energized
	OFF	Relay de-energized
Power/Tamper (LED7)	Solid GREEN	Cover on
	Slow GREEN flashing	Cover off
	Fast GREEN flashing	Coin Cell battery voltage critical
USB (LED2)	Alternating RED/GREEN	SUS coupling
	Slow GREEN flashing	USB connected
DEBUG (LED1)	GREEN for 1 second	Factory Default Reset completed successfully
	5 Quick GREEN flashes	Master construction credential programmed successfully / user construction credential programmed successfully / 20-sec timeout
	Solid GREEN (20 seconds-max)	Waiting for user construction credential, after master presented

Sequenced Operations

Factory Default Reset	Press and hold **BOTH SCHLAGE** and **LINK** buttons for **3 secs.**
Coupling	Press and hold **SCHLAGE** button, press **LINK** button **3 times** within **5 secs.** Coupling window is enabled for **30 secs.**
Construction-Mode Programming	**To program a master construction credential *:** Press and hold **SCHLAGE** button, then present valid credential to the reader within 5 secs. If the credential is not presented within 5 seconds, time-out will occur. * Note: CT5000 must be in factory default state to program the master construction credential. **To program each user construction credential:** Present the master construction credential to the reader. The DEBUG LED will light green. Present the credential to be programmed to the reader within 20 seconds or time-out will occur.
Test	While holding the **SCHLAGE** button, press and release **RESET** button. All relays, onboard LEDs, reader LEDs, and reader beeper will remain active while the **SCHLAGE** button is pressed.

NOTE:
This information pertains ONLY to the CT5000 controller device. If this CT5000 is changed to a Wireless Reader Interface (WRI400) or Wireless Status Monitor (WSM400), this label should be replaced with the appropriate device information.

Contact your local authorized dealer or visit www.schlage.com/support

LED2 — USB
S1 — SCHLAGE
S2 — LINK
RELAY STATUS
LED4 — STRIKE
LED5 — AUX
LED6 — ALARM
LED7 — Power / Tamper
LED1 — DEBUG
RX / TX
LED3
S3 — RESET
RELAY 1
RELAY 2
RELAY 3
J6
J2
1

Note: Locations of objects and scale of diagram are approximate.

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

© Allegion 2018
Printed in U.S.A.
P516-104 Rev. 05/18-e