TS0870x Smart Card Reader Installation and Programming Guide

P/N MAINST-TS0870 • REV 6.1 • ISS 10JAN25

Copyright

©2025 Aritech, All rights reserved.

Trademarks and patents

The TS0870x Smart Card Reader name and logo are trademarks of KGS Fire and Security Australia Pty. Ltd.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products

Manufacturer

Made in China by KGS Safety System (Hebei) Co., Ltd.
No. 80, Changjiang East Road, QETDZ, Qinhuangdao, Hebei, P. R. China 066004

Imported by KGS Fire and Security Australia Pty Ltd
Suite 4.01, 2 Ferntree Place,
Notting Hill, Victoria, 3168, Australia

Product warnings and disclaimers

THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. KGS FIRE AND SECURITY AUSTRALIA PTY. LTD. CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY “AUTHORIZED DEALER” OR “AUTHORIZED RESELLER”, IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.

For more information on warranty disclaimers and product safety information, please check https://aritech.com.au/aritech-product-warranty/ or scan the QR code.

ACMA compliance

N4131

When installed as directed, this product conforms to the standards set by Standards Australia on behalf of the Australian Communications and Media Authority (ACMA).

Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Contact information

For contact information, see www.aritech.com.au

Content

Important information

Disclaimer

The customer is responsible for testing and determining the suitability of this product for specific applications. In no event is KGS Fire and Security Australia Pty Ltd (trading as Aritech) responsible or liable for any damages incurred by the buyer or any third party arising from its use, or their inability to use the product.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

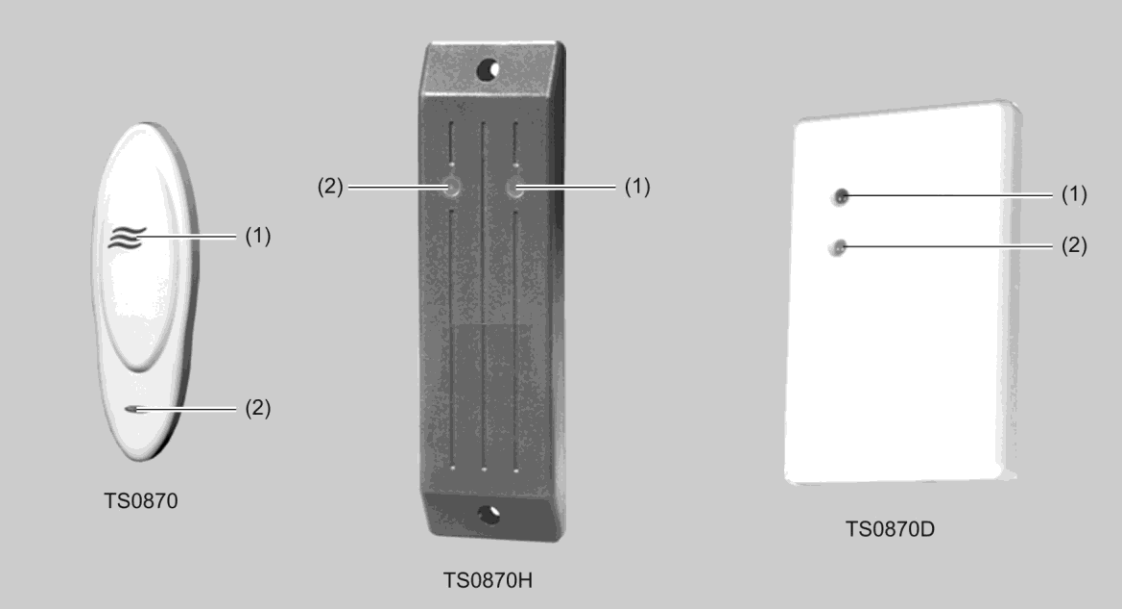
Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Product overview

The TS0870, TS0870H (heavy duty), and TS0870D (decorative) Smart Card Readers are multifunction, all-purpose proximity card readers suitable for most locations requiring a short-range reader.

Figure 1: Locations of blue LED (1) and red LED (2) on TS0870 models



Product features include:

- Programmable via an LCD RAS on the LAN or by using a reader configuration card.
- In systems with Intelligent User Memory (IUM), readers can use the unique card serial number on blank (un-programmed) Smart Cards for access control.
- Readers can be used in online mode (connected to system LAN or door/lift controller sub-LAN), or offline mode (connected to Wiegand interface) with little or no programming.
- Operates from 9 V to 14 V DC and has a quiescent current consumption less than 25 mA (less than 80 mA when reading a card).
- The TS0870 Smart Card Reader is supplied standard with a white removable dress cover that may be interchanged with one of a range of other colours (shown above in white). The TS0870D is supplied with an easily-installed, removable white Clipsal dress cover.
- Readers can be used as a standalone reader with a credit facility for use with photocopiers, soft drink vending machines, and other systems.

Specifications

Voltage	Nominal 13.8 VDC (9 to 14 VDC)
Read range	Approximately 7 cm (depending on environment)
Power consumption	
Maximum	80 mA @ 13.8 VDC
Normal (all areas armed)	25 mA @ 13.8 VDC
Maximum open collector current	50 mA @ 14 VDC
Operating environment	
Temperature	-35 to 66°C
Humidity	0 to 95% noncondensing
IP rating	IP54
Dimensions with cover (W x H x D)	
TS0870	36 x 110 x 20 mm
TS0870H	42 x 150 x 16 mm
TS0870D	74 x 115 x 13 mm

Installation

Notice! A qualified service person, complying with all applicable codes, should perform all required hardware installation.

Product contents

Table 1: TS0870x Smart Card Reader shipping list

Quantity	Item
1	Smart Card Reader
1	White dress cover (for TS0870 or TS0870D)
1	470 Ω end-of-line resistor
1	Installation and Programming Guide

Inspect the package and contents for visible damage. If any components are damaged or missing, do not use the unit; contact the supplier immediately. If you need to return the unit, you must ship it in the original box.

Before you begin

Before you can successfully install the reader you need to know some details about the system, depending on whether the reader is to be normally used in *online* or *offline* mode. These modes are described in the following sections.

Online mode

A reader connected to a controller's RS-485 LAN is said to be online, and you need to know:

- The LAN address.
- The system layout, in order to fit the LAN termination end-of-line resistor (if required).
- Whether you need to install RTE (request to exit, or egress) via a push button.
- Whether the reader is to be powered from the LAN or from a separate 12 V power supply, such as TS0073.

If the new reader is to be used on an RS-485 LAN you must have some means to program polling to the new reader, such as:

- By using a RAS with a liquid crystal display (LCD) on the LAN.
- By using the system management software (such as TITAN, Ares, Forcefield, or Security Commander).

Offline mode

A reader connected to a Wiegand interface, is said to be offline, and you need to know:

- Whether a tamper input is required. If a tamper input is required you need to connect a 10K resistor via the violet wire (see Figure 4) to a zone input, and configure the open collector output as Tamper. See *RAS Menu Option 8. Open Collector Output* on page 15. For later versions of 4-door/4-lift intelligent access controller firmware, the reader watch dog option may be used to monitor the reader tamper. See *Using tamper functionality* on page 7.
- Whether the reader is to be programmed for one-wire or two-wire LED control. See RAS Menu Option 2. LEDs Off-Line on page15.

Mounting the reader

Mount the reader on any flat surface with two pan-head screws, 3.0 to 3.5 mm diameter. Do not use countersunk screws, as they may damage the reader.

When mounting TS0870 or TS0870D readers:

- Gently prise or pull cover from the main body to remove the dress cover and expose the mounting screw holes. Avoid using excessive force as you may damage the reader.
- If mounting in an outdoor environment, ensure that the blue LED is at the top.
- After mounting, gently press the cover over the main body until it locks into place.

A slightly reduced card reading range occurs when mounted on a metal surface.

RS-485 LAN termination

Smart Card readers are not fitted with a LAN termination 'TERM' switch or link. A 470 Ω end-of-line resistor (supplied) is used for LAN termination. Connect the end-of-line resistor between the green and white wires (D+ and D–) when the LAN termination needs to be ON.

If the reader is the last device on the RS-485 LAN the LAN termination should be ON. In a star wiring configuration, the RS-485 LAN may consist of a number of cable runs (branches). LAN termination should be set to ON only at the devices at the far ends of the two longest branches. A star LAN that has multiple branches in excess of 100 m may need to use TS0893 Isolated RS-485 to RS-485 Interface modules to isolate the LAN segments that do not have LAN termination set to ON.

Programming the reader's address

Smart Card Readers have a default LAN address of 16. Changing the LAN address is described in *Programming* on page 11.

Using tamper functionality

The reader has an optical tamper. When connected to the LAN, tamper data is transmitted to the control panel along with system data. If the TS0870D is mounted onto a compatible mounting block (instead of flush mounting), then it may be necessary to disable the RAS tamper. Refer to programming option *17—Tamper Options* on page 18 for details.

An external open collector output (violet wire) may be configured as a tamper control for offline mode.

For TS0870x readers with firmware version V07 or later, the watch dog option may be used to monitor the tamper for offline mode. Wiegand watch dog data is transmitted when the tamper is sealed. See option 7—Watch Dog on page 15 for details.

Wiring details

TS0870x readers can be used in a variety of applications. Insulate and secure any unused wires.

Table 2: Reader wire applications

Colour	Application	Colour	Application
Red	+12 V nominal (9 to 14 VDC supply)	Black	0V (DC supply ground)
Brown	Configurable via programming of RAS menu option 2—LEDs Off-line. When set to two-wire control, the brown wire controls the red LED: • Grounded, red LED on. • Open or at +5 V to +14 V, red LED off. When set to one-wire control, the brown wire controls both the red and the blue LEDs: • Grounded, blue LED on. • Open, both LEDs off. • At +5 V to +14 V, red LED on.	Yellow	Configurable via programming of RAS menu option 2— LEDs Off-line. When set to two-wire control, the yellow wire controls the blue LED: • Grounded, blue LED on. • Open or at +5 V to +14 V, blue LED off. Configurable via programming of RAS menu option 10—RTE (Egress). Connect the yellow wire to a normally open push button and select “Door Relay” in option 8—O/C Output.
Green	D0/D– /Clock, may be used for: • D0 (Wiegand data) • D– (RS-485 data) • Magnetic stripe clock Absolute maximum voltage +12 V @ 10 mA.	Blue	Buzzer/beeper, may be used for offline buzzer control: • Open or +5 V to +12 V, buzzer off • Grounded (0V), buzzer on.

Colour	Application	Colour	Application
White	D1/D+ /Data, may be used for: • D1 (Wiegand data) • D+ (RS-485 data) • Magnetic stripe data Absolute maximum voltage +12 V @ 10 mA.	Violet	Open collector — Configurable as door relay, tamper output, or magnetic stripe data present. This is a low current output and must not be used to directly energize high current door openers. Absolute maximum 14 V @ 50 mA.

Connections

The following connection diagrams depict a TS0870 reader. Details are the same for TS0870H and TS0870D models.

LAN connection (D+ and D–)

The reader is connected to the Challenger panel via the RS-485 LAN, with a LAN cable length of up to 1.5 km from the control panel or the four-door controller. We recommend that you use 2-pair twisted shielded data cable (such as Belden 8723) for the RS-485 LAN.

The shield of any LAN cable must be connected to system ground at one end only. The reader is not provided with an Earth connection for this purpose. If the LAN is ‘daisy-chained’ to the reader, ensure that the shield of the cable is jointed to provide continuity of data cable shield.

The white wire is the D+ (data positive) connection of the LAN data bus. The green wire is the D– (data negative) connection of the LAN data bus. Connect the end-of-line resistor between the green and white wires if the reader is the last device on the LAN. Refer to the control panel’s installation manual for details.

Figure 2: LAN connections to Challenger panel

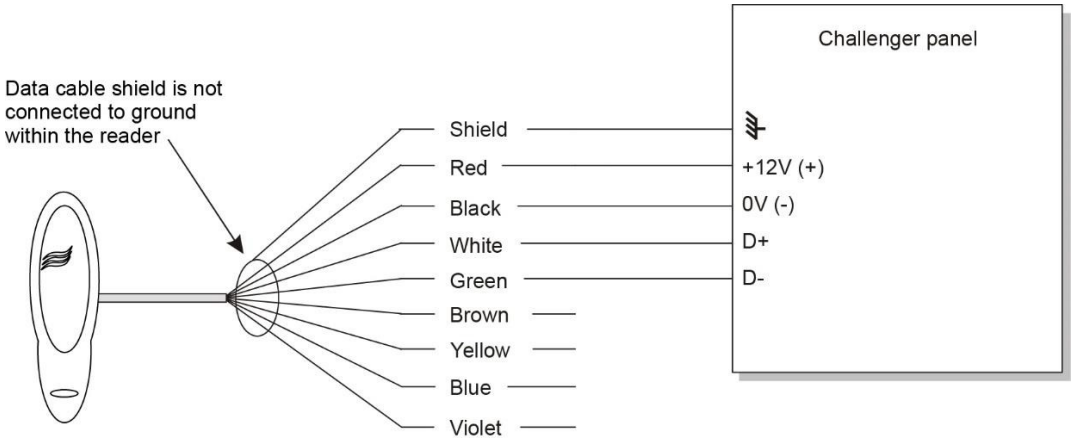
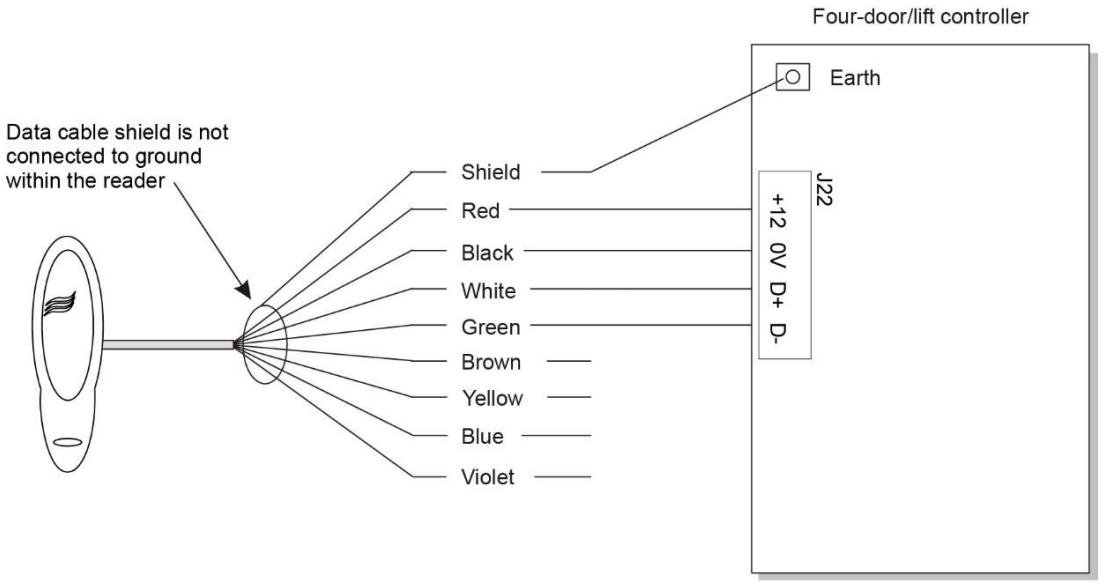
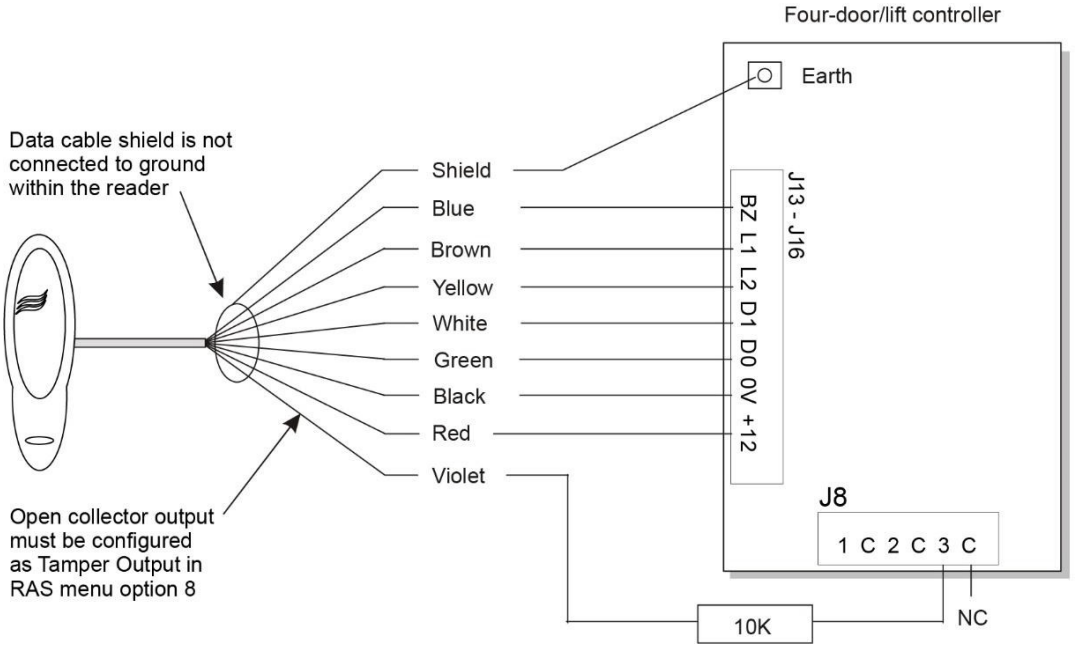


Figure 3: LAN connection to Intelligent 4-Door or 4-Lift Controller



Wiegand connection

Figure 4: 'Offline' mode connection to Wiegand interface (with optional tamper input)



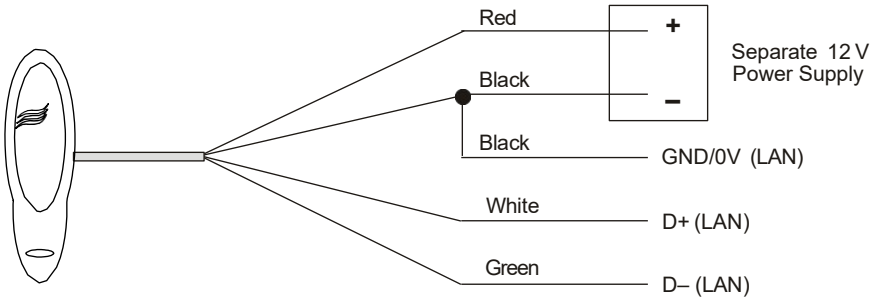
Auxiliary power supply (+12 and 0V)

The reader can be powered using the LAN + and – power from the control panel or Intelligent Access Controller if the cabling distance is no more than 100 m (if using Belden 8723). Use a separate power supply (such as TS0073) if the cable length is greater than 100 m, or if electrical isolation is required.

When using an auxiliary power supply:

- Connect the ‘+’ of the local power supply to the red wire of the reader. Do not connect the + power of the LAN to the reader.
- Connect the ‘–’ of the local power supply to the black wire of the reader and to the – power of the LAN.
- For optimal performance, adjust the power supply to 13.8 VDC.

Figure 5: Connections for powering the reader from a separate power supply



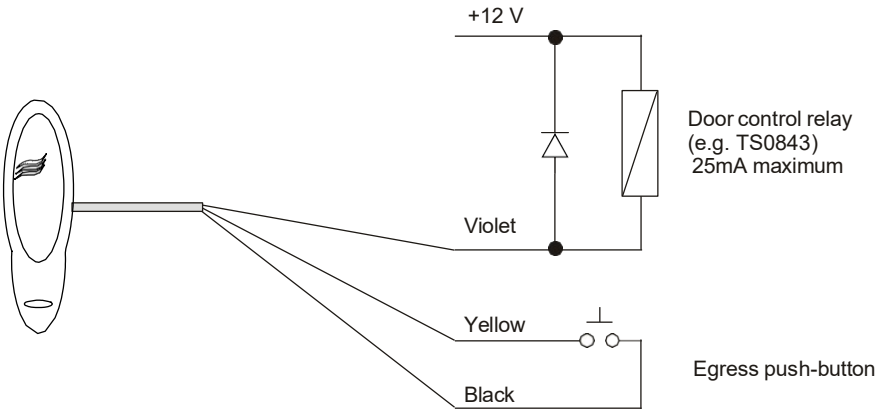
Egress control and open collector

The yellow and violet wires are optionally used for egress control and door relay operation when the reader is connected to the LAN.

Yellow wire — An Egress button (normally open, momentary push-button switch) can be connected across the yellow and black wires (see Figure 6). When pressed, the button controls the request to exit function to the panel.

Violet wire — Open collector output must be assigned with the first relay number of the relay control group assigned to the reader.

Figure 6: Door relay and simple push button connections



Programming

Readers can be programmed for use in ‘unsecured’ or ‘secured’ mode (see *16—Security mode* on page 18 for details).

There are two main methods that can be used to program (configure) readers:

- Using an LCD RAS on the system LAN (or on the door/lift controller sub-LAN) and polling the reader. See *Method A — Using a RAS* below.
- Using a reader configuration card. See Method B — Using a reader configuration card on page 12.

Method A — Using a RAS

This method is not suitable for the initial programming of readers for use in secured mode. Use only *Method B — Using a reader configuration card* on page 12 for secured mode.

In order to program a reader via an LCD RAS, you must first be able to communicate with the reader. This is accomplished by polling the reader from the panel, or the door/lift controller, as applicable. You must have an LCD RAS connected to the system LAN (or on the door/lift controller sub-LAN).

- When connected to the system LAN, polling is enabled via Installer menu 3-RAS Database. Once polled, access the reader menu via option 28 – Remote Controllers.
- When connected to a door/lift controller sub-LAN, you must first enable polling for the address of the controller via Installer advanced menu 28 – To Remote Devices, option 1 (DGP). The Door/Lift Controller Options menu is used to enable polling at the RAS address.

Refer to the specific control panel or door/lift controller programming manuals for details about accessing the RAS menu and enabling polling.

In both cases, the overall process is as follows.

1. Poll the reader at address 16.
2. Use an LCD RAS to program the required address (except for a reader that’s supposed to be at address 16). You can also change other reader programming from the factory defaults at this time. Refer to *Reader programming* on page 14 for details about the programming options that apply to the TS0870x-series Smart Card Readers.
3. When finished programming the reader, exit the RAS menu to apply the new programming.
4. Poll the reader at the required address.
5. When finished adding readers, de-poll address 16 (if not needed for a reader).

Method B — Using a reader configuration card

This method is required for programming readers for use in secured mode. This is the only means of transferring the security password to the reader.

Reader configuration cards may be used in two ways:

- A reader configuration card may be programmed for the individual reader (including the LAN address). See *Single-address programming* below.
- A reader configuration card may be programmed generically (without a LAN address). The reader address is then set using the built-in beeper to select the required address. See *Multi-address programming* on page13.

Single-address programming

You can create a reader configuration card to program a single reader. The reader configuration card is used only for a reader at the address programmed into the reader configuration card.

The reader configuration card is programmed using appropriate software (e.g. TITAN, Alliance, etc.) in conjunction with a TS0870P Smart Card Programmer. Refer to the management software online help for details of how to program the reader configuration card.

Refer to *Reader programming* on page 14 for details about the programming options that apply to the TS0870x-series Smart Card Readers.

Use the following steps to program the reader:

1. Program the reader configuration card with the options required for the reader, including the required address.
2. Connect the reader to the LAN or sub-LAN or a 12 VDC supply as described in the *Installation Guide*.
3. Enable polling for RAS address 16, and enable polling for the required address (if not address 16).
4. Badge the reader configuration card once. The reader will beep either one or two times.

   A single beep indicates that the details programmed into the reader configuration card are identical to the details programmed into the reader. Two beeps indicates that the details programmed into the reader configuration card are different from the details programmed into the reader (this is the expected result).

   After a few seconds, the reader will begin three sets of coded beeps to indicate its current address. Refer to *Beep codes for LAN addresses* on page 14 to interpret the coded beeps.
5. The reader will respond to polling at its new address after the next four coded address beeps.
6. When finished adding readers, de-poll address 16 (if not needed for a reader).

Multi-address programming

Use an ATS1481 Reader Configuration Card, or create a reader configuration card to program multiple readers, regardless of address. The required address is set using the reader's built-in beeper.

The reader configuration card is programmed using the system management software (e.g. TITAN, Forcefield, Alliance, etc.) in conjunction with a TS0870P Smart Card Programmer. Refer to the management software online help for details of how to program the reader configuration card.

Refer to *Reader programming* on page 14 for details about the programming options that apply to the TS0870x-series Smart Card Readers.

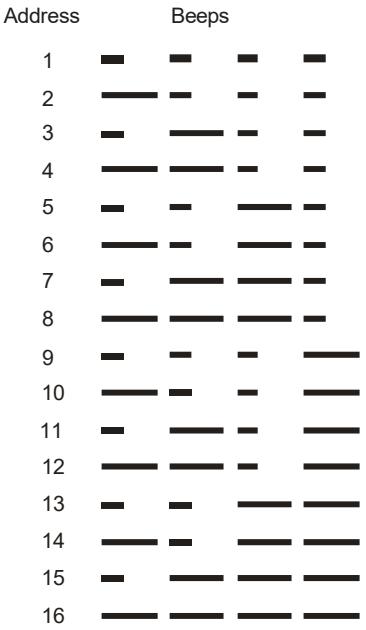
Use the following steps to program the reader:

1. Program the reader configuration card with the details required for the reader, leaving the address field blank.
2. Connect the reader to the LAN or sub-LAN or a 12 VDC supply as described in the *Installation Guide*.
3. Enable polling for RAS address 16, and enable polling for the required address (if not address 16).
4. Badge the reader configuration card once. After a few seconds, the reader will begin three sets of coded beeps to indicate its current address of 16. Refer to *Beep codes for LAN addresses* on page 14 to interpret the coded beeps.
5. Before the three sets of coded beeps stop, badge the reader configuration card one time again to change the reader address from the default of 16 to address 1.
6. If required, badge the reader configuration card one time again to increment the address to 2, and repeat until the required address is reached (after address 16 it will revert to address 1 again).
7. The reader will respond to polling at its new address after the next four coded address beeps.
8. When finished adding readers, de-poll address 16 (if not needed for a reader).

Beep codes for LAN addresses

The image in Figure 7 below (also printed on the ATS1481 Reader Configuration Card) shows the beep lengths for each RAS address.

Figure 7: RAS address beep coding (four long beeps indicates LAN address 16)



Unlocking a reader

If the reader configuration card is programmed with the option 9—Option Card value set to disable, then the reader configuration card may be used only to initially set the RAS address (whilst the reader continues beeping). After the beeping stops, the reader is locked against further changes by a reader configuration card. See *9—Option Card* on page 16 for details about enabling the use of the reader configuration card.

Reader programming

This section describes the reader menu options as displayed on an LCD RAS. If using system management software and a Smart Card Programmer to program a reader configuration card, use this section for reference purposes when programming using the management software (along with the management software online help).

Reader Menu Option	Description
1—LEDs Online *The reader is 'online' when connected to system LAN or sub-LAN.*	Programs the online actions of the blue and red LEDs. The default setting is: • Blue LED — Door Unlocked Only • Red LED — Armed Select option 1 to program the blue LED. One of the following options displays: • Door Unlocked Only — Blue LED flashes when the door is open. • Area Disarmed + Door Unlocked — Blue LED flashes when the door is open, and remains on when the area is disarmed. Press * to change (toggle between the options), or press ENTER to select the displayed setting. Select option 2 to program the red LED. One of the following options displays: • Area Armed — Red LED remains on when the area is armed. • Area Armed + Door Unlocked — Red LED flashes when the door is open, and remains on when the area is armed. Press * to change (toggle between the options), or press ENTER to select the displayed setting.
2—LEDs Offline *The reader is 'offline' when connected to Wiegand interface.*	Programs the offline control of the LEDs. The options are: • Two-wire LED control (default setting) — The red LED is controlled by the brown wire and the blue LED is controlled by the yellow wire. • One-wire LED control — Both the blue LED and the red LED are controlled by the brown wire. Press * to change (toggle between the options), or press ENTER to select the displayed setting.
3—Valid Card Flash	If enabled, the blue LED will give one short flash when the card is badged. The panel controls subsequent flashes.
4—Night Light	If enabled, and the blue LED is required to be off, the blue LED will always be dimly lit.
5—Protocol Options	Select either Wiegand or Magnetic stripe to determine the method by which the card reader sends data to the panel. Refer to *Data transmission details* on page 20 for details. The result of this selection is further determined by the reader's operating modes: • online or offline, and • secured or unsecured (see option 16).
6—Card Beep	If enabled, the beeper will give a short beep when a card is badged. The panel controls subsequent beeper activity.
7—Watch Dog	Offline mode only. If enabled, data is sent to the host every one minute to indicate that the RAS is connected and operating normally. The tamper must be sealed for watch dog messages to be transmitted.

8—O/C Output (Open Collector Output)	Select one of the following options: • Door relay (online mode only) — The open collector output activates (active low) when the door open signal is received by the TS0870x. • Tamper (online or offline modes) — The open collector output activates (active low) when the tamper is unsealed (if enabled in option 17—Tamper Options). • Mag Stripe Data Present (offline mode only) — The open collector output activates (active low) when the card data is being sent to the host. • Credit Relay Pulsed — The relay output will operate as a pulsed output (active low) when the reader is configured to operate as a credit activated device, and a credit transaction is completed. The pulse width is configurable from 10 milliseconds to 2.55 seconds on a configuration card. See *Programming credit options* on page 18. • Credit Relay Timed — The relay output operates as a timed output (active low) when the reader is configured to operate as a credit activated device, and a credit transaction is completed. The time is configurable from 1 to 65535 seconds, multiplied by the relay time factor. See *Programming credit options* on page 18. • Credit Relay Latched — The relay output operates as a latched output if the reader is configured to operate as a credit activated device. When a Smart Card with valid credit data is badged and the transaction is successfully completed, the relay output is turned on. The relay output is turned off when a valid Smart Card is badged next, with or without credits. See *Programming credit options* on page 18.
9—Option Card	If enabled, reader configuration (option) cards may be used to program the card reader any number of times. If disabled, reader configuration cards are ignored. If disabled, this option cannot be re-enabled using a configuration card. It may only be re-enabled by the following means: • Using menu option 9—Option Card. • Using menu option 11—Factory Defaults. • By badging a default configuration card on the reader.
10—RTE (request to exit, or egress)	The RAS may be connected to a simple push button. The open collector output may be used to control a door relay. RTE control is available only when the card reader is online. Select one of the following options: • RTE Disabled. When egress is not used, it is recommended that it be disabled. • RTE Only. This option requires a simple push button to be connected. A press of the button will release the door lock relay. To implement RTE only, connect the yellow wire to a normally open push button and select “Door Relay” in option 8—O/C Output. • RTE + Arm/Disarm. This option is used with the TS0064 Expanded Button Interface (discontinued product) to Arm and Disarm areas. See the alarm panel programming guide for details.

11—Factory Defaults	Restores the RAS options to the factory default settings. These are: 1—LEDs Online (blue LED indicates door open, red LED indicates secure) 2—LEDs Offline (two wire control) 3—Valid Card Flash (enabled) 4— Night Light (enabled) 5— Protocol Options (Wiegand) 6— Card Beep (enabled) 7—Watch Dog (disabled) 8—O/C Output (door relay) 9— Option Card (enabled) 10— RTE (disabled) 12—Reader address (RAS 16) 14—Credit Setup (disabled) 16—Security mode (unsecured) 17—Tamper Options (enabled)
12—Reader address	Changes the reader address from the default 16 to the required address.
13—Last Card	This menu option is not a programming option, it is a display (on an LCD RAS) of the most recent card data read by the designated RAS address. The format of the data displayed depends on whether the card was in unsecured or secured mode. In unsecured mode, the last card badged displays in the format XXX, XXX, XXX, XXX, XXX, XXX where XXX is a decimal number. In secured mode, the last card badged displays in the format FC=XXXXX, ID=YYYYYYY where XXXXX is the 5-digit site (facility) code and YYYYYYY is the 7-digit card number.
14—Credit Setup	This option is used for credit functionality. See *Programming credit options* on page 18.
15—Last Card Credit	This option is used for credit functionality. See *Programming credit options* on page 18. Use this option to display on an LCD RAS the details of the most recent valid credit Smart Card transaction. Each successive screen indicates the following card details: • The location identifier numbers assigned to thecard. • The access level assigned to the card. • Account number and credit units balance for each of the four possible accounts in sequence. A credit units balance of ***** indicates that the card is a ‘master’ card with unlimited credits.

16—Security mode	Smart cards may be used in either the default unsecured mode or in secured mode. The card reader must be programmed to use the same security mode as the cards. The modes are as follows: • **Unsecured** mode allows the reader to recognise blank or un-programmed user cards by using the card's unique serial number. Unsecured mode can be used in Intelligent User Memory (IUM) systems only. • **Secured** mode requires the use of a Smart Card Programmer to program user cards and reader configuration cards with a card security password. The card security password ensures that a reader configuration card or a reader default card from one system cannot be used to reprogram readers in another system. Refer to the *TS0870P Smart Card Programmer Installation Sheet* for details.
17—Tamper Options	If enabled (default setting), the optical tamper states are sent to the panel. If disabled, tamper states are not sent to the panel. If disabled, this option cannot be re-enabled using a configuration card. It may only be re-enabled by the following means: • Using menu option 17—Tamper Options. • Using menu option 11—Factory Defaults. • By badging a default configuration card on the reader.

Programming credit options

TS0870x-series Smart Card Readers can be set-up to respond to badging by operating relay-activated devices such as photocopiers, drink dispensers, etc., instead of being used for access purposes. To do so, the Smart Card must be programmed with the correct access level, credits, and location, in order to activate the relay output.

The credit Smart Card Reader is programmed using the same methods as described in *Programming* on page 11.

You can check the credit status of a Smart Card by using the RAS menu option *15—Last Card Credit* described on page 17.

Whether programming the credit Smart Card Reader using a reader configuration card, or using an LCD RAS, the requirements are the same. These are:

- The reader's token value must be greater than zero. See Reader token value on page 19.
- The card being badged must have a credit account number (1 through 4) that matches the reader's credit account number. See Credit account number on page 19.
- The card being badged must have an access level (1 through 16) that is equal to or greater than the reader's access level. See Access level on page 19,
- The card being badged must have a location identifier (1 through 4) that matches the reader's location identifier. See Location identifier on page 19.

- The card being badged must have a credit units balance that is equal to or greater than the reader's token value.

The following sections appear in the same order as they are accessed via an LCD RAS using option 14—Credit Setup.

Reader token value

Enter a number in the range of 1 through 65534 to specify the reader's token value. The token value sets how many credits equal one token, to be deducted when a card is badged.

Example: On a photocopier, one token equals two credits (one credit equals 10 cents). Each time an A4 copy is made with the card, one token is deducted (two credits or 20 cents).

Note: Enter the special value 65535 to program a card with unlimited credits (the token value is not deducted when a card is badged).

Credit account number

Enter a number in the range of 1 through 4 to identify the reader's active credit account.

Access level

Enter a number in the range of 1 through 16 to identify the reader's access level.

Example: A Smart Card reader at a photocopier has an access level of 4 (which permits operation by users with access levels of 4 through 16). If a user has a card with access level 5, then they can use the photocopier. Another user with a card with credit access level of 2 cannot use the photocopier.

Location identifier

Enter a number in the range of 1 through 4 to identify the reader's location.

Example: You might have already given some staff the highest access level of 16, but you want to prevent them from using the admin photocopier. If the admin photocopier has a location identifier of 2 and the staff have cards with a location identifier of 1, then they cannot use the photocopier.

Relay time factor

Enter a number in the range of 1 through 256 to specify the relay time factor. The relay time factor modifies the pulse width output of the Credit Relay Pulsed option or the energised time for the Credit Relay Timed option (whichever is defined in option *8—O/C Output* on page 16).

The pulse width for the Credit Relay Pulsed option is the relay time factor multiplied by .01 seconds (10 milliseconds). This gives a pulse width between 0.01 – 2.56 seconds.

The activation time for the Credit Relay Timed option is the relay time factor multiplied by the token value of the reader. This gives a range of between 1 second and around 193 days.

Data transmission details

The following tables list the formats by which the card reader transmits data, as determined by:

- Whether the reader is used online or offline, and by
- Menu option 5—Protocol Options (Wiegand or Magnetic stripe), andby
- Menu option 16—Secured mode (Secured or Unsecured).

Note: In online mode, select ‘Wiegand’ in menu 5 to use 26 or 27 bit data, or select ‘Magnetic stripe’ to use 32 bit data.

Table 3: Online mode (connected to the RS-485 LAN)

Online	26 or 27 bit data	32 bit data
Card format: Secured	When a secured card (4-byte code used) is badged on a reader using the Wiegand protocol, 26 or 27 bit data is transmitted, depending on whether the card is programmed as Standard 26 bit or Tecom 27 bit ASC.	When a secured card (4-byte code used) is badged on a reader using the magnetic stripe protocol, 32 bit data is transmitted.
Card format: Unsecured	When an unsecured card (4-byte code not used) is badged on a reader, the full 32 bit card ID data is always transmitted to the panel.	

Table 4: Offline mode (connected to a Wiegand interface)

Offline	Reader protocol: Wiegand	Reader protocol: Magnetic stripe
Card format: Secured	When a secured card (4-byte code used) is badged on a reader using the Wiegand protocol, 26 or 27 bit data is transmitted, depending on whether the card is programmed as Standard 26 bit or Tecom 27 bit ASC.	When a secured card (4-byte code used) is badged on a reader using the magnetic stripe protocol, magnetic stripe format data is transmitted. A “card present” signal is available on the relay output (violet wire), if selected in menu option 8—O/C Output.
Card format: Unsecured	When an unsecured card (4-byte code not used) is badged on a reader using the Wiegand protocol, the full 32 bit card ID number is transmitted.	When an unsecured card (4-byte code not used) is badged on a reader using the magnetic stripe protocol, the full 32 bit card ID number is transmitted.