

System1

User's manual

6656-0118 Issue 4.1

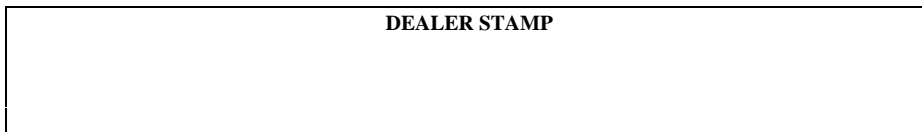
Supplier information:

The Microlock System 1 is designed and manufactured by:

TDSi Ltd.,
Crestworth House,
Sterte Avenue West,
Poole,
Dorset BH15 2AL
England

Telephone: Within U.K. 01202 666222
International +44 1202 666222
Fax: Within U.K. 01202 679730
International +44 1202 679730
E-mail address: info@tdsi.co.uk

Other supplier information:



Copyright:

Copyright © 1994 Time and Data Systems International Ltd., Poole. All rights reserved. This document, and any software supplied with it, may not be reproduced in any form or by any means in whole or in part without prior written consent of the copyright owners.

Policy:

TDSi has a policy to continuously improve its products. Therefore the company reserve the right to change specifications, colours or prices of its products at any time without prior notice.

Disclaimer:

Limited Warranty: Subject to the provisions of the Limitation of Liability given below, Seller warrants to Buyer, and only to Buyer, that under normal use and service the System sold and the Software licensed hereunder shall be free of defects in material or workmanship, ordinary wear and tear excepted, and where applicable shall meet the specifications contained or expressly referred to in the Special Conditions (if any) for a period of one (1) year after the date of manufacture, provided that (a) the System and the Software are installed, maintained and operated in strict compliance with the Seller's specifications and recommendations, (b) the System is altered or modified by Buyer only with the express written approval of Seller in accordance with Seller's instructions, (c) the Software is not modified or altered in any manner by Buyer, and (d) the System is not subject to any misuse, abuse, neglect, accident, improper alteration or modification or negligence in use, storage, transportation or handling. Should the System or the Software prove defective during the warranty period, Buyer shall notify Seller in writing of such defect promptly, but in no event later than ten (10) days after the expiration of the warranty period. Seller's sole obligation, and Buyer's exclusive remedy under this warranty shall be limited to the repair or replacement, at Seller's option, of any part of the System or Software which proves defective in materials or workmanship during the warranty period. **Except as expressly provided in this paragraph, seller makes no representations or warranties of any kind, nature or description, express or implied, including, without limitation, any warranty of merchantability or fitness of any and all of the system or software for any particular purpose, and hereby disclaims the same. Seller shall not be responsible for any defects in the system or the software arising out of any design made, furnished or supplied by the buyer.**

Limitation of liability:

In no event shall seller be liable to buyer, whether in contract or in tort or under any other legal theory, for lost profits or revenues, loss of use, or similar economic loss, or for any indirect, special, incidental, consequential or similar damages, arising out of or in connection with the sale, delivery, non-delivery, servicing, use, maintenance, condition or possession of any and all of the system or software, or for any claim made against buyer by any other party, even if seller has been advised of the possibility of such claim. In no event shall seller's liability under any claim made by buyer exceed the amounts paid for the system and the use of the software in respect of which such claim is made.

Table of Contents

HOW TO USE THIS MANUAL	5
INTRODUCTION	6
Concept.....	6
S1 model.....	6
S1x model.....	7
Programming.....	7
Possible configurations.....	7
Description of options.....	7
Programming System1	10
REFERENCE SECTION	15
How to use this section	15
Defaults.....	15
Alarms	15
Anti pass-back - M#5nn	16
Card+PIN access - M#60x, M#63xxyy	17
Clock and calendar - M#3xx, M#1lx.....	19
Communications.....	21
Communications diagnostics - M*9/M**	23
Door ajar alarm - M#7nn, M#8nn	24
Door sensor type - M#10x.....	25
Egress.....	26
Inputs.....	27
Keypad.....	28
Lock time - M#0xx.....	29
Master card - M9#4, M9#5	30
Memory partition - M5#nnn.....	31
Messages - M0#nn and M1#nn	32
Password - M9#8abcdabcd, M#62n	36
PIN-only access - M*5, M*6, M#62n	38
Printer	41
Printouts	42
Quit	45
Reader type - M#61x	46
Relays.....	47
Resets - M#9xx.....	50
Validating cards	51
Voiding cards.....	53
Unit number - M#4nn.....	54
APPENDIX 1: TROUBLE-SHOOTING	55
Card won't release lock.....	55
Relay doesn't come on when expected.....	55

APPENDIX 2: PRINTER MESSAGES.....56
 Card/keypad messages.....56
 Other messages56
 Interpretation of printer messages57

APPENDIX 3: ACCESS CRITERIA.....58

APPENDIX 4: GLOSSARY.....59
 ACU.....59
 Card-only access59
 PIN-Only59

APPENDIX 5: CARD NUMBERS.....60
 Infra Red Cards60
 Mag-Stripe Cards61
 Wiegand, Proximity and Hands Free Cards61

APPENDIX 6: DEFAULT STATES62

EFFECTIVITY NOTICE.....63

INDEX65

How to use this Manual

This manual deals with programming System1 using the built-in programming keypad. If you have a PC running Ultragard software, then you should be using the manual supplied with Ultragard instead of this manual.

This manual starts where the Installer manual left off. In other words, it assumes that System1 is correctly installed and that power is ON.

FIRST

Read the Introduction which starts overleaf. We strongly recommend that you read every word in the introduction section. The introduction section contains the following:

- a brief description of every option that can be programmed in System1
- a description of the programming method
- a list of all the programming sequences

THEN

Use the Reference section

Once you know what you want to do, look it up in the main part of this manual under its subject heading. This part of the manual is arranged alphabetically with cross-references where appropriate. But if you can't find what you're looking for, try the index which is at the back of the manual

If you find that something isn't working as you would expect, use the Troubleshooting section (Appendix 1).

Introduction

Concept

System1 is a one-door access control unit which:

- uses TDSi's unique reader technology
- will accept most other reader technologies
- is easy to install
- is highly protected from static
- is available in two models
- is easily upgradeable
- is compatible with System2, TDSi's 2-door controller
- can be controlled and monitored either stand-alone or computer- linked
- is suitable for own-labelling and re-packaging

Two models are available: S1 and S1x; an upgrade kit is available to convert an S1 to an S1x.

S1 model

This is the basic model, which can control access for up to 3000 people. It has the following inputs and outputs:

Inputs

- Card reader (various technologies)
- Door sensor
- Egress button
- 2 spare inputs

Outputs

- RS232 Serial data output
- Relay for lock strike
- Spare relay for alarm

S1x model

This is the same as S1 with the following additions:

- Real-time clock
- User-keypad option (for Card+PIN and PIN-only access)
- RS485 communications for computer linking

Programming

Programming is by means of a keypad. Security is provided by a “password” - a 4-8 digit PIN. Commands are entered as a sequence of letters and numbers.

Alternatively, System1 may be programmed from a computer running Ultragard software. Extra facilities become available when this is the case: these are time zones and timed relay operation.

Possible configurations

- Stand-alone (use S1x if keypad is needed, S1 otherwise)
- Single unit linked to serial printer (or parallel printer if serial/parallel converter used) (use S1 if no keypad or times are needed, S1x otherwise).
- One or more units linked to a PC running Ultragard2 software (use S1x)

Description of options

Anti pass-back

Anti Pass-Back works on a TIMED basis - cards may not be used twice within the programmed time period. The programmable range is 0-99 minutes. Default is 0; i.e. no anti pass-back.

Block-validate cards

Validates a range of cards from a start number to an end number.

Block-void cards

voids a range of cards from a start number to an end number.

Card+PIN

If this is ON then if a person uses a valid card at the reader he must also key-in a 4-digit PIN. The first time a card is used after this feature is turned on, then no PIN exists in memory against his card number, and so the person can type in ANY PIN. He is allowed access and that PIN is put in memory: it becomes his PIN from that point onwards. There is an automatic DURESS AL*RM function associated with Card+PIN entry. Default is OFF; i.e. no PIN is required. You can program the times of day when this feature is to be ON.

Clock and calendar

This allows you to set the correct date and time, to pre-program the change-over for daylight savings, and to program the desired date format to use for printed reports.

Communications

This allows you to choose which communications mode System1 is to operate in. There are two modes: one is used when System1 is connected directly to a printer ("printer mode"); the other is used for when one or more control units are connected to a PC running Ultragard software ("computer mode"). The printer mode defaults to 9600 baud, eight-bit word, no parity, but you can change this to suit your printer.

Communications diagnostics

If System1 is connected to a printer, it can be useful when setting up the installation to have a continuous stream of data coming from System1 to allow you to check the connections and programmed settings. The communications diagnostics feature does just this.

Door ajar local time

If the door stays open for more than this time then the "Door ajar (local)" alarm is triggered: this may cause a message to the printer and/or relay 2 to turn on. Default is 15 seconds.

Door ajar remote time

If the door stays open for more than this time then the "Door ajar (remote)" alarm is triggered: this may cause a message to the printer and/or relay 2 to turn on. Default is 45 minutes.

Door sensor type

This allows connection of either normally-open or normally-closed contacts. Default is normally-closed (i.e. door open = contacts closed).

Lock time

This is the maximum length of time the lock release relay will be energised for. The relay is de-energised if the door opens before this time has expired. Default is 4 seconds.

Master Card

This allows you to validate cards at a reader (much faster than by keypad!). First, you validate a "master card" at the keypad. Then, at your convenience, you can take the master card to the reader together with all the cards you wish to validate.

Memory partition

Allows you to select how the memory is shared between cards and "event record". The event record is un-transmitted data about events which have occurred. In printer mode, data is normally transmitted immediately. But if the printer is unavailable (switched off, or out of paper) then the events will be saved until the printer becomes available again.

Messages

This function allows you to turn off individual messages that are sent to the printer. Default is all messages ON.

Password

Allows you to change the password required to start programming. Default is 1234.

PIN-only

For PIN-only access, there are two requirements: PIN-only must be ON and the PIN you want to use must be valid (see "Validate PIN-only"). This might seem unnecessary, having to use two commands to use the function. But it does allow you to turn the function on and off (for example ON during the day and OFF at night). There is a "duress alarm" function associated with PIN-only entry. Default for the PIN-only function is OFF. You can choose how many digits are required for a PIN, from 4 to 8 digits. You can program the times of day when this feature is to be ON.

Reader type

Allows selection of reader type from the following: TDSi-technology, Proximity, Hands-Free Wiegand, Mag-stripe or bar-code (note: Bar-code option only available to special-order at time of writing). Default is TDSi- technology.

Relays

There are two relays on System1. One is used as the lock strike relay; the other can be programmed to come ON if a particular alarm condition occurs, or if an input is triggered. The default for this relay is to act as an "alarm shunt". You can also turn ON or OFF either relay, regardless of its programmed function.

Reports

In normal use, the controller will send event reports directly to the printer as and when they occur. The "reports" option is a separate function to allow you to interrogate the controller. There are two reports - parameters (i.e. the programmable functions and their current settings) and valid cards.

Resets

Several "reset" functions are provided in case you want to clear out certain parts of the programming.

Unit Number

This allows you to set the number (i.e. "address") of the System1 controller. This is only necessary when more than one unit is connected to a PC.

Validate card

This allows you to validate new cards. You will be told if the card was already in memory.

Validate PIN-only

Same as "Validate card".

Void card

This allows you to erase a card from memory. You will be told if the card was not in memory.

Void PIN-only

Same as VOID card.

Programming System1

Introduction

System1, despite its small size and limited number of keys, is very easy to program.

The LED next to the built-in programming keypad tells you all you need to know about what state System1 is in:

LED flashing

Brief flash every two seconds

System1 is in normal operating mode. No-one may do any programming unless they know the password.

Brief flash every 0.5 seconds

System1 is waiting for you to complete the entry of a PIN - this may be a PIN-only for access (if PIN-only mode is "ON") or the master password.

Four brief flashes

System1 is telling you that it cannot do what you asked - for example you may have tried to void a card which was not in memory, or to validate one already in memory.

One second on one second off

System1 is performing a "block validate" or "block void" instruction.

Eight brief flashes

This occurs if you try to validate a card when the memory is full.

LED permanently on

The lock strike relay is on.

LED permanently off

System1 is in programming mode; i.e. the master password has been entered. As you press keys, the LED comes on. When you press the last key in a sequence, the LED comes on for one second to indicate successful completion. If you make a mistake, press the "#" key once, twice or three times until you exit from programming mode - the LED resumes its normal flashing (once every two seconds). If you do not press any keys for one minute, System1 exits programming mode.

Programming sequences

All programming sequences are similar in structure, comprising three elements:

- a master-password (a four- to eight-digit PIN)
- the “feature selection code”
- any “variable data”

For example, to set the lock release time, the command as shown later in this manual is:

M#0nn

where M = the master password

#0 = the “lock strike time” selection code

nn = the lock strike time in seconds

So, if the master password in your System1 is “1234”, and you want to set the lock strike time to 15 seconds, you enter at the keypad:

1234#015

Sometimes, there is no concept of variable data in a command; for example, to “latch on” the lock strike. This kind of command is in two parts: for example, to latch on the lock strike, the command as shown later in this manual is:

M*1

where M = the master password

*1 = the “lock strike relay ON” command

So, if the master password in your System1 is “1234”, and you want to latch the lock strike ON, you enter at the keypad:

1234*1

Programming using the user keypad

If a user keypad (i.e. one installed with the card reader) is installed, you can use this for programming as well as the built-in keypad. If you regard this as a security risk, refer to “Keypad” in the Reference section for a way of preventing programming at the user keypad.

If you are using the user-keypad for programming, the A key = the * key, and the B key = the # key.

Programming List

Anti pass-back	M#5nn (nn = time in minutes) 00 = no anti pass-back
Block validate cards	M9#6aaaaaaabbbbbbb aaaaaaa = first card bbbbbbb = last card
Block void cards	M9#7aaaaaaabbbbbbb aaaaaaa = first card bbbbbbb = last card
Clock set	M3#hhmm (use 24-hour format)
Clocks forward	M6#ddmm
Clocks back	M7#ddmm
Clock calibrate	M2#0y = slow down by y*5 seconds/month M2#1y = speed up by y*5 seconds/month
Calendar	M4#ddmmyy
Card+PIN access	M#600 = OFF M#601 = ON M#63xyy = times of operation
Communications mode	M#300 = printer mode M#301 = computer mode
Communications data rate	M#255 = 300 baud M#277 = 1200 baud M#2** = 9600 baud
Communications word length	M#317 = 7-bit word (plus 1 parity bit) M#318 = 8-bit word
Communications parity	M#320 = even parity M#321 = odd parity M#322 = space parity M#323 = mark parity M#324 = no parity
Communications stop bits	M#331 = 1 stop-bit M#332 = 2 stop-bits
Communications duplex	M#340 = half-duplex M#341 = full duplex
Communications handshake	M#350 = none M#351 = XON/XOF M#352 = CTS M#353 = CTS and XON/XOF
Communications diagnostics	M*9 = start transmitting M** = stop transmitting
Date format	M#110 = day-month-year M#111 = month-day-year M#112 = year-month-day
Door ajar local alarm	M#7nn (nn = time in seconds)
Door ajar remote alarm	M#8nn (nn = time in minutes)

Door sensor type	M#100 = normally closed M#101 = normally open
Lock release time	M#Onn (nn = time in seconds)
Master card	M9#4aaaaaaaa = validate M9#5aaaaaaaa = void
Memory partition	M5#nnn (nnn*10 = number of cards)
Messages	M0#nn = disable message nn M1#nn = enable message nn 00 Access granted 01 Access denied: card not valid 02 Access denied: card expired 03 Access denied: anti pass-back 04 Access denied: no PIN 05 Access denied: wrong PIN 06 Access denied: Too many wrong PINs 07 Access denied: lock relay latched off 08 Timed Card+PIN on 09 Timed Card+PIN off 10 Input 3 on 11 Input 3 off 12 Input 4 on 13 Input 4 off 14 Read error 15 Duress 16 Door open 17 Door forced 18 Door ajar (local) 19 Door ajar (remote) 20 Egress on 21 Egress off 22 Reader gone 23 Reader returned 24 Clocks forward } 25 Clocks back 26 Restart 27 Timed PIN-only ON 28 Timed PIN-only OFF
Password	M9#8abcdabcd abcd = new password M#62x = no of digits
PIN-only	M*5 = enable PIN-only M*6 = disable PIN-only M#62x = no of digits M#64xyy = times of operation
Reports	M*3 = print card list M*4 = print parameters

Reader type	M#611 = TDSi-technology M#612 = Wiegand M#613 = Proximity M#614 = Mag-stripe swipe M#615 = Mag-stripe insert M#616 = Bar-code
Relay 2 programming	M8#2yy yy = function: 00 = Lock strike 01 = Alarm shunt 02 = Door ajar (local alarm) 03 = Door ajar (remote alarm) 04 = Door forced 05 = Duress 06 = access denied 07 = 4th wrong PIN 08 = Reader gone 09 = Input 1 ON 10 = Input 2 ON 11 = Input 3 ON 12 = Input 4 ON
Relay Control	M#*xy (x = relay number) y = 0 = OFF y = 1 = ON y = 2 = Normal
Resets	M#912 = Reset parameters M#987 = Reset cards M#934 = Reset trail M#969 = Reset everything
Unit number	M#4nnn (nnn = unit number)
Validate card	M9#0aaaaaaaa
Validate PIN-only	M9#2aaaa
Void card	M9#1 aaaaaaaaa
Void PIN-only	M9#3aaaa

Reference section

How to use this section

This section of the manual is in alphabetical order.

Cross-references are provided in a lot of cases, but the index is more comprehensive if you are having difficulty finding what you want.

Note that some features of System1 are only accessible when using a PC with Ultragard software. These features are not included in this manual. If you are using Ultragard, you should be using the Ultragard manual INSTEAD of this manual

Defaults

Defaults are the settings that apply after a RESET, which is usually the case in units as they are shipped from the factory. However, to be sure, part of the installation procedure involves performing a full reset. This is covered both in the installation manual and in this manual.

Alarms

In System1, an alarm occurs when something unusual happens; for example, someone uses a card which is not valid. There is no programming function for alarms - what you program is what happens when a specific alarm occurs. There are two things that can happen as a result of an alarm:

- an alarm may result in a message to the printer (see MESSAGES).
- an alarm may also cause relay 2 to come on (see RELAYS).

Anti pass-back - M#5nn

Command:	M#5nn
Default:	M#500 = No anti pass-back
Range:	M#501- M#599 (1-99 minutes)

Application

Anti pass-back is used to stop someone from passing their card back to someone else, so that two people cannot get in using one card.

In System1, this is done on a timed basis. If you have turned this feature on, then once a card has been used it cannot be used again for a certain time. This time is something which you can program in the range 1-99 minutes.

If access is denied because of anti pass-back, this will result in an ALARM message to the printer (unless the message has been turned off). It may also result in relay 2 being energised, if you have programmed for this.

Note that when you turn anti pass-back ON then some cards will be denied access straight away - for each card, the system behaves as if anti pass-back was in force when the card was last used. For example, if you set the anti pass-back time to 30 minutes, any cards used in the last 30 minutes will be denied access.

Accuracy

The accuracy is approximately one-fifteenth of the programmed time. For example, if you have programmed 30 minutes then the actual timing will be in the range 29-31 minutes.

To turn anti pass-back ON

(If you turn anti pass-back on, then it applies to all cards in memory in the controller. When you program the time limit, it also applies to all cards).

Decide on how many minutes you want cards to be denied access for, then enter the command M#5nn where nn is the number of minutes.

To turn anti pass-back off

Enter the command M#500

Related topics

Messages, Alarms, Relays

Card+PIN access - M#60x, M#63xxyy

Command:	M#601 = Card+PIN access ON
Default:	M#600 = Card+PIN access TIMED
Command:	M#63xxyy = ON at xx hours, OFF at yy hours
Default:	M#630000 = OFF at all times

Application

The Card+PIN function provides a higher level of security than card alone. This is because if a card is lost or stolen, you may not get chance to void it before someone tries to use it. Every card can have a different PIN: each card-holder chooses his own PIN the first time the card is used after this feature is turned on.

Restrictions

Obviously, you should only program Card+PIN access at a door if a user keypad is fitted. Note that PIN-only access can be ON or OFF as required, as it does not conflict with Card+PIN access.

24-hour Card+PIN access

Enter the command M#601. Every card-holder must now use a four-digit PIN. This over-rides the timed command.

Timed Card+PIN access

If you wish, you can turn the Card+PIN access requirement on and off according to the time of day. Typically, you might want to turn the feature off during the day, and on overnight when more security is required because fewer people are around.

Enter the command M#63xxyy where xx is the on time and yy is the off time. For example, to turn the feature on at 7pm (1900 hours) and off at 8am (0800 hours) you would enter the command M#631908. Note that for timed Card+PIN to work, the M#6xx parameter must be set to M#600.

No Card+PIN access

To be sure that Card+PIN access is never on, enter both the following commands; M#600, M#63000.

When Card+PIN is ON

If Card+PIN is ON, when you use a valid card at the reader the LED starts flashing at a faster rate. This signals the fact that you must now key-in the correct PIN. 10 seconds are allowed for entering the PIN.

If no PIN exists in memory against the card number (i.e. this is the first time the card has been used since the feature was turned on), you can type in any four digits. You are allowed access and that PIN is put in memory: it becomes your PIN from that point onwards.

Of course, all other access criteria have to be satisfied as well. There is a set order in which the System1 controller checks a PIN-only to decide whether to allow access. This order is described in Appendix 4 Access criteria.

Wrong PIN

If the digits you enter don't match the number in memory then you are given another three attempts to get it right. If you don't get it right at the fourth attempt, then this is treated as an ALARM. There is a message to the printer (unless you have turned the message off). You can also program relay 2 to energise for such an alarm. **The card cannot be used again until it has been re-validated.**

If you realise you have made a mistake part-way through the PIN entry, then press the A or B key and start again (this is not counted as a wrong PIN). If you re-start more than four times, then it is counted as an incomplete PIN and YOU will have to re-enter the card.

Incomplete PIN

If you don't complete a PIN entry in time then you can try again; this is not counted as a wrong PIN as far as the "fourth wrong PIN" alarm is concerned.

Forgotten PIN

If a card-holder has forgotten their PIN, re-validate the card. The PIN is re-set to the un-known state, and the card-holder can choose a new PIN the next time the card is used.

Duress Pin

If the PIN you enter is one higher in value than the PIN for that card (for example, you enter 1235, when 1234 is in memory) then this causes a DURESS alarm. The lock release relay will still be energised.

Related topics

Validate card, Relays, Messages

Clock and calendar - M#3xx, M#lxx

Clock set:	M3#hhmm
Clocks forward:	M6#ddmm
Clocks back:	M7#ddmm
Clock calibrate:	M2#xy - see below for meaning of x and y
Calendar set:	M4#ddmmyy
Date format:	M#110 = ddmmyy
	M#111 = mmddy
	M#112 = yymmdd

Application

These commands are only relevant if the clock option is fitted.

It is important to have the correct time and date set in the controller for two reasons:

- the time and date is recorded as part of every event record (only relevant if System1 is connected to a printer or a PC)
- the time is used for automatically turning the Card+PIN and PIN-only features on and off (if required).

To set the clock

Enter the command M3#hhmm where hhmm is the time in 24-hour format (e.g. 6 p.m. = 1800). As you enter the last digit, the time is set to the exact minute.

To set the calendar

Enter the command M4#ddmmyy where ddmmyy is the date (e.g. 1st April 1990 = M4#010490). Any date between 1st January '90 and 31st December '99 is assumed to be 1990-1999; any other date is assumed to be the year 2000 onwards. You must always enter the date in this format, even if you have selected a different date format for printing.

To set the date format for printing

Day/Month/Year:	enter the command M#110
Month/Day/Year:	enter the command M#111
Year/Month/Day:	enter the command M#112

Clocks forward

Enter the command M6#ddmm where ddmm is the date of the change (e.g. 25th March = M6#2503). The clock will go forward one hour on the specified date at 1.00 am (0100), i.e. it will change from 0100 to 0200. If Card+PIN or PIN-only is programmed to change between these two times then the change will occur simultaneously with the clock change.

Clocks back

Enter the command M7#ddmm where ddmm is the date of the change (e.g. 23rd September = M7#2309). The clock will go back one hour at 0200 (to 0100) on the specified date. If Card+PIN or Pin-only is programmed to change between these two times then the change will be actioned twice.

Clock calibrate

The accuracy of the clock in System1 is quoted at +/- two minutes per month. In practice this means that (assuming constant temperature) the clock will run either consistently fast or consistently slow, by no more than two minutes per month. The clock calibration allows you to speed up or slow down the clock and therefore achieve a much better accuracy than the quoted one.

To speed up

Enter the command M2#0n, where $n \times 5$ is the number of seconds per month the clock will speed up by (e.g. M2#06 will speed up the clock by 30 seconds per month). If you need to speed up the clock by more than $9 \times 5 = 45$ seconds per month, execute the command more than once; e.g. M2#09 followed by M2#03 will speed up the clock by $9 \times 5 + 3 \times 5 = 60$ seconds per month. This is exactly the same as entering M2#06 twice. There is a limit - if you try to exceed it you will get four flashes from the LED.

To slow down

Enter the command M2#1n, where $n \times 5$ is the number of seconds per month the clock will speed up by (e.g. M2#16 will slow down the clock by one minute per month). If you need to slow down the clock by more than $9 \times 5 = 45$ seconds per month, execute the command more than once; e.g. M2#19 followed by M2#13 will slow down the clock by $9 \times 5 + 3 \times 5 = 60$ seconds per month. This is exactly the same as entering M2#16 twice. There is a limit - if you try to exceed it you will get four flashes from the LED.

Communications

Application

This part of the manual can be ignored if the controller is NOT connected to a printer or a PC. If the controller is connected to a PC running Ultragard software then you should be using the Ultragard manual INSTEAD of this manual.

Types of communication

There are only two modes of communications with a System1 controller:

Printer mode

The controller will transmit details of events as and when they occur; this is called "immediate transmit". This is usually to a dumb printer or VDU; you must program the controller to match the communications parameters of the printer/VDU (baud rate, parity, handshake etc.) If the controller is to be connected to a parallel printer then a serial/parallel converter will have to be used; the controller must then be programmed to match the parameters of the converter.

Transmission will not occur if the handshake conditions prevent this. The number of events that System1 memory can hold (before starting to over-write the oldest events) is determined by the memory partition - see "Memory partition" elsewhere in this manual.

Computer mode

This is the default mode.

The controller will only transmit when requested to by a PC; this is called "polling". This form of communication is pre-set at 9600 baud (but will work at other rates providing the PC is set to the same rate). The communications parameters change to suit the special TDSi protocol - you cannot change these parameters.

If the computer does not poll System1, then the events remain in memory until the memory is full - this is called the "trail record". The number of events that System1 memory can hold (before starting to over-write the oldest events) is determined by the memory partition - see "Memory partition" elsewhere in this manual.

Defaults

System1 defaults to computer mode, with the default parameters set as below. Whenever you select a particular communications mode (even if you are already in that mode) then the parameters are returned to their default settings.

Printer mode - default parameters

9600 baud
7-bit word
even parity bit
one start bit
one stop bit
full duplex
XON/XOF handshake

Computer mode - default parameters

Special TDSi protocol, designed for use with Ultragard software. Only the baud rate can be changed.

Setting up System1 to work with a printer

Enter the command M#300, followed by any commands need to change the default parameters to those required by the printer. Note that there must always be 10 bits in a character (including the start bit) - so some of the commands you can enter will over-ride other commands:

- selecting 8-bit word forces no parity, 1 stop bit
- selecting any parity option forces 7-bit word, 1 stop bit
- selecting 2 stop bits forces 7-bit word, no parity

Communications data rate (baud rate): M#2xx

M#255 for 300 baud
M#277 for 1200 baud
M#2AA for 9600 baud

Communications word length: M#31x

M#317 = 7-bit word (plus 1 parity bit)
M#318 = 8-bit word (forces no parity, one stop bit)

Communications parity: M#32x

M#320 = even parity (forces 7-bit word, 1 stop bit)
M#321 = odd parity (ditto)
M#322 = space parity (ditto)
M#323 = mark parity (ditto)
M#324 = no parity

Communications stop bits: M#33x

M#331 = 1 stop-bit
M#332 = 2 stop-bits (forces 7-bit word, no parity)

Communications duplex: M#34x

M#340 = half-duplex
M#341 = full duplex

Communications handshake: M#35x

M#350 = none
M#351 = XON/XOF
M#352 = CTS
M#353 = CTS and XON/XOF

Communications diagnostics - M*9/M**

This feature causes the message "TDSi" to be sent repeatedly to the printer. This is very useful for checking that installation and set-up of the communications link are correct. This feature only works if "printer mode" has already been selected.

To start transmitting: M*9

To stop transmitting: M**

Door ajar alarm - M#7nn, M#8nn

Application

This is an ALARM function. Alarm functions result in a message to the printer (unless the message has been turned OFF). Alarms may also cause relay 2 to come on if you have programmed it to do so (see Relay Programming).

There are two door ajar alarms: LOCAL and REMOTE. You can program the time that the door can be open before each alarm will occur. You can program each door differently.

Why are there two different door ajar alarms?

The only difference between the two is that the LOCAL time is usually less than the REMOTE. It is normal to have the LOCAL alarm connected to a bell close to the appropriate door. The REMOTE alarm would be connected to a bell in the main office or similar, where there would always be someone available to respond. The REMOTE alarm would ring if the LOCAL one had been ignored for the given time.

Defaults

LOCAL: 15 seconds
REMOTE: 45 minutes

How to set the door ajar alarm times

Note: the LOCAL time is set in seconds (1-99) and the REMOTE time is set in minutes (also 1-99).

LOCAL: Enter the command M#7nn
REMOTE: Enter the command M#8nn

Related topics

Messages, Relays, Alarms, Door sensor

Door sensor type - M#10x

Command: M#101 = normally closed
M#100 = normally open
Default: M#101 = normally closed

Application

This function allows you to choose which type of door sensor is fitted: “normally open” (door open = contacts open) or “normally closed” (door open = contacts closed). The correct selection should have been made by the installer during installation. Change it only if you are sure you need to.

What the door sensor does

For access **control**, the door sensor provides an extra level of security, in the following way. If the lock release time is set to, say, 10 seconds, it is quite possible for someone to get through the door in only two or three seconds after using their card. This leaves seven or eight seconds of “un-expired” time, during which (if no door sensor was fitted) the door could still be opened. However, if a door sensor is fitted, then as soon as the door opens the lock release is de-energised.

For access **monitoring**, having a door sensor fitted means that all occurrences of the door opening and closing can be monitored on the printer. Also, relays can be set to operate if a door opens when it shouldn't (door forced), or stays open for too long (door ajar). These occurrences will also be reported to the printer.

Restrictions

You must have the correct type selected; the lock strike relay will not be energised if the controller thinks the door is open. If no sensor is fitted then you must leave this set at the default i.e. normally closed otherwise Svstem1 will think the door is permanently open.

Default

Normally closed (i.e. door open = contacts closed)

How to select “normally open” door contacts

Enter the command M#100

How to select “normally closed” door contacts

Enter the command M#101

Related topics

Door ajar alarm

Egress

System1 is provided with an input which can be used for a “Free Egress” function. If this input is momentarily closed-circuit then the lock will be released just as if a card had been used i.e. for the length of the lock release time.

There are three possible uses for this:

- The “door forced” alarm will be triggered if the door opens without the lock having been released. Installing an egress button means that the door forced alarm doesn't occur without good reason.
- Installing a push-button in the reception area means that the receptionist can allow access to visitors without cards.
- By installing a time switch to operate the egress input the lock will remain released for a period of time. This can be useful if there are periods when no access control is required.

There is a message each time the input goes closed-circuit, and a message each time the input goes open-circuit. These messages can be suppressed: see MESSAGES.

Related topics

Lock time, Messages, Input diagnostics

Inputs

System1 has four inputs numbered 1 to 4:

- Input 1 is the door sensor
- Input 2 is the egress input
- Input 3 is spare
- Input 4 is spare

Inputs 3 and 4 can be used to monitor things, an emergency exit for example. If one of these input changes state (from open circuit to closed circuit or vice versa) then two things may happen:

- A message is sent to the printer (unless the message has been turned off)
- Relay 2 is operated (if programmed to do so)

Related topics

Messages Relays, Alarms

Keypad

If you have a keypad installed alongside a card reader (i.e., a user keypad rather than the programming keypad on the controller) you can make use of two additional features: Card+PIN access and PIN-only access.

Note that the user-keypad may also be used for programming. If you regard this as a security risk, then take the following steps:

- Disconnect the A/0/B row (the keypad black wire, pin 26)
- Choose a new master PIN containing at least one “0”
- Make sure that all other PIN numbers have no “0” in them and do not end in “9” if you want to use the duress feature

Card+PIN access

This means that as well as entering a valid card, you must type in a number to be granted access. This number is the one that was chosen by the card-holder the first time the card is used.

This provides a higher level of security than card-only access. Lost, stolen and "borrowed" cards should be voided as soon as possible - but this is sometimes not soon enough.

There is a Duress Alarm feature. The alarm occurs if a card holder enters a PIN one higher than his own (e.g. 1235 instead of 1234).

See “Card+PIN” and “Validate card” for more information.

PIN-only access

This means that no card is required, only a personal identification number You can program up to 10 PINs in memory. See VALIDATE PIN-only for more information.

There is a Duress Alarm feature. The alarm occurs if a PIN is entered that is one higher than one of the PIN-only numbers in memory (e.g. 1235 instead of 1234).

Related topics

Card+PIN, PIN-only

Lock time - M#0xx

Command: M#0xx (xx = time in seconds)
Default: M#004 (Four seconds)
Range: M#001- M#099 (1-99 seconds)

Application

You can set the maximum time that the lock strike relay will be energised for after a valid access event (Card entry, Card+PIN entry, PIN-only entry, Egress button pressed). If a door sensor is fitted, the lock strike relay is de-energised if the door opens before this time has expired.

Restrictions

The lock time can be set in the range 01-99 seconds. You cannot set a lock time of 0 seconds - if you want to bar all access through a door then use the "Relay control" feature to latch the lock strike relay off.

Default

4 seconds.

How to change the lock time

Enter the command M#0xx where xx is the lock time in seconds.

Related topics

Relays, Door sensor, Egress

Master card - M9#4, M9#5

Command: M9#4aaaaaaaa = validate master card number aaaaaaaa
Command: M9#5 = void master card
Default: No master card
Range: Maximum 1 master card

Application

This feature provides a faster way of validating cards than by using the keypad.

If you have the cards in your possession, then you can validate them by using them at the reader. For security reasons, you do not want to set the controller in “validate card” mode before walking to the reader - while you were in transit anyone might come up to the reader and validate their own card!

Instead, you create a master card using the M9#4 command. Then, when you get to the reader, enter the master card and the controller is automatically set into “validate cards” mode (the LED stops flashing to signal this). Enter all cards you wish to be validated (the LED lights to signal acceptance - wait for it to go out before entering the next card). When you have finished, enter the master card again - the LED resumes its regular flashing (if you forget to use the master card, the controller will automatically drop back into normal mode after one minute).

Memory partition - M5#nnn

System1's memory is used for holding the numbers of valid cards, and for holding the un-transmitted events (trail record).

The maximum number of cards and events combined that can be held in System1 is 3008. Note that PIN-only numbers are included in this figure.

The default memory partition allows 2000 cards and 1008 events. You can make more memory available for either cards or trail record by using the "memory partition" command. (See "Communications" for an explanation as to why you might want more trail record).

To change the memory partition

The memory partition command works in multiples of 10. Decide how many cards you want as a maximum, and divide this number by 10. Then enter the command M5#nnn where nnn is your answer. For example, to have 230 cards maximum, enter the command M5#023.

Commands which attempt to allow more cards than will fit will be rejected. Remember that cards + events = 3008, therefore the maximum number of cards is 3000 (M5#300).

Messages - M0#nn and M1#nn

Application

Messages are reports of events (including alarms) sent to the printer or PC.

You may not be interested in seeing every event that occurs. The “Messages” function allows you to turn off individual messages, so that you only see what is important to you.

How to turn messages on and off

To turn off a message: enter the command M0#nn where nn is the message number

To turn on a message: enter the command M1#nn where nn is the message number

The table overleaf shows the messages which can be turned on and off (see “Glossary” after the table for explanations):

No.	Message
00	Access granted
01	Access denied: card not valid
02	Access denied: card expired
03	Access denied: anti pass-back enforced
04	Access denied: no PIN entered
05	Access denied: wrong PIN entered
06	Access denied: fourth or more wrong PIN entered
07	Access denied: lock relay latched off 08 Timed CARD+PIN on
09	Timed CARD+PIN off
10	Input 3 on
11	Input 3 off
12	Input 4 on
13	Input 4 off
14	Reader error
15	Duress
16	Door open
17	Door forced
18	Door ajar (local)
19	Door ajar (remote)
20	Egress on
21	Egress off
22	Reader gone
23	Reader returned
24	Clocks forward
25	Clocks back
26	Restart
27	Timed PIN-only on
28	Timed PIN-only off

Default

All messages ON

Glossary

Access granted

This refers to any valid access event where access was granted: Card only, Card+PIN or PIN-only. If you turn off this message then you will not see the number, nor the time if clock is fitted (S1x). You will not even see the FACT that a valid access event occurred. But you WILL see the door open/closed messages unless you turn them off.

Access denied

There is a set order in which System1 checks to see whether it can allow access. Only the first reason encountered will be identified. This order appears in Appendix 4.

Timed CARD+PIN

This refers to the function, which allows you to turn on and off the Card+PIN feature at a specific time of day. There is a message for ON as well as OFF

Input

Each input generates a message for ON (closed circuit) and one for OFF (open circuit).

Reader error

This message usually occurs because a card-holder has taken too long in entering his card at the reader. Jerkiness is another cause.

Duress

The duress event occurs when someone uses a PIN one digit greater than the correct PIN - whether as part of a Card+PIN entry, or a PIN-only entry.

Door open

This relates to when the door has opened and closed as part of a valid access event. This function disables both those messages.

Door forced

In some installations, people may exit by turning a handle to open the door. This creates a "door forced" message (if a door sensor is fitted). The proper way round this is to install a "free egress" button. Alternatively, you can disable the door forced message (this automatically includes the "closed-after-forced" message).

Door ajar (I) and (r)

Each of these messages will be generated if the door is open for longer than the pre-programmed time limit. Turn off either or both of these messages if you don't need to know that these events have occurred. This automatically turns off the "closed-after-ajar" messages.

Egress

If an egress button is installed, then when the button is pressed a message is created. Another message is created when the button is released. This might seem unnecessary, having two messages, but sometimes the egress button is replaced by a switch to allow free access for longer periods of time. It is then very useful to know when the switch is turned off as well as on.

Reader gone/returned

These events are most unlikely to occur in practice. The cause of the messages is disconnection and re-connection of an TDSi-technology reader. With other types of reader, these events cannot be detected.

Clocks forward and back

These messages are self-explanatory.

Controller restarted

If the power to the controller is disconnected, or fails, then this message is generated when the power is restored. This message is also generated after certain types of RESET, and after certain parameter changes (reader-type, communications mode....)

Timed PIN-only

This refers to the function, which allows you to turn on and off the PIN-only feature at a specific time of day. There is a message for ON as well as OFF.

Password - M9#8abcdabcd, M#62n

Command: M#62n sets password to have n digits (n = 4-8)
Command: M9#8abcdabcd sets password to abcd
Default: 1234

Application

The password (actually, a PIN;) is used to prevent unauthorised people from re-programming the controller. Anyone wanting to program the controller must first key-in the correct password (see PROGRAMMING in the first part of this manual).

The factory-default password is 1234. We advise you change this immediately after installation for your own security - this procedure is explained below. If you want, you can also choose to have more than 4 digits in the password.

How to choose the number of digits in the password

Warning: this command also changes the number of digits in a PIN-only number. Any PIN-only numbers already in memory become unusable. We recommend that you do an MB987 reset to erase all card and PIN-only numbers after changing the number of digits.

Enter the command M#62n, where n is the number of digits in the password (in the range 4-8). When you enter this command, a new password will apply. If you increase the number of digits, then the appropriate number of leading zeroes are added; for example:

Old Password = 1256
Enter command M#626 (for 6-digit password)
New password = 001256

If you decrease the number of digits, then the appropriate number of leading digits will be omitted; for example:

Old Password = 125690
Enter command M#624 (for 4-digit password)
New password = 5690

How to change the password

Enter the command M9#8abcdabcd where abcd is the new password. Note that you have to enter the new password twice; this is to protect you from making a mistake. For example if you want the new password to be 3456 you will enter M9#834563456.

When you change the password, the factory default is forgotten. But if you do a "Reset parameters" command or a "Reset everything" command then the password is also reset, to 1234.

If you enter the wrong password

Anyone wanting to program the controller must first key-in the correct password (see "Programming System1" in the Introduction section). If you enter the wrong password then what happens depends on whether PIN-only is ON:

If PIN-only is off

then nothing appears to happen - you are simply denied access to programming mode. You get four chances to get it right after which the keypad is disabled for 10 minutes (a message to this effect will appear at the printer).

If PIN-only is on

then you will get the message INCORRECT PIN at the printer (unless the PIN entered happens to be the same as one of the PIN-only numbers that are currently valid!). You get four chances to get it right after which the keypad is disabled (a message to this effect will appear at the printer). If PIN-only is ON then this means that anyone trying to gain access using a PIN-only number is “locked out” for 10 minutes.

What to do if you forget the password

There is no secret “master” password. This is your guarantee of security. But if you forget the password then the only way to start using the controller is to disconnect all power and disconnect the memory battery for at least 20 seconds (see the Installer manual). All data will be lost and all programmable functions will be returned to their default settings. The password will now be 1234. You will have to re-program everything in the controller, including card numbers.

Related Topics

Keypad

PIN-only access - M*5, M*6, M#62n

Commands: M*5 = PIN-only access on
 M*6 = PIN-only access timed
 M#62n = set number of digits to n
 M9#2nnnn = validate PIN-only number nnnn
 M#64xxyy = on at xx hours, off at yy hours
Defaults: PIN-only access off, four digit PINs and password.

Application

The PIN-only function allows access without the use of a card, simply by keying-in a number. You can choose how many digits there are in a PIN-only number; the minimum is four, the maximum is eight.

In most ways a PIN-only number is treated like a card. For example, anti pass-back will apply if appropriate. Of course, although you can give a card a PIN (i.e. Card+PIN access), you cannot give a PIN-only a PIN.

PIN-only access does not cancel or conflict with Card-only access or Card+PIN access.

For security reasons, the event message sent to the printer does not include the PIN number used.

Restrictions

No matter how many digits you have chosen to be in a PIN-only number, each one occupies the same space in memory as a card. In other words if you have five PINs validated, then that leaves room for five fewer cards.

Obviously, you can only use PIN-only access if a user keypad is fitted.

If you validate a PIN-only number which happens to be the same as the password, then the password takes priority - i.e. the door will not open; instead the controller is put into master mode whenever that number is used.

How to choose the number of digits in a PIN

Warning: this command changes the number of digits in the password, and therefore the password will revert to its default. Any PIN-only numbers already in memory become unusable. We recommend that you do an MB987 reset to erase all card and PIN-only numbers after changing the number of digits.

Enter the command M#62n, where n is the number of digits in every PIN- only number (in the range 4-8).

How to allow PIN-only access

You must do two things for PIN-only access to be allowed:

1. Turn ON the PIN-only feature

Enter the command M*5 for 24-hour PIN-only access.

Alternatively, you can turn the Card+PIN access requirement on and off according to the time of day. Typically, you might want to turn the feature on during the day, and off overnight when more security is required because fewer people are around. Enter the command M#64xxyy where xx is the on time and yy is the off time. For example, to turn the feature on at 8am (0800 hours) and off at 7pm (1900 hours) you would enter the command M#640819. Note that you should also enter the command M*6 to be sure that 24-hour PIN-only access is disabled.

2. Validate the desired PIN-only numbers

This is described in “Validate card” section, as it is so similar to validating cards.

This might seem unnecessary, having to use two commands to use the function. But it does allow you to turn the function on and off (for example ON during the day and OFF at night), while leaving all the PINs validated in memory.

How to gain access using a PIN-only number

If you press any number key, this is taken as the first digit of a PIN (or password) entry and the flashing rate of the indicator light on the reader next to the keypad changes. You have 10 seconds to complete the entry.

Of course, all other access criteria have to be satisfied as well. There is a set order in which the controller checks a PIN-only to decide whether to allow access. This order is described in Appendix 4: Access criteria.

For obvious security reasons, the PIN-only number never appears at the printer as part of an event message.

Wrong PIN

If the digits you enter don't exactly match any of the PIN-only numbers in memory (or if you don't complete the entry in time) then you are given another three goes to get it right. If you still don't get it right, then this is treated as an ALARM. There is a message to the printer unless you have turned the message off.

If you realise you have made a mistake part-way through a PIN-only entry, then press the A or B key and start again (this is not counted as a wrong PIN).

Duress PIN

If the PIN you enter is one higher in value than one of the numbers in memory (for example, you enter 1235, when 1234 is in memory) then this causes a “Duress” alarm. The lock release relay will still be energised.

How to disallow PIN-only access

Enter the command M*6.

This disallows access for all PIN-only numbers in memory, but does not erase the numbers. When you next turn on the function, then those same PINs will now be allowed. If you want to disallow access for only one PIN-only number, then use the VOID option.

Related topics

Alarms, Messages, Validate, Void, Keypad

Printer

To find out how to set up the controller to suit your printer, see “Communications”.

To find out what the messages on the printer mean, see Appendix 3.

To find out how to stop certain messages being printed, see “Messages”.

To find out how to add a printer to your system, see the Installer Manual.

To find out how to ask for a print-out of the information held in the controller, see “Printouts”.

Printouts

Application

If you have a printer connected, you can ask the controller to report on either the current list of valid cards, or the parameters programmed into System1 .

This is entirely separate from the normal event reporting which is going on all the time. But obviously, when you want to get a report of the programmed settings, event reporting is suspended during printing of the report.

Important

Whilst the print-out is being transferred to the printer's buffer, all other operations in System1 are suspended. If something happens to prevent the print-out (printer not on, out of paper, off-line etc.) then System1 will wait until the fault is rectified. If you wish to cancel the print out, use the command M#301 followed by M#300 to return to normal operation.

How to request a print-out

Check that the printer is on, and ready, before selecting which print-out you require.

To print the valid card list, enter the command M*3

To print the parameters, enter the command M*4

Valid card list: sample report

12:15:33 2, 05.03.91

Q2 9

0-00005678	0	15	0
1-12345678	0	15	0
1-12345679	0	15	0
1-12345680	0	15	0
1-12345681	0	15	0
1-12345682	0	15	0
1-12345683	0	15	0
1-12345684	0	15	0
1-12345685	0	15	0

Valid card list: explanation of sample report

The report starts with a page-break character (ASCII 12 decimal).

The first line shows the current time, day-of-week and date.

The second line is blank.

The third line shows the card “quadrant” that System1 has aligned itself to - this occurs on the first card through the reader after an M#969 or M#987 reset. In normal use, only Q1 and Q2 will be encountered. Q1 = six-digit cards (A-series, F-series, G-series etc. - see Appendix 5). Q2 = eight-digit cards. Also shown on the third line is the total number of valid cards and PIN-only numbers.

The fourth line is blank.

The fifth line is the start of the list of valid cards and PIN-only numbers. Each line starts with a space, followed by an “ID-type”:

O = PIN-only
1 = Microcard
2 = Wiegand
3 = Proximity
4 = Mag-stripe
5 = Bar-code

In normal use, apart from PIN-only numbers, only one card type will be valid in System1. After the ID-type is a hyphen (“-“) and then the eight digits which are the card or PIN-only number. Eight digits are always used, even if 4-digit PINs or 6-digit cards are used.

After the ID number is a space, then three sets of numbers:

The first number is the Time Group. In normal use this will always be “0”, meaning 24-hour access. It can only be changed from Ultragard - and if you are using Ultragard you are unlikely to be using the M*3 printout feature.

The second figure shows the “Expiry” value. In normal use this will be “15”, meaning that the card never expires. Unless using Ultragard, the only other value you might see here is “0” meaning that the card has been expired and cannot be used unless you re-validate it. The reason for it being set to “0” is if Card+PIN is enabled - if someone has four attempts at his PIN and gets them all wrong then the expiry flag will be set to “0” thus preventing further attempts. If using Ultragard then you can make use of the expiry feature which allows you to make a card valid only for a fixed number of days (1-14), after which it “expires”.

The final figure shows the Anti pass-back flag. This can be in the range 0-15 depending how recently the card has been used. When a card is used its flag is set to 15, and then starts decrementing gradually to 0. The speed of decrementation is determined by the setting of the M#5nn parameter- the larger the parameter value, the longer it takes for each card's anti pass-back flag to decrement to “0”. If the M#5 parameter is set to 00 then the value of a card's anti pass-back flag is irrelevant. If the M#5nn parameter is non-zero then each card is only allowed access if its anti pass-back flag is “0”.

Parameters list: sample report

```
12:25:31 6, 06.01.90  
  
MA0 MA6  
MB004 MB101 MB110 MB2AA  
MB300 MB317 MB320 MB331 MB341 MB351  
MB4001 MB500  
MB600 MB611 MB624 MB630000 MB640000  
MB715 MB845  
MBA12 MBA22 MBA30 MBA40  
M0B:  
M5B200 (2000/1072)  
M6BFFFF M7BFFFF  
M8B201 M8B300 M8B400
```

Parameters list: explanation of sample report

The example report is of an S1x after a reset, but after “printer mode” is enabled.

The first line shows the current time, day-of-week and date.

The second line is blank.

The third line always shows MA0 - ignore this. It is followed by MA6 which shows that PIN-only is disabled.

The fourth line shows a lock-strike time of 4 seconds (MB004), a normally closed door-sensor (MB101), date format of ddmmyy (MB101) and a baud rate of 9600 (MB2AA).

The fifth line shows that printer mode is enabled (MB300); the remainder of this line shows all the other communication parameters.

The sixth line shows a unit number of 001 (MB4001) and that anti pass-back is off (MB500).

The seventh line shows that Card+PIN is disabled (MB600); Infra Red reader is selected (MB611); PIN-only numbers have four digits (MB624); Timed Card+PIN is not enabled (MB630000) and Timed PIN-only is not enabled (MB640000).

The eighth line shows that the local door ajar alarm is set to 15 seconds (MB715) and that the remote door ajar alarm is set to 45 minutes (MB845).

The ninth line shows that Relay 1 (the lock strike relay) and Relay 2 are in normal operation (MBA12 and MBA22); the MBA30 and MBA40 refer to unused outputs - you can change them but they have no effect.

The tenth line shows which messages are currently disabled; in the example, none of them are disabled.

The eleventh line shows memory partition information. M5B200 means 200x10 cards; this is confirmed in brackets as 2000 cards and 1072 events.

The twelfth line shows the clocks forward and clocks back dates; any setting including one or more “F” characters or a setting of “0000” means that no dates have been set.

The final line shows that Relay 2 is programmed as an Alarm shunt relay. The M8B300 and M8B400 refer to unused outputs; you can change them but they have no effect.

Quit

This refers to the action of leaving programming mode and returning to normal operating mode. This is done automatically at the end of each completed command, with the exception of validating and voiding cards.

You can choose to quit while part-way through a command, or while validating or voiding (whether part-way through or at the end of a number) simply by pressing the # key once, twice or three times. The actual number of presses depends on exactly how far through a sequence you are at the time.

If you do not quit, then System1 will quit of its own accord after 10 seconds if no keys are pressed.

Reader type - M#61x

Command:	M#61x
Options:	M#611 = TDSi-technology Reader M#612 = Wiegand Reader M#613 = Proximity Reader or Hands-free Reader M#614 = Mag-stripe swipe Reader M#615 = Mag-stripe insert Reader M#616 = Bar-code Reader
Default:	M#611 = TDSi-technology Reader

Application

This allows you to select the reader type that is to be used with the controller. Note that in all cases except bar-code and mag-stripe the readers and the cards **MUST** be supplied by Time and Data Systems to be compatible with Microlock System1. (Bar-code is only available to special order at the time of writing).

Note that TDSi produce Microcards in four distinct categories known as “quadrants”. System1 self-aligns to the appropriate card quadrant when it sees the first card through the reader after either a reset (M#912 or M#969) or reader selection command. After this self-alignment, System1 will **ONLY** read cards from that “quadrant” - cards from other quadrants will always generate a “reader error” message.

System-1 is capable of reading mag-stripe cards swiped in either direction. If you have an insert reader, you must select M#615 otherwise System-1 will read each card twice - once going in and once coming out.

Restrictions

This programming operation should have been carried out during installation, after which there should never be any need to change it.

When you change from one reader type to another, cards in memory are **NOT** erased. You must do an M#987 reset to clear them out.

How to select a reader

Enter the appropriate command from the list at the top of this page.

Relays

Application

There are two relays fitted as standard to System. Each of these has a default function:

- Relay 1 is the lock release relay
- Relay 2 is the alarm shunt relay

You cannot re-program relay 1, but you can re-program relay 2 to provide another function instead of its default function.

Each relay provides a single change-over contact. This means that when relay 2 is ON (energised), it may have turned something ON or OFF - this depends on the connections made during installation.

There are two options available to you: "Program" (relay 2 only) and "Control" (either relay 1 or relay 2).

Program

The program function allows you to program Relay 2 to energise for one of two reasons:

- input-following
- alarm indication

Control

You can latch either relay ON or OFF using the CONTROL function. This includes the lock strike relay in this way you can bar all access, or allow free access by latching the relay (but beware of the duty cycle specification of the lock strike itself - some lock strikes should not be left on for extended periods of time).

How to program relay 2

Enter the command M8#2yy, where yy is taken from the list below (see the glossary after the table for an explanation of each event):

- 01 = Alarm shunt
- 02 = Door ajar (local alarm)
- 03 = Door ajar (remote alarm)
- 04 = Door forced
- 05 = Duress
- 06 = Access denied
- 07 = 4th wrong PIN
- 08 = Reader gone
- 09 = Input 1 ON (i.e. door sense)
- 10 = Input 2 ON (i.e. egress)
- 11 = Input 3 ON
- 12 = Input 4 ON

Glossary

Alarm shunt

If you program relay 2 to perform an alarm shunt function, the relay will turn on with the lock strike. If the door does not open, it will go off when the lock time ends. If the door opens before the lock time ends, then this relay will only go off when the door closes - no matter how much later this happens. This function is provided so that a person who is allowed through a door can get through the door without setting off the intruder alarm system. The relay must be connected across the alarm contacts so that as far as the intruder alarm is concerned the door appears to stay shut.

Door ajar (local)

The door was open for longer than the programmed permitted time.

Door ajar (remote)

The door was open for longer than the programmed permitted time.

Door forced

The door opened while the lock release relay was not energised. (The lock release relay can be energised in one of three ways: access granted after a card or PIN entry, egress button used, relay latched on).

Duress

A PIN has been used (as part of a PIN-only or a Card+PIN sequence) which was one digit higher than the expected PIN. For example, if 1234 was expected, then entering 1235 will cause this alarm.

Access denied

Access may be denied for any of the following reasons:

- Card not valid
- Wrong PIN (four attempts allowed)
- Anti pass-back applied
- Lock relay latched off
- Card “expired” (after four failed PINs - card must be re-validated)

Note that any message will identify WHY access was denied. But if you want relay 2 to come on then it will come on for ANY of the above reasons.

4th wrong PIN

After four (or more) unsuccessful attempts to enter a PIN (as part of a PIN- only or a Card+PIN sequence).

Reader gone

The reader wires have been cut or disconnected.

Input ON

This means that the input has been connected to 0V.

How to control a relay

Enter the command M#*xy, where x is the relay number and y is taken from the list below:

0 = OFF

1 = ON

2 = Normal

Note that when you return a relay to NORMAL, it will be either on or off according to its programmed function: if the relay is programmed to follow an input, or to indicate an alarm event, the relay will be on or off according to the current state of the alarm or input.

Resets - M#9xx

Commands: M#912 = reset parameters
 M#987 = reset cards
 M#934 = reset trail
 M#969 = reset everything

Application

These resets allow you to clear out all or part of the information held in System1. In normal use you should not find it necessary to use any of these resets.

Reset types

Reset parameters = M#912

This refers to all the programmable functions of the controller. For example, lock strike time, whether Card+PIN is in use, which messages have been turned off etc. If you execute this reset then ALL parameters will be returned to their default settings. Apart from the cards, PIN-only numbers and trail record, the only area NOT affected by this reset is the clock/calendar. Refer to Appendix 7 for a complete list of the default settings in System1.

Reset cards = M#987

This refers to all cards and PIN-only numbers.

Reset trail = M#934

This refers to the trail record memory. This is the information on events which have occurred; this information is erased anyway once it has been sent so this reset clears un-transmitted information. For example, if the printer ran out of paper then the event messages would be held in memory until the situation was rectified. Then all the events would be sent to the printer - this could be quite a lot of information and you might decide that you don't want it. You would use this function to clear out the trail record.

Reset everything = M#969

This reset is the same as executing all three of the above resets, and in addition the clock and calendar.

Validating cards

Note: this section also relates to validating PIN-only numbers. Throughout this section, any reference to “card” can be taken to include PIN-only numbers, unless otherwise stated.

Application

You must make a card or PIN-only number “valid” in order for it to be allowed access (“valid” means the card number is in the memory of the controller).

Note that there are two ways of validating a card:

- Validate card (single card at a time)
- Block validation (several cards) (does not apply to PIN-only)

Both of these methods are explained in this section.

The maximum number of cards allowed in memory is determined by you, up to an absolute maximum of 3000. See “Memory partition” elsewhere in this manual.

How to validate a single card

There are two ways of validating cards one at a time: from the keypad or at the reader. Doing it at the reader is faster, but you must have the cards in your possession - refer to the section titled “Master card” for more information .

To validate a card at the keypad, enter the command `M9#0abcdefgh` where `abcdefgh` is the number of the card, as printed on the card. See Appendix 6 if your card number is not 8 digits. Note that System1 stays in programming mode after the long flash which signals acceptance of the card. You can now enter another card number, without having to use the “M9#0” prefix. When you have finished entering card numbers, press “#” to quit. If you don't press any key for 10 seconds, System1 will quit anyway.

If you make a mistake

If you make a mistake part-way through entering a card number, press “*” and re-enter the number (without the “M9#0” prefix). If you make a mistake on the very last digit, you will need to void the card you have just validated.

How to validate a PIN-only number

Enter the command `M9#2abcd`, where `abcd` is the PIN-only number (and can comprise of 4, 5, 6, 7 or 8 digits). Read the section above “How to validate a single card” for additional information.

To change the number of digits in a PIN-only

Enter the command `M#62x` where `x` is the desired number of digits. When you execute this command, all existing PIN-only numbers will be erased.

How to validate a block of cards

Enter the command `M9#6abcdefghijklnop` where `abcdefgh` is the number printed on the first card in the block, and `ijklnop` is the number printed on the last card in the block. See Appendix 6 If card number is not 8 digits and “if you make a mistake” above for additional information. When you have completed the command the LED will flash 0.5 seconds on, 0.5 seconds off repeatedly until System1 has finished executing the command. But if the block of cards is small then you may only see one quick flash.

Important

This operation can take a short while to be processed. In normal use this will only be a few seconds - but if you are not careful it could take several minutes. The following guidelines will help you to avoid this:

- If you have two blocks to validate, then validate the LOWER of the two first.
- Do not exceed the available capacity of the controller (as set by you using the “Memory partition” command)

Voiding cards

Note: this section also relates to voiding PIN-only numbers. Throughout this section, any reference to “card” can be taken to include PIN-only numbers, unless otherwise stated.

Application

There are two ways of voiding cards: singly or in a block. PIN-only numbers can only be deleted singly.

How to void a single card

Enter the command M9#1abcdefgh where abcdefgh is the number printed on the card you wish to void. See Appendix 6 if card number is not 8 digits. Note that System1 stays in programming mode after the long flash which signals acceptance of the card. You can now enter another card number, without having to use the “M9#0” prefix. When you have finished entering card numbers, press “#” to quit. If you don't press any key for one minute, System1 will quit anyway.

If you make a mistake

If you make a mistake part-way through entering a card number, press “*” and re-enter the number (without the “M9#0” prefix). If you make a mistake on the very last digit, you will need to void the card. you have just validated.

How to void a block of cards

Enter the command M9#7abcdefghijklmnop where abcdefgh is the number printed on the first card in the block, and ijklmnop is the number printed on the last card in the block. See Appendix 6 if card number is not 6 digits. Read “how to void a single card” for additional information. When you have completed the command the LED will flash 0.5 seconds on, 0.5 seconds off repeatedly until System1 has finished executing the command. But if the block of cards is small then you may only see one quick flash.

How to void a PIN-only number

Enter the command M93Babcd, where abcd is the PIN-only number (and can comprise of 4, 5, 6, 7 or 8 digits). Read “how to void a single card” for additional information.

How to void all cards and PIN-only numbers

Enter the command M#987 - see RESETS for more information.

Unit number - M#4nn

Command: M#4nnn = set unit number to nnn
Range: 000-999
Default: M#4001 (unit number 001)

Application

In an Ultragard installation, each System1 (and System2) must be allocated a unique number. This number is used during communications with the units, and if two units have the same number then communication with those units will be impossible.

Restrictions

Ultragard "S" releases 1, 2 and 3 allow for unit numbers to be in the range 1 to 30.

Ultragard "S" release 4 allows for unit numbers to be in the range 1 to 60.

Default

The default is M#4001; i.e. unit number 001. There is no need to change this number if the unit is not connected to Ultragard.

How to set the unit number

Enter the command M#4nnn, where nnn is the required unit number.

Appendix 1: Trouble-shooting

As with most things, trouble-shooting System1 is simply a question of methodically eliminating the possible causes one by one, until the problem is solved.

This appendix assumes that the installation did work OK at one time - in other words, that no mistakes have been made during installation. The purpose of this appendix is to help you to find your own programming errors, or to identify equipment that has failed.

AS A FIRST STEP check that the LED on the reader is flashing. If it isn't, then there are two possible explanations: System1 is either in programming mode or the power may have failed. To confirm which is the case, switch off the power for 10 seconds, and switch it on again - System1 will definitely not be in programming mode so if the reader isn't flashing then the power has most likely failed.

Card won't release lock

- Power supply to lock has failed (listen for click from relay to confirm whether System1 is trying to release the lock)
- Card not known
- Card not valid in door
- Anti pass-back in force
- PIN time-out
- Wrong PIN
- Door already open, door sensor faulty or wrong door sensor type selected
- Lock relay latched OFF
- Faulty card-reader or wrong reader selected

Relay doesn't come on when expected

- Programming incorrect
- Relay latched OFF

Appendix 2: Printer messages

Messages appearing at the printer fall into two categories:

- Card/keypad messages
- Other messages

Card/keypad messages

Essentially, a card or keypad message contains four pieces of information: when, where, what and who.

For example:

```
18/05/90 12:15 003-0 M03451234 A
```

tells us that Microcard (M) number 03451234 was allowed access (A) at the door controlled by unit number 003 at 12:15 on May 18th 1990. (The “-O” identifier is included for compatibility with our two-door controller, System2, but means nothing in System1's case.) There are two space characters between the date and the time, and between the time and the unit number.

PIN-only numbers appear as “*****” (no matter how many digits used) for security reasons, and the line is padded with spaces to make it the same length as for a card message:

```
18/05/90 12:15 003-0 K***** A
```

Other messages

These messages relate to alarms, inputs, relays and the system. These messages are like card and keypad messages but do not require the “who” part, for example:

```
18/05/90 12:19 003-0 X05
```

This tells us that the door forced alarm (X05) occurred at 12:19 on May 18th 1990. The -0 identifier is omitted for Input, Relay and System messages.

Input, Timed Relay, Timed Card+PIN and Timed PIN-only messages

These messages have an extra character at the end which tell us whether the message relates to switching on (1) or switching off (0). For example, Relay 2 switching on would generate a message looking like this:

```
18/05/90 12:19 003 R02 1
```

Interpretation of printer messages

Card type:

M = Microcard (i.e. TDSi-technology card)
W = Wiegand
P = Proximity/Hands Free
K = PIN-Only
A = Mag-Stripe
B = Bar-code

Result:

A = access granted
B = ID not in memory
C = ID not valid for door
D = ID expired
E = out of Time Zone
F = anti pass-back enforced
G = PIN time-out
H = wrong PIN
I = 4th (or more) wrong PIN
J = man-trap enforced
K = Relay latched off

Other messages

X01 = Card read error
X02 = Duress
X03 = Door opened
X04 = Door closed
X05 = Door forced
X06 = Door ajar (local)
X07 = Door ajar (remote)
X08 = Egress on
X09 = Egress off
X12 = Reader gone
X13 = Reader back
R02 = Relay 2
R05 = Timed PIN-only
R06 = Timed Card+PIN
I03 = Input 3
I04 = Input 4
Z01 = clocks forward
Z02 = clocks back
Z11 = Restart (after power down or reset command)

Appendix 3: Access criteria

There is a set order in which the ACU checks a card's validity. If there is more than one reason for a card to be denied access, then only the first reason will be seen on any print-out.

1. Card not known
2. Wrong PIN
3. Anti pass-back enforced
4. Card expired (i.e. 4 or more wrong PINs)
5. Lock disabled (lock release relay latched off)

Appendix 4: Glossary

ACU

This is the box containing all the electronics, which can control access through one door.

Card-only access

This is the opposite of Card+PIN access - if Card+PIN access is off then what you have is Card-only access.

PIN-Only

Normally, having an access control system means that you issue people with cards which they use to gain access to various parts of your premises. Sometimes you might want to allow someone to gain access without the use of a card, while everyone else must still use cards. If you have a keypad installed next to a card reader, the "PIN-only" option allows you to program in a 4-8-digit code which, typed in at the keypad, will allow access. The ACU (q.v.) treats PIN-only numbers in an almost identical way to cards with one exception while you can set up Card+PIN access (i.e. people must use a card PLUS the correct PIN to gain access) there is no such thing as PIN+PIN access.

Appendix 5: Card numbers

Infra Red Cards

Mostly, 8-digit cards are used with System1. Validation and voiding operations use all eight digits. These cards are in Quadrant 2 (see Printouts for the significance of card quadrant).

If for reasons of compatibility with other TDSi products, you are using 6-digit cards then these cards will also have a letter of the alphabet preceding the six digits; for example F123456. Usually, these are in Quadrant 1. However, in Great Britain Quadrant 0 is also in use and the table below includes those cards for completeness.

Because you must always use eight digits, you will need to precede the six digit card number with two extra digits. These depend on the letter on the card; see table below. For example, for card F123456, you will use 02123456.

Letter	Digits	Quadrant
A	01	1
B	05	0
C	06	0
F	02	1
G	04	1
H	07	1
J	00	0
K	03	1
L	05	1
N	00	1
R	07	0
S	04	0
T	03	0
U	02	0
V	01	0

Mag-Stripe Cards

For mag-stripe cards, this is usually the last 8 digits of the account number. However this is not always the case so, if you have any problems, connect a printer to System1 and see what number appears at the printer when a card is used. Then try to see how this number relates to the number printed on the card. If there is no obvious relationship between the two numbers, then you will have to “log” every card in this way and keep a permanent record, for use when validating and voiding cards.

Wiegand, Proximity and Hands Free Cards

Wiegand, proximity and hands-free cards should be preceded by “03”.

Appendix 6: Default states

The following describes the state of System1 after a “Reset everything” or a “Reset parameters” command.

No PIN-only access
Lock release time = 4 seconds
Door sensor type = Normally closed (or not fitted)
Date format = day/month/year
Comms. mode = PC mode (9600 baud, special TDSi protocol)
Unit number = 001
No Anti pass-back
No Card+PIN access
TDSi-technology reader
4 digits in PIN-only and password
Door ajar (local) alarm after 15 seconds
Door ajar (remote) alarm after 45 minutes
All messages enabled
Memory partition = 3000 cards, 1008 events
Relay 2 = alarm shunt
Password = 1234

If you change from PC mode to printer mode, the following communications parameters apply:

9600 baud
7-bit word, even parity, 1 stop bit
XON/XOF handshake
full duplex

Effectivity Notice

This notice shows the following:

- The issue level of this document
- The revision level of every page in this document
- The modification history of this document.

However, the only way to be sure that you have a current copy of this document is to contact TDSi and ask to be told the current issue level of this document.

Document title	System1 User's Manual
Document Reference	6656-0118
Issue date	August 1996
Issue / Revision	4.1
No. of pages in this notice	2
Modification History	<p>Issue 1.1: First issue</p> <p>Issue 2.1 (M1386 April 1991): Complete re-issue following MSIN AC22.</p> <p>Issue 2.2 (M1457 December 1991): Error in block-void command (p 67). Added note about small blocks (p 66, 67).</p> <p>Issue 3.1 (M1725, 1740, 2096 May 1993): Errors in Card+PIN and Relay Control commands and Memory partition size. Reference to S1c removed. Manual re-issued in double-sided format.</p> <p>Issue 4.1 (M3528 August 1996): Complete re-issue in new style.</p>

Page	Rev.
1	4.1
2	4.1
3	4.1
4	4.1
5	4.1
6	4.1
7	4.1
8	4.1
9	4.1
10	4.1

Page	Rev.
11	4.1
12	4.1
13	4.1
15	4.1
16	4.1
17	4.1
18	4.1
19	4.1
20	4.1
21	4.1

Page	Rev.
22	4.1
23	4.1
24	4.1
25	4.1
26	4.1
27	4.1
28	4.1
29	4.1
30	4.1
31	4.1

Page	Rev.
32	4.1
33	4.1
34	4.1
35	4.1
36	4.1
37	4.1
38	4.1
39	4.1
40	4.1
41	4.1

42	4.1
43	4.1
44	4.1
45	4.1
46	4.1
47	4.1
48	4.1

49	4.1
50	4.1
51	4.1
52	4.1
53	4.1
54	4.1
55	4.1

56	4.1
57	4.1
58	4.1
59	4.1
60	4.1
61	4.1
62	4.1

63	4.1
64	4.1
65	4.1
66	4.1

Index

4

4th wrong PIN · 48

6

6-digit cards · 60

8

8-digit cards · 60

A

Access

- criteria · 58
- denied · 34, 48
- granted · 34

ACU · 59

ajar · 24

alarm shunt · 47, 48

Alarms · 15

Anti pass-back · 7, 16, 43, 48

B

Bar-code Reader · 46

baud rate · 22

Block validation · 51

Block-validate cards · 7

Block-void cards · 7

C

Calendar · 19

Card "expired" · 48

Card numbers · 60

Card/keypad messages · 56

Card+PIN · 7

- access · 17, 28

Card-only access · 59

Clock and calendar · 8, 19

Clocks forward and back · 35

Communications · 8, 21

- diagnostics · 8, 23

Computer mode · 21

Controller restarted · 35

D

data rate · 22

date · 19

format · 19

Door

forced · 25, 26, 34, 48

open · 34

sensor · 27, 29, 34

sensor type · 8, 25

Door ajar · 25

(I) and (r) · 34

(local) · 48

(remote) · 48

alarm · 24

local time · 8

remote time · 8

duplex · 22

Duress · 18, 28, 34, 39, 47

E

Effectivity Notice · 63

Egress · 26, 27, 34

Expiry · 43

F

Free Egress · 26

H

Hands-free

cards · 61

Reader · 46

handshake · 21, 22

I

immediate transmit · 21

Infra Red Cards · 60

Input ON · 48

Inputs · 6, 27, 34

K

Keypad · 28

L

LED · 10, 55

lock release · 47

Lock time · 8, 29

M

Mag-stripe

Cards · 61
 insert Reader · 46
 swipe Reader · 46
Master Card · 8, 30
Memory partition · 8, 31
Messages · 8, 32, 56

O

Outputs · 6

P

parameters · 42, 50
parity · 22
Password · 9, 10, 36
PIN-only · 9, 35, 51, 53, 59
 access · 28, 38
polling · 21
Printer · 41
 messages · 56
 mode · 21
Printouts · 42
Programming · 7, 28
 List · 12
 sequences · 11
Proximity
 cards · 61
 Reader · 46

Q

quadrant · 43, 46, 60
Quit · 45

R

Reader
 error · 34
 gone · 48
 gone/returned · 35
 type · 9, 35, 46
Relays · 9, 47
Reports · 9

Resets · 9, 50

S

stop bits · 22

T

TDSi-technology reader · 35, 46
 Application · 46
Time Group · 43
Timed
 Card+PIN · 17, 34
 PIN-only · 35
trail record · 21, 31, 50
Trouble-shooting · 55

U

Ultragard · 54
Unit Number · 9, 54

V

valid card list · 42
Validate
 card · 9
 PIN-only · 9
Validating cards · 51
Void
 card · 9
 PIN-only · 9
Voiding cards · 53

W

Wiegand
 cards · 61
 Proximity and Hands Free Cards · 61
 Reader · 46
word length · 22
Wrong PIN · 18, 39, 48