LogLock 3000/Mini v3.58

Attendance and Access Control System

User Manual, October 10, 2013, Rev. 53

Hardware and Firmware designed by:
ASPiSYS Ltd.
P.O. Box 14386, Athens 11510, GREECE (EU)
http://www.aspisys.com

Thank you for purchasing the all-new LogLock by ASPiSYS Ltd, an electronics design and manufacturing company. All systems are designed by us and manufactured in the EU.

This manual covers both LogLock 3000 (*the larger PCB*) and LogLock Mini (*the smaller UNiLOCK-sized PCB*)[1]. For most practical purposes, these two are identical but a few minor differences do exist. *This document refers to either system as simply LogLock, and where there are differences, they are noted.*

LogLock is a sophisticated, highly reliable, stand-alone access control and/or time-attendance system for use at homes, schools, universities, hospitals, and in almost any size business, from very small to quite large. LogLock is an enhanced version of the older LogLock 2000 product and it is in most ways identical to previous versions but offers additional functionality. User and log capacity is different, however, while several user/log ratios are possible upon ordering. *The major differences with LogLock 2000 are the lack of the PIN capability, and the smaller overall user/log file sizes. In most respects, however, LogLock outperforms LogLock 2000 both in features and speed; to name a few, various ordering options for up to 3520 maximum users, about 10 times faster overall speed (e.g., searches), 6 times faster log retrievals due to significantly increased internal baud rate, alarm connection capability, and, very importantly, simple fail-proof over-the-network firmware updates without loss of current users and log.*

Because of the entry/exit 'audit trail' capability in a single device, one can use any LogLock system not only to control access, but also as an attendance clock, or as a 'tracking' system for access to sensitive resources *(e.g. computer room, machinery room, office supplies locker, etc.)*

Due to the various versions available, some commands or capabilities may not be enabled or active in all versions. For example, the sound option is not available in the smaller *LogLock Mini* version. Also, although both PCB versions support the connection of a 20x4 LCD *(for date/time, and user ID/name display during entry or exit),* one may not be offered with all versions, mostly depending on the enclosure used. *Unless other arrangements are made in advance, both systems are currently available in PCB format (without a specific enclosure). LogLock Mini's dimensions are 100% compatible to our simpler UNiLOCK product, so a UNiLOCK enclosure is readily available, on request.*

[1] See drawings at the end of this document

About the keys

LogLock uses factory-guaranteed non-copiable world-unique electronic keys from stainless steel *(known as iButtons ®[2])* to identify each user. Each user need only be given a single key regardless of the number of access points *(LogLock or UNiLOCK units – our other system)* installed at one's premises. Unlike 'credit card'-like keys, iButtons can withstand heavy abuse including extreme levels of heat, cold, and moisture. One can step on them or even take them into water. They are virtually indestructible. All types of iButtons can be used with LogLock without affecting third-party systems these iButtons may be used with.

General Characteristics / Capacity[3]

The two major characteristics of LogLock are reliability and ease of use. Just touch the special battery-free electronic key to the corresponding key reader, and *(if you meet all access control requirements)* you're in, *all in less than one second*.

LogLock uses a highly optimized real-time multitasking Operating System (our own OS8) which makes it possible to have the system operate continuously *(except during firmware updates)*, even when making changes or retrieving the log through the terminal. *Compare this to many competitor systems where the main functions must be suspended during log retrieval or system configuration.*

LogLock is completely stand-alone, meaning that once programmed with its various parameters, user database, and access control rights, no further connection to a PC is required for operation. A PC is only required to make configuration changes or to retrieve the log.

The wrapping log keeps as many of the most recent actions as can fit in the device. This means, one may leave the device unattended and only connect to it to retrieve the log when there is need *(e.g., for payroll use, a once-a-month connection may be enough in many situations).*

The system has a built-in calendar clock *backed by a user-replaceable battery (CR2032/CR2025)*. The clock auto-switches from/to DST based on EU rules.

[2] *iButton is a registered trademark of Maxim Integrated Products/Dallas Semiconductor*

[3] Specifications are subject to change without prior notice.

One significant feature of LogLock that sets it apart from most, if not all, competition is that the complete operating software is built-in, and it uses plain language commands. No special PC software is required; any telnet terminal emulator will do. This means, the system is not tied to a specific computer platform. It can be connected to from any operating system, as long as it has a telnet application *(practically all do)*. One can even connect from a smart *[cell]* phone with a telnet application[4]. Strong 20-char user-defined passwords *with 5-sec delays on each failed attempt* protect from unauthorized terminal access.

Because of the standard Ethernet connectivity, the device can participate in a larger network and, therefore, connected to from any part of the world[5]. As an example, one can have hundreds or thousands of units deployed all over the world, all fully managed from a single location.

Even firmware upgrades can be performed from a distance, without placing the controlled area at risk during the upgrade procedure, as the system defaults to no access during such times. Firmware upgrades take less than a minute to complete not causing any major downtime.

One important feature of the system is the use of ‘passive’ key readers *(i.e., they contain no electronic circuit)* that are simple and nearly cost-free, while the actual system is always securely installed inside the protected area. One may also connect in parallel two *(or more)* readers so that if the main *(obvious)* reader is ever vandalized, one can still use another reader *(placed somewhere less obvious and less easy to reach)* to gain access. With most competitor systems *(especially those not based on the iButton technology)*, the reader is active *(contains electronic circuit)* and, if it breaks, the system becomes non-functional until the reader is repaired or replaced.

Another important feature of LogLock is the ability of a single device to control up to two doors, one for both entry and exit, or one for entry and a different one for exit. This is mostly useful for garage or one-way turnstile installations.

Only one device is needed to control both sides of the door. Compare that to many competitor systems which require a unit on each side of the door, increasing both cost and installation complexity. With LogLock, only a single pair of wires need to cross the wall to the outside. *The wires themselves can act as a reader if the actual reader is vandalized.*

In the default OEM configuration, each LogLock device can hold up to 448 unique users *(keys), each with their own name and optional zone access restrictions*, and a wrapping log of up to 5733 actions.

Note: If a version with a larger number of maximum keys is requested this will most likely affect the maximum possible log size. For example, for 896 users, the available

[4] A data plan and service availability is required. Charges may apply and depend on one’s service plan.

[5] Internet connectivity is required in this case.

log is 4485. Because memory size is fixed, as one file size increases (maximum users and/or username length) another decreases (maximum log) and vice versa. This manual references file sizes for the default version. If ordering a different version, please specify your actual user requirements taking into account possible near future increases in user population.

Each time a verified user enters or exits the controlled area, LogLock records the date, time, direction, and unique user ID while striking the door open. This allows the owner or manager of the system to figure out how much time people spent inside, or simply see when they showed up to work. One can optionally have the device record both successful and unsuccessful attempts from registered users. This feature lets one see if anyone attempted to enter outside of his or her approved 'shift'.

When a key is either lost or stolen, the user should be deactivated from the system. This renders the key totally useless to whoever has it, and the original user can replace it with a new one.

<u>In short, these are the features of the LogLock system.</u>

Maximum unique keys (people):	448 (*default*) to 3520 (*depends on version*)
Maximum day-of-week/time zones:	1020 zone entries (in up to 254 zones)
Special fixed zones:	'Always Allowed' (0) & 'Never Allowed' (255)
Maximum fixed holidays:	256 entered as `DDMM`
Maximum entry/exit recordings:	5733 with most recent 5695 always available (depends on version). *Note: The maximum log size may be smaller in versions with greater number of maximum keys.*
Languages supported:	English *(anywhere)* or Greek *(LCD and user names in listings only).* *For larger orders, we may be able to replace Greek with another language, on request.*
Door-open delay setting:	0 *(strike disabled)* to 25.5 seconds with 1/10th of a second resolution. The delay is entered as integer; for example, for 1.5 seconds, enter 15 *(with no dot in between).* Optionally, use different delay for each strike.
Door-strike mode:	AC-like (*less quiet strike, less current, better feedback*) or DC (*quiet strike, or for driving external relays*). Optionally, use different mode for each strike.
Alarm mode:	Optionally, use an external alarm for detecting door-left-open using a delay from 1 to 255 seconds to activate and a separate delay from 0 to 255 seconds to de-activate. *The alarm starts immediately if opening the door 'illegally', and after specified On Delay for 'legal' openings if door remains open after specified timeout. The alarm stops after specified Off Delay unless there is a valid access in between.*
Sounds/Beeps:	Enabled *(for better feedback)* Disabled *(for minimum noise tolerance)* *The sound option is not available with LogLock Mini.*
PIN mode:	Not available with either PCB version. **<u>Prefer the original LogLock 2000 system, if the PIN feature is a must.</u>** *Note: PINs are still defined in user records for compatibility with backup files from previous and/or future LogLock versions, but not saved.*
Password protection:	Case-sensitive 20-char long. Separate passwords for terminal access (`LOCK`) and system configuration (`PASS`). Protects system from unauthorized browsing or configuration changes.

Date and time setting: CR2032/CR2025 battery-backed Real Time Clock (RTC)

File/Settings directory: Shows total, used, and free sizes for each file, current settings, and special conditions.

Backup/Restore/Clone: Dedicated backup command *(ASCII terminal screen capture.)* Restore or clone to another device simply by sending the ASCII backup to the device.

Search who is currently logged in: Search all or restrict by [partial] name.

Log listing and backup: Show all actions or restrict by [partial] name. Backup with terminal screen capture – *for security reasons, a captured log cannot be loaded back to the device.*

User listing and backup: Search all or restrict by [partial] name. *(Backup via terminal screen-capture)*

Zone listing and backup: Show all or specific zone number *(Backup via terminal screen-capture)*

Holiday listing and backup: Show all *(Backup via terminal screen-capture)*

Log restricted by date range: Yes, None, `FROM / TO`, `FROM` only, `TO` only.

Monitor mode: Easily grab any iButton key IDs, or see who’s attempting access, even non-users.

Single entry & exit control Entries and exits using the same ‘door’.

Separate entry & exit control Entries and exits using separate ‘doors’. This is useful for dual lane [entry/exit] garages, or separate turnstiles.

Open entry and/or exit control Useful for rush hours or special events. Manual on/off, or automatic on/off based on zone schedules.

Optionally, restrict on ‘boss’ Access won’t be granted to anyone if (all) the boss(es) is (are) out. *Optionally, it can allow only certain zones to enter (e.g., cleaning lady) when the boss(es) is (are) out.*

To get a list of the available commands, type `'?'` or `'HELP'` on a blank terminal line and press `[ENTER]`. Press `[ESC]` to cancel the listing or to clear the command line, press `[CTRL-S]` *(i.e., while holding down `[CTRL]` press `[S]`)* to temporarily pause the listing, and `[CTRL-Q]` to continue a paused listing.

Note: If the system seems non-responsive to anything you type, try `[ESC]` followed by `[CTRL-Q]`, preferably in that order, in case the system was either halted or in monitor mode. Also, when sending commands automatically from any application, please make sure to start each communication session by issuing these two characters to place the device's terminal in a known state, again for the same reason.

Commands that have no parameters (like `CLS`) work immediately, as described in the general help screen.

Commands that display user information or log activity (i.e., `U, L, LAST, LL,` and `WHO`) may be followed by a partial or full name to match only those records that have a match in all or part of the name.

Most commands that require parameters *(except for those of the previous paragraph needing a name and a few special ones)*, if typed without any, print a short help message particular to that command.

Note: The available command set is subject to change with each new firmware revision (without prior notice) to either improve or add functionality. Every effort is made to keep changes backwards compatible, but in some cases this is just not feasible.

This is the main help screen:

```
Commands
========
AC .................. Pulsed strike
AH .................. Add holiday
ALARM ............... Set alarm times
ANSI ................ ANSI cls
AU .................. Add user
AUTO ................ Auto-exit
AZ .................. Add zone
BACKUP .............. Backup config
C ................... Set clock
CLEAR ............... Clear counters
CLEARALLFILES ....... Clear ALL files
CLEARLOG ............ Clear log
CLS ................. Clear screen
D ................... Set log date range
DC .................. DC strike
DEVICE .............. Show/change device name (? deletes)
DH .................. Delete holiday
DIR ................. Show settings
DT .................. Doorstrike time
DU .................. Delete user
DZ .................. Delete zone
```

```
DZU ................. Delete zone users
EN .................. English
ENTRY ............... Open Entry [zone]
EXIT ................ Open Exit [zone]
GR .................. Greek DOS
GRW ................. Greek Win
H ................... Show holidays
HIDE ................ Hide IDs & names
IN .................. LCD is inside
INFO ................ OEM info
L ................... Show [named] user log
LAST ................ Show last [named] user log
LCD1 ................ Uni-LCD
LCD2 ................ Bi-LCD
LL .................. Show quick user log
LOAD ................ Load config
LOCK ................ Change lock password
LOGALL .............. Log all attempts
LOGSAME ............. Log same actions
LOGUNIQ ............. Log unique actions
M ................... Monitor [min timeout]
MASTER-RESET ........ Reset passwords
MU .................. Move user zone
NOAUTO .............. No auto-exit
NOENTRY ............. Closed Entry
NOEXIT .............. Closed Exit
NOHIDE .............. Show IDs & names
NOLOGALL ............ Log successful attempts
NOPASS .............. Exit current mode
NOZZI ............... Normal ZZR
NOZZR ............... Normal zone check
OUT ................. LCD is outside
PACK ................ Remove deleted
PASS ................ Enter config mode / change password
PBZ ................. Set push-button zone
RESET ............... Restart unit
REM ................. Remark [string]
REN ................. Request Entry
REX ................. Request Exit
S1 .................. Single door
S2 .................. Split door
SAVE ................ Save config & passwords
U ................... Show [named] users
UPGRADE ............. Firmware upgrade
WHO ................. Show [named] IN users
ZZI ................. Invert ZZR
ZZR ................. ZeroZone requirement [level]
Z ................... Show [n] zones
```

The following commands may also display in the help screen *(e.g., LogLock 3000, or special-purpose versions).*

```
LIMIT ............... Limit Users-In
NS .................. No sound
S ................... Sound
```

Quick Start: A brief description of each command (OEM defaults are shown underlined)

`AC` Tells the system to use **AC**-like pulses for driving one or both door strikes. The PWM ratio is 70%. *If followed by AC or DC the exit strike may differ, accordingly. The first value is for entries, and the second for exits.*

`AH` **A**dds a single **H**oliday record.

`ALARM` Any value from 1 to 255 enables the **`ALARM`** feature for the specified number of seconds. Use zero to completely disable the alarm feature. An optional second value from 0 to 255 turns off the alarm so many seconds after the alarm condition has stopped. An alarm condition begins either immediately upon opening a door without using a valid key or an allowed `REN/REX` command *(based on current date/time, zone, and `ZZR` settings)* or after specified delay *(in case door was left open after valid use).*

`ANSI` Similar to `CLS` *(see below)* but changes an **ANSI** terminal's color to black on gray *(some people find it easier on the eyes).*

`AU` **A**dds a **U**ser *(you must provide iButton ID, zone, and name).*

`AUTO` Enables the auto-exit feature. Auto-exit works only for zone entries with the `AUTO` option defined. If followed by a zone number *(including zero zone)* the auto-exit is performed immediately for the specified zone. *This feature is not available along with the `LIMIT` command.*

`AZ` **A**dds a single **Z**one entry.

`BACKUP` Creates an ASCII **BACKUP** of all files and configuration settings. Sending the created file to any compatible LogLock device creates a clone. *For security reasons, the log file or the secret passwords are not backed up, so these two aspects of the device cannot be cloned. (The `CAA` and `TEMP` commands are backed up but their values are specific to a single device and may not apply to another device for cloning.)*

`C` Set the Real Time **C**lock. Use the `YYMMDDhhmmss` format for entering the clock date and time. *If the clock has lost its date/time, the status LED will blink rapidly (LogLock Mini) and the `DIR` display will show `[INVALID]` next to the time.*

`CAA` **C**lock **A**ccuracy **A**djustment changes the accuracy of the clock. *You should <u>not</u> change this value from the OEM default 1000 (milliseconds per second). This command is used primarily for OEM testing but it is made available because it can also be used in the unlikely case that after years of operation the clock is running way too fast or way too slow, due to crystal aging. [Please note it is normal for any clock to run a little slow or fast which is noticeable over a 'long' period of time (e.g. month). Such tiny adjustments are not possible with the `CAA` command. You may have to re-set the clock every so often to correct the time, if extreme clock precision is required.]*

`CLEAR` **CLEAR**s the various counters (alarm, failed password attempts, and resets) shown in the `DIR` display, next to the alarm delay settings. All counters count up to 255.

`CLEARLOG` **CLEAR**s (empties) the **LOG** file.

`CLEARALLFILES` **CLEAR**s (empties) **ALL FILES** (user, zone, holiday, and log). Does not affect settings or passwords.

`CLS` **CL**ears the terminal **S**creen.

`D` Clears or sets the **D**ate range used for log filtering.

`DC` Tells the system to use **DC** for driving one or both door strikes. The PWM ratio is 100%. *If followed by AC or DC the exit strike may differ, accordingly. The first value is for entries, and the second for exits.*

`DEVICE` Shows the current string or defines a new **`DEVICE`** string *(e.g., name or comment)*. Use `?` as the string to remove the current setting. The string length is limited to 60 characters. The string displays either by using the `DEVICE` command without any parameters, or as part of the `INFO` command. *Available since v3.31*

`DH` **D**eletes a **H**oliday record.

`DIR` Shows a **DIR**ectory with the current files, sizes, and settings.

`DT` Sets the **D**oor-strike **T**ime in 1/10th second increments from zero (disabled) to 25.5 seconds. *If two values follow, then the entry and exit strike durations may be set differently. The first value is for entries, and the second for exits.*

`DU` **D**eletes a **U**ser by ID.

`DZ` **D**eletes a **Z**one (all its entries) by Zone Number.

`DZU` **D**eletes all users assigned to a specific zone, provided as parameter to the command. If the zone is not given, the current PBZ zone will be assumed. Because this command is potentially dangerous, you must answer Y(es) to the confirmation prompt to proceed. Any other key press will cancel the command. For protection against mistakes, this command is restricted from removing zero zones. *(Hint: You may use the actual PushButton after setting PBZ to zero to remove all zero zones in one step, if needed. Don't forget to change the PBZ zone back to a non-zero number, however.)*

`EN` Sets the device to use the **EN**glish language.

`ENTRY` Engages the **ENTRY** strike *(opens the entry door)* if the current `ENTRY` zone is zero, or assigns the entry zone. A zone other than zero disables the manual `ENTRY` command.

`EXIT` Engages the **EXIT** strike *(opens the exit door)* if the current `EXIT` zone is zero, or assigns the exit zone. A zone other than zero disables the manual `EXIT` command.

`GR` Sets the device to use the **GR**eek language *using a DOS codepage*.

`GRW` Sets the device to use the **GR**eek language *using a Windows codepage*.

`H` Shows the list of defined **H**olidays.

`HIDE`	Partially **HIDE**s the display of user IDs (and user names on the LCD) when in normal mode. *Config mode always shows complete IDs.*
`IN`	Uses the inside reader for the `PBZ` option. LCD equipped units only: The LCD is assumed to be on the **IN**side; therefore, it shows actions and names for exits.
`INFO`	Displays the firmware version, ROM version, custom user message *(see `DEVICE` command)*, and OEM contact details (when followed by any parameter).
`L`	Shows the user **L**og for all or specific user names.
`LAST`	Shows all *or specific* users' **LAST** action(s), based on current log status. (This is similar to the `WHO` command but it shows all actions, not just the entries.) *Available since v3.19*
`LCD1`	Shows access-related LCD messages for one side only (either entry or exit, depending on whether the unit location is Outside or Inside). *Available since v3.44*
`LCD2`	Shows access-related LCD messages for both sides (ignoring the unit location setting). This is useful when the device LCD is monitored by a guard, or the device is used only as a time-attendance clock with both readers on the same side, near the LCD. *Available since v3.44*
`LIMIT`	Places a **LIMIT** on the number of users who may be inside at any one time by not allowing further entries when the limit is reached and until someone exits to make room for another user. A value of zero disables the limit feature. *This command is available only on request for special-purpose versions (e.g. special garage use).*
`LL`	Shows **L**imited **L**og; same as L but with no username display. It can be used for faster retrieval of longer log files, and/or better privacy from prying eyes.
`LOAD`	Re**LOAD**s configuration & passwords (canceling all unsaved changes).
`LOCK`	If in terminal locked mode, it enters user mode *using the `LOCK` password*. In user mode, it does nothing. In config mode, it changes the `LOCK` password. *Available since v3.23*
`LOGALL`	Sets the logging mode to '**Log all** attempts'.
`LOGSAME`	Sets the logging mode to '**Log** repeated **same** actions'.
`LOGUNIQ`	Sets the logging mode to '**Log uniq**ue actions only'.
`M`	Enables **M**onitor mode. *Normal mode can only enable this mode for up to one minute at a time. Config mode can enable the Monitor for up to 1440 minutes (24 hours). You can exit Monitor mode at any time by pressing [ESC].*
`MASTER-RESET`	Resets all passwords. *WARNING: It requires a one-time access code from ASPiSYS.*
`MU`	**M**ove **U**ser *(by ID)* to another zone. A quicker way to change a user's zone. *Available since v3.20*

`NOAUTO` Disables the auto-exit feature. Auto-exit works only for zone entries with the `AUTO` option defined. *This feature is not available along with the `LIMIT` command.*

`NOENTRY` Disengages the entry door-strike *(closes the entry door)* if the current `ENTRY` zone is zero.

`NOEXIT` Disengages the exit door-strike *(closes the exit door)* if the current `EXIT` zone is zero.

`NOHIDE` Shows the complete user IDs (and user names on the LCD) when in normal mode. *Config mode always shows complete IDs.*

`NOLOGALL` Sets the logging mode to ‘Log successful attempts’.

`NOPASS` If in config mode, exits to user mode. If already in user mode, it exits to locked terminal mode. *No system changes are possible.*

`NOZZI` Cancels the `ZZI` sub-mode.

`NOZZR` Sets the `ZZR` mode to ‘Normal zone check’.

`NS` **N**o **S**ound. Turns off system sound (beeps). Possible alarm events may still occur.
Not available with LogLock Mini.

`OUT` Uses the outside reader for the `PBZ` option.
LCD equipped units only: The LCD is assumed to be on the **OUT**side; therefore, it shows actions and names for entries.

`PACK` **PACK**s all files by removing any deleted records.

`PASS` If in terminal locked mode, it enters user mode *using the `LOCK` password – just like the `LOCK` command*. If already in user mode, it enters config mode *using the `PASS` password*. If already in config mode, it changes the `PASS` **pass**word.

`PBZ` Define the active **P**ush-**B**utton **Z**one.
This feature is available with LogLock Mini only.

`RESET` **RESET**s (restarts) the device, as if when powered-up. It loses any unsaved settings.

`REM` **REM**ark string. Useful for script files *(such as backup configuration files)* for adding comments or blank lines. Does not do anything.

`REN` **R**equests **EN**try, the entry strike activates for the primary `DT` time.
Same action as pressing the `REN` push-button (if connected).

`REX` **R**equests **EX**it, the exit strike activates for the primary `DT` time *(if in `S1` mode)*, or the secondary `DT` time *(if in `S2` mode)*.
Same action as pressing the `REX` push-button (if connected).

`S` Turns on system **S**ound (beeps).
Not available with LogLock Mini.

`S1` Selects ‘Single door’ mode for entries and/or exits. *The zoned `EXIT` command is active even in the `S1` mode.* In `S1` mode, entries, exits, and the `ENTRY` command always activate the primary ‘door’ strike, but a zoned `EXIT` command activates the secondary ‘door’ strike. *A simple (zone zero) `EXIT` or `NOEXIT` command automatically sets the device in `S2` mode to get the expected behavior.* When in `S1` mode, the secondary ‘door’ strike can be used as a timed on/off switch to drive an external relay for various functions (e.g., it can be used to automatically turn on/off the power supply to air-conditioning or other power-hungry equipment, or the store's light signs during hours dictated by the `EXIT` zone and current `ZZR` mode). Because in `S1` mode the secondary strike assumes an auxiliary function and it is no longer used for exits, the alarm is not affected by the current state of the secondary strike.

`S2` Selects 'Split door' *(separate entry / exit)* mode. Entries and the `ENTRY` command always activate the primary 'door' strike, while exits and the `EXIT` command always activate the secondary 'door' strike.

`SAVE` **SAVE**s active configuration & passwords.

`TEMP` Defines a signed correction offset for the internal MCU **TEMP**erature measurement.
You should <u>not</u> change this value from the default 0 (no offset) or you may get incorrect readings in the `DIR` command. This command is for OEM use. In the LogLock Mini version, it is normal for the temperature to reach about 65º Celsius, due to the close proximity of the Ethernet module to the MCU. It is not a malfunction.

`U` Shows all or specific **U**sers.

`UPGRADE` Initiates a firmware **UPGRADE** procedure. ***WARNING: Make sure you have the appropriate firmware file (for your specific model and ROM version) available before answering 'Y'es – case insensitive – to the confirmation prompt, or you'll lose the current firmware, and the device will become unusable for access control. Press [ESC] to cancel (the system will auto-reset).*** Detailed instructions for upgrading are provided later on.

`WHO` Shows all *or specific* users **WHO** are currently inside the controlled area, based on current log status. (This is similar to the `LAST` command but it shows only entries.)

`ZZI` Inverts the permission of the `ZZR` mode.

`ZZR` Sets the `ZZR` mode to "**Z**ero**Z**one **R**equired", or changes the "ZZR Check Above" level to the number that follows.

`Z` Shows all **Z**one entries, or all entries for one specific zone.

About Zones

Access control is based primarily on two aspects: Having a valid key (the iButton ID – token), and being allowed to enter on a given day-of-week and time zone. So, what is a zone?

A zone is used to define days-of-week and hours *with down to the minute resolution* within those days when access is allowed. *Note: Zones may also be used in conjunction with the `ENTRY` and `EXIT` commands, see appropriate section for details.*

As an example, employees following a typical Monday thru Friday, 9am to 5pm schedule would be assigned to a zone where Monday, Tuesday, Wednesday, Thursday, and Friday excluding holidays are allowed, but only from the hours between 9am and 5pm. During all other hours, or during any hours on Saturdays, Sundays, or holidays, they are not allowed access.

The `AZ` (Add Zone) command is used to create a new zone entry. A single zone may have more than one entry. This accommodates situations where a single entry isn't capable of defining the complete schedule for a zone. All entries of the same zone act as a single zone; therefore, a user assigned to any one zone is affected by all its entries. Here's the help screen of the `AZ` command:

```
Use: AZ n SMTWTFSH hhmm hhmm [AUTO]
     n=1-254
     For SMTWTFSH (Sun-Sat & Holidays) a dash (-) turns the
     corresponding bit off. Anything else turns it on.
     Times in hhmm format, e.g., 0900 1700 for 9am-5pm
```

A user-defined zone may be numbered from 1 to 254. A user, however, can be assigned to a zone numbered from 0 to 255. The two extra zones, 0 and 255, are special and always defined by the system. *Zone 0 is to be assigned to those with no access restrictions whatsoever, while zone 255 is to be assigned to anyone whose attempts to enter we want to monitor but whom we never want to allow entrance. For some commands, zone 255 is used to effectively turn off the relevant feature.*

Days can be defined as a series of eight 'flags' of either dashes (-) or any other printable characters (except for space, dash, or special control characters) in their natural sequence, Sun-Mon-Tue-Wed-Thu-Fri-Sat followed by the Holiday indicator. A dash means the day *(or holiday)* isn't accessible for that zone entry; any other character makes the corresponding day accessible. The holiday bit of the flags indicates whether or not the zone also allows access on fixed holidays. *Starting with v3.32 the holiday bit can be set by itself (i.e., without any days), in which case the particular zone entry affects only holidays, regardless of the actual day-of-week.* Fixed holidays are defined separately *(see the `AH` command). Currently, there is no provision for defining moving holidays, but a workaround mentioned later on is possible.*

To add the zone mentioned in the earlier example, one would give the command:

```
az 1 -MTWTF-- 0900 1700
```

(or the equivalent simpler and quicker to type `az 1 -11111-- 0900 1700`)

You can verify your entry by giving the command `Z` to display all zones. If you have many zones defined and want to view only a specific zone number, follow `Z` by the desired zone number (in this example, `z 1`).

The zone number in the example above is 1, so any user who must obey this zone's restrictions must be assigned to zone 1. A zone may have more than one entry, if necessary. However, when deleting a zone with the `DZ` (Delete Zone) command, all entries for that zone are deleted, i.e., the whole zone is deleted. One cannot delete only a single entry of a zone.

Zones are independent of one another. If a zone covers certain day-of-week and time combinations, it does not restrict another zone from covering the same days and times.

It is not required that one adds all zone entries for the same zone together. One can add one entry for zone 1, then add an entry for zone 2, then go back *(days or months later)* to adding one more entry for zone 1, and so on, as the circumstances dictate.

Let's take the example of a typical *Greek* retail store with morning and evening hours, as well as Saturday mornings. The following defines a schedule for Monday thru Friday from 9:00am to 2:00pm, Tuesdays, Thursdays, and Fridays from 5:30pm to 8:00pm in addition to morning hours, Saturdays from 10:00am to 3:00pm, and never on holidays, *all time boundaries inclusive (e.g., the end time of 1400 blocks access when time changes to 14:01:00, use 1359 if you want access to terminate at exactly 14:00:00).*

```
az 2 -MTWTF-- 0900 1400
az 2 --T-TF-- 1730 2000
az 2 ------S- 1000 1500
```

A person with access in zone 2 *(above)* may enter in any of these days and within those hours. S/he can exit anytime *(see note in box below)*.

If multiple entries in a zone give opposing or overlapping rights, the effective combination of these zone entries is applied during the authentication check. So, for example:

```
az 3 -MTWTF-- 0800 1400
az 3 -MTWTF-- 1000 2000
```

allows entry on weekdays from 8:00am to 8:00pm (inclusive), which is the effective schedule of the two zone 3 entries combined.

IMPORTANT: A zone has effect only for the entry of a person, not the exit. In other words, if a person enters on time *based on their assigned zone*, they will be able to exit any time or date afterwards, preventing a potential 'locked in' situation. This means that the actual zone can be limited to the expected entry times only, rather than the whole day schedule. So, for a 9am to 5pm scenario instead of defining `0900 1700` (as indicated in the earlier example), one could define `0850 1100` to allow people arriving a little early to enter rather than wait outside, but not allow anyone over two hours late to enter, provided this is the assumed company policy. *This works well only if employees are expected to stay in throughout their work hours. If they may go out for lunch (for example) one must allow for those times also.*

To assign a zone that spans midnight, one MUST break it up into two pieces, the first until 23:59 and the second from 00:00 to the end time, or it will not work as one might think, e.g.,

```
az 4 –M-W-F-- 2100 2359
az 4 ––T-T-S- 0000 0100
```

lets those in zone 4 enter on Monday-Wednesday-Friday's from 9:00pm to 1:00am, which is always on the following day, as also shown in the definition. This, on the other hand, will not work: *`az 4 –M-W-F-- 2100 0100`* because not only does it ignore Tue/Thu/Sat's but also because it is saved as `az 4 –M-W-F-- 0100 2100` with the time automatically swapped *if needed* so that the starting/earlier time is always before the ending/later time.

One can also define a schedule just for holidays. For example, a telephone operator's allowed shift may be defined as follows:

```
az 5 SMTWTFS- 0800 2200
az 5 -------H 1000 1600
```

This allows entry anytime between 8:00am and 10:00pm on all non-holiday days, and only between 10:00am and 4:00pm on holidays *regardless of day-of-week*. A zone with only the holiday bit was not possible in earlier versions. The addition of this new option is fully backwards compatible, and does not alter the behavior of zones defined as in earlier versions.

One can define auto-exit zone entries. For this feature to work, the system must be in `AUTO` mode *(see `DIR` screen and commands `AUTO` and `NOAUTO`, the OEM default is `NOAUTO`, which is compatible with previous versions). Only zoned people may have auto-exits. ZeroZone people cannot be auto-exited because they do not belong to any user-defined zone. If the `AUTO` command is followed by a zone number (including zero zone) the auto-exit is performed immediately for the specified zone. Auto-exits do not strike the 'door', they only record a hypothetical exit (marked as `AEXIT`) based on schedule.*

As an example for this feature, one may want to automatically exit people who have a tendency to not register when they leave. The system will auto-exit anyone whose zone entry is followed by the keyword `AUTO` at the last minute of that specific zone entry. For example,

```
az 6 -MTWTF-- 0900 1700 AUTO
```

will auto-exit any person belonging to zone 6 at 5:00pm on weekdays.

If a person strikes a true exit after the auto exit, this action will be registered, separately. If a person strikes a true exit before the auto exit *(and, therefore, that person is no longer inside)*, no auto exit will occur for that person.

A zone can have some entries with and some entries without the `AUTO` option to get the specific effect one needs. For example,

```
az 7 –M-W---- 0900 1400 AUTO
az 7 --T-TF-- 0900 1400
az 7 --T-TF-- 1730 2000 AUTO
az 7 ------S- 1000 1500 AUTO
```

This is similar to example zone 2 *(defined earlier)*, but it will auto-exit people at the end of their workday. Note that for Tue-Thu-Fri's where there are morning and evening hours, the auto-exit in this example occurs only at the end of the evening hours.

One may cause specific auto exit times within longer schedules by adding only the auto exit times as separate entries. For example,

```
az 8 -MTWTF-- 0900 2100 AUTO
az 8 -MTWTF-- 1300 1300 AUTO
az 8 -MTWTF-- 1700 1700 AUTO
```

The above enables people to enter on weekdays from 9:00am to 9:00pm, and it auto-exits people at 1:00pm, 5:00pm, and 9:00pm. *People who enter at the exact moment time changes to 1:00pm, 5:00pm, or 9:00pm may be immediately auto-exited by the system. The times for auto-exit should be realistic for each zone. So, if some people arrive at or about the time of the auto-exit, they should be assigned to a different zone with different or no auto-exit times.*

Automatic exits are shown in the log as `AEXIT` rather than `EXIT`. *Please note that attempted (but unauthorized) 'doorman' exits also show `AEXIT`.*

Note: The zone-based auto-exit check is made once a minute at the beginning of the minute. It is possible *but very unlikely* that if a person enters on the last minute of an `AUTO` zone entry, the system will immediately log them off. In nearly all cases, the person entering on the last minute of an `AUTO` zone entry will remain inside until a true exit or until the next `AUTO` zone match, whichever comes first. A manual auto-exit on the other hand, is performed immediately.

To disable the auto-exit feature without redefining any of the `AUTO` zone entries, give [and optionally `SAVE`] the `NOAUTO` command. The manual auto-exit *(giving `AUTO` followed by a specific zone number)* is always available, even when the auto-exit feature is disabled.

Now, to what zone do you assign yourself *(i.e., the boss, or security manager)*? Most likely, you and a select few others with equal authority within the company, organization, or even your home want unlimited access. Although one could define a zone with all days *(including holidays)* and hours enabled, and then assign himself to that zone, there is a better way. Assign yourself to the pseudo-zone 0 which can never be redefined, or deleted. A zero zone allows one to enter without any zone restrictions, whatsoever, even if no zones are defined at all. *Zero-zone users are the only people guaranteed to enter even if the clock is wrong due, perhaps, to a restart following a power failure combined with a dead clock backup battery, or if the `ZZR` mode is active.* This also saves a regular zone number (1-254) for other uses.

Note: If a ZeroZone person is restricted by the optional StartDate/EndDate, access is not guaranteed when the clock is lost.

Now, what good is the other special pseudo-zone 255? Well, that's for users one wants to keep registered in the system, but never give access to. "*Why would anyone want to do that?*" you may ask. Because one may want to be able to only track those people's attempts to enter but never really let them in. The system can track *(log)* unsuccessful attempts – with the command setting of `LOGALL` – for registered users only, not any random iButton ID someone may use. So, if one has a person with authorization for only one section of a building but not another, one can check if that person ever attempts to gain access to the non-authorized area. Another reason for using zone 255 is for keeping deleted or possible future users. One can not search the log for deleted users so, if there is enough spare user file space, changing users from any zone to zone 255 *(with the `MU` command[6])* effectively deletes them *for entry authorization* but since these users are still in the system their log shows correctly, instead of `*** RECORD DELETED ***`.

A description of the commands `ZZR` (*Zero Zone Required*) and its complement, `NOZZR` *(OEM default)*, follows.

With the `ZZR` command, one tells the system to allow people already restricted by zones 1 to 254 to enter based on their defined day-and-time schedules as usual, but considering the additional restriction that at least one zero-zone person is already in. *This restriction also applies to the zoned `ENTRY` and `EXIT` commands.* With this feature, the system administrator has the flexibility to let people in, or engage the automatic 'entry' and/or 'exit', only when at least one of the trusted *zero-zone* people is already in. Since **zero-zone people are** normally the owner, the security managers, or other **fully trusted** people, when none of these people are inside the controlled area, all others will have to remain outside, even if their zones would otherwise let them in. *For example, a storeowner may not want his employees entering the store if he himself hasn't arrived yet. The employees can still attempt access simply for recording show-up time for payroll purposes (must be in `LOGALL` mode to record the attempt).* The same reasoning applies to auto `ENTRY` and `EXIT` in `ZZR` mode, i.e., only if at least one of the zero-zone 'managers' is already logged-in, the 'garage barriers' will be automatically activated based on their defined schedule(s).

But what if one wants to keep everyone out when zero zone people aren't in yet, <u>except</u> for a select few non-zero-zone people? The cleaning lady, for example, one may want to allow entrance even when the boss is out; they usually do their job better prior to anyone coming in to work, or after everyone has left. But, we still do not want to make her zero zone because:

1. We want to assign her a day-of-week/time schedule *and zero zones don't have any*, and most importantly because…
2. If we were to make her zero-zone *when in `ZZR` mode*, her entry would automatically enable all others to enter, too *as if the boss just walked in*. We

[6] `MU` is available since v3.20. For previous versions, you need two commands (`DU` followed by `AU`) to change a user's zone.

only want to exempt her from the `ZZR` requirement, without any undesired side effects.

Fortunately, there is a way to do this. The *ZZR Check Above* level defines the zone level above which `ZZR` checks are performed. The OEM default value is 0, which means anyone assigned to a non-zero zone is subject to ZZR checking. If we set the *ZZR Check Above* level to, say, 1 *(with the command `ZZR 1`)* then only people assigned to zones above 1 (exclusive) will be subject to `ZZR` checking. Now, assigning the cleaning lady to zone 1 will make her zone restricted but not `ZZR` restricted.

WARNING: When the `ZZR` mode is enabled, non-zero zone checks *above the ZZR Level* may take significantly longer to complete; the actual time depends on the total number of zero-zone users, and the current size of the log file. The delay ranges from being unnoticeable to a minute or so for an almost full-system with hundreds of zero-zone people.

Therefore, to help minimize these possible delays when using the `ZZR` feature, try to restrict the number of zero-zone people to the absolute minimum needed, even if you don't intend on using the `ZZR` mode all the time. For those who are free from specific schedules but still may be subject to a possible future ZZR mode, create a zone where all days and times are enabled (e.g., `AZ 1 SMTWTFSH 0000 2359`) just like with zero-zone, and assign them to that zone instead of zone zero, so their status is not checked during `ZZR` mode authentication, making things faster *and safer*.

WARNING: When in `ZZR` mode, **it's crucial that ALL zero-zone people always exit** properly ***using their key***, even if non-zero-zone people *unfortunately* sometimes don't follow the rules (e.g., they may exit by manually opening the door, or along with a friend's legitimate exit *bypassing the system*, despite your warnings against it). Having said that, be careful whom you assign to zone zero, or they could jeopardize your whole security scheme when in `ZZR` mode.

Current versions include a speed optimization related to the `ZZR` mode, where this extra check occurs only under some conditions, specifically, following a reset, a zero-zone person's exit, or a `ZZR` command. As such, one should hardly ever notice any delays in entry authorization.

About Holidays

'Holidays' is simply a list of all dates *in `DDMM` format* of fixed (*non-moving*) holidays. Year is irrelevant because normal holidays repeat each year. For example, in most Western countries, January 1st and December 25th of every year are holidays. Each country, or territory may have additional holidays, such as national independence days, etc. Fixed holiday examples include USA's July 4th and Greece's March 25th and October 28th, etc.

Moving holidays, such as Easter day, can be added to the list each year, e.g., around the beginning of the year for the year ahead while removing the same holidays for the past year. A holiday is added with the command:

```
AH DDMM
```

where `DD` is the date, and `MM` is the month. For example, `AH 2512` defines Christmas day (December 25th) as a holiday.

Some companies are closed during a fixed period each year for summer vacation. In such cases, one would normally enter each of these dates as holidays, too. One may also use the holiday feature to block access to most people at once (i.e., all those lacking the holiday bit in their zones) for specific days (e.g., during office renovation works, unplanned closings due to emergency situations, etc).

Any user assigned to a zone where the holiday bit is not set is not allowed access on dates that are defined as holidays, regardless if the specific day happens to be in the allowed day list.

One can delete a holiday with the `DH` (Delete Holiday) command followed by the date in `DDMM` format as you entered it when adding the holiday. *Note: No check is made if adding the same holiday date multiple times, so other than unnecessarily filling up the holidays file, there is no problem. When deleting, however, all same dates are removed in a single command.*

One can store up to 256 holidays, *an insanely large number for holidays you may think.* This should accommodate practically anyone in any country. Because one may delete holidays *(e.g. when redefining moving holidays)* one may start running out of space (*as deleting any record does not free up space*). If running out of holiday space *because of deleted records*, use the `PACK` command to remove those deleted holiday records and make room for new ones.

About the passwords

The LogLock terminal can operate in locked `[!]`, normal `[>]`, or config `[#]` mode, indicated by the corresponding prompt symbol inside the square brackets. The current terminal mode does not affect the operation of the remaining system.

Locked mode has no functionality at all, providing the most privacy. Use the command `LOCK` to (re-) define the terminal lock password in the same way one does with the `PASS` password. One must be in `#` mode to change any passwords.

A `NOPASS` command from the `[>]` mode goes into locked mode *(indicated by the prompt `[!]`).* In locked mode, only the following harmless commands are available: `ANSI`, `CLS`, `DEVICE`, `INFO`, `REM`, `LOCK`, `PASS`, and `MASTER-RESET`. [`MASTER_RESET` is available in all modes in case one's locked out by lost/forgotten password(s).] Only the `INFO` command is shown in the associated help screen, however. Locked mode protects from casual browsing of settings, or the user and log lists by chance visitors (e.g., if the unit is accessible over the Internet).

Normal mode allows limited functionality, e.g., viewing the settings, log, and user database. To enter normal mode from config mode, issue the `NOPASS` command. To enter normal mode from locked mode, issue either the `LOCK` or `PASS` command giving the `LOCK` password. To enter config mode directly from locked mode, give the `PASS` password, instead. *If the two passwords are the same, then the first `PASS` command takes one to normal mode, and a second `PASS` command takes one to config mode.*

To add or delete users, zones, or holidays, or to change any of the system settings or passwords one must be in config mode. For security reasons, a user cannot add or delete from the database lest they change their own user rights. A user cannot change the clock, again for security reasons. Only in config mode *(# prompt)* one can perform any of these actions.

As it ships, LogLock has no passwords installed, so it starts up in config mode *(# prompt)* to allow initial programming. If the LogLock unit's terminal is accessible by anyone other than yourself, *or whoever the supervisor is,* locally or even over the Internet, it is strongly recommended that you protect it by assigning the config mode a password. It is also advised you assign a different `LOCK` password for even greater security. *Remember, config mode has commands that let one open the door directly (e.g., `REN` and `REX`) without even being on location or having a valid key. For this reason, besides assigning a password to config mode, one should always leave the system in normal (> prompt) or even better in locked mode (`!` prompt), when done viewing the log or making changes. For similar security reasons, it is also strongly advised to assign a password to the Ethernet Module via the DS Manager.*

Be sure to **remember the passwords** you define at all times, but never write them down or disclose them to anyone else to prevent 'leakage'. If you believe a password has been compromised, you must make sure to change it as soon as possible. The command to assign the first time password, or change it thereafter, is:

`PASS <password>` for the config mode password
or
`LOCK <password>` for the terminal access password

A `<password>` is up to 20 characters long, case sensitive, meaning that `'My Secret Password'` and `'My secret password'` are two different passwords, and can include any printable ASCII character *(letters, numbers, punctuation marks, single spaces, etc.)*.

If you don't want people around you to see your password as you type it, or if you want to enter character codes not possible to type – e.g. function keys, multiple spaces, etc., don't type the password on the command line. Instead, type `PASS` (or `LOCK` for the locked mode password) and press `[ENTER]`. This will show:

Enter password (it will not display):

Then, you can enter the password secretly. Each typed character will be shown as an asterisk (`*`) instead of the actual character you type. You can backspace to correct mistakes, if required.

To remove a password completely, one must use the second method *(secret entry)* and just press `[ENTER]` when asked for a password. This undefines the current password.

IMPORTANT: The password one defines *or undefines* will be saved during the next `SAVE` command, not immediately. If you have changed your mind and don't want to save the changes, issue either the `LOAD` command *(more immediate)* or the `RESET` command. This reloads the system ignoring any configuration changes made since the last `SAVE` command. *The `SAVE` command does not affect user, zone, or holiday changes, which are always saved immediately.*

Commands that are only accessible when a valid `PASS` password is entered *(i.e., in config mode)* are shown in the help screen (displayed when `?[ENTER]` is given at the command prompt) only from within the `#` mode. To exit config mode and return to normal mode, give the `NOPASS` command. To exit the normal mode, and go into locked mode, give the `NOPASS` command once more.

IMPORTANT: Make sure you do NOT forget either password. If one becomes locked out from the terminal console, the only way to reset the unit's passwords is by calling ASPiSYS Ltd. for instructions, and a special one-time code to remove all passwords. *Removing all power from the system and the built-in clock backup battery for any length of time does not cause it to forget the passwords.* Before contacting ASPiSYS Ltd. for a password reset procedure, one must be connected to their LogLock via a terminal. One may also be required to verify their identity before we give them the one-time unlock code. One can give the `INFO` command for contact information.

The DIR command

To check the current device status *(file sizes, settings, etc.)*, use the `DIR` command. The following is a sample display of the command. One's actual display may be different based on their own settings or version.

```
Filename Total Used+  Free
-------- ----- ----- -----
Users...   448    30   418
Log.....  5733     0  5733
Zones...  1020     5  1015
Holidays   256    12   244

Clock: Mon 2009-09-07 17:00:00 DST

Lang. Code Page : Win Greek
Alarm sec On/Off: 15/5 sec, Alarms=0, PASS attempts=0, Resets=0
Entry/Exit delay: 1.5/1.0 sec
Entry/Exit mode : AC (noisy, less current)/DC (quiet, more current)
Unit Location   : Outside
Separate Strikes: Yes
Zone bindings   : ENTRY=2, EXIT=1, PUSH-BUTTON=255 (Off)
ZZR Mode / Above: On [BLOCKED]/1
Sound/Hide IDs  : On/On
Log Mode        : All unique auto-exit
MCU Volts & Temp: 2.94V [25C | 77F]

From Date YYMMDD: Fri 2000-01-01 00:00
To Date   YYMMDD: Thu 2099-12-31 23:59
```

The DEVICE command

One may give their device a name or description. This is particularly useful if one has multiple units installed, and wants to quickly check which unit one's connected to.

Use the `DEVICE` command alone to display the current setting (if any). Follow the command with a string parameter to change the current setting to a new value. The string may be up to 60 characters long. *Longer strings are accepted but truncated to the first 60 characters.* This feature can be used to either assign a unique name to this device *(within one's organization)*, or simply to describe its location, ownership, or person in charge, etc.

Example strings are:

```
College, Math Dept.
My Company
Tom's House
```

Changing the name/description string is only possible in `#` mode. To remove the string completely, give just the character `?`. Viewing the device name/description can be done in any mode. If a device string is defined it is included in a `BACKUP` command. The string is raw, and it is not affected by the current language setting *(as with user names)*.

Adding / deleting users

Before gaining access, a user must be entered into the LogLock's database. This is done via the `AU` (Add User) command, whose format is shown below *as when one issues the command without any parameters*:

```
Use: AU ID(16) PIN(4) ZONE(3) [FROMDATE(6) [TODATE(6)]] "username(20)"
     Dates in YYMMDD format, e.g. 090117 = Jan 17, 2009
     Username: Lower=Greek, Upper=English
     ZONE 1-254, (0=Always, 255=Never)
     PIN="NONE"
```

The numbers in brackets indicate the expected, or maximum length for that element of the command. The username length may be different from the one displayed above depending on the specific version one owns. Square brackets embrace optional portions of the command.

DOS Greek (`GR`), Windows Greek (`GRW`) character codes or lower case English characters in the user name field are interpreted as Greek *when in Greek modes*, while uppercase are always interpreted as English (Latin alphabet). When in English mode (`EN`), one may use both upper- or lower-case names, but searching for them (`U`, `L`, `LL`, and `WHO` commands) is case-sensitive, so one must remember to type them the same way one entered them with the `AU` command.

The iButton ID is the unique code of the user's iButton key. Usually, it can be found engraved on the iButton key itself *but one doesn't need to memorize it, or write it down*. You can use the Monitor mode to quickly have the iButton number display on the terminal each time you touch it on either reader, regardless if it is already registered in the device. Alternatively (*for units equipped with an LCD*), one may hold it firmly on either key reader of the unit (depending on the *Unit Location* setting) for about 2 seconds until the key code displays on the LCD. The code will keep displaying until one removes the iButton from the reader. This code is always exactly 16 characters long, comprised of hexadecimal digits *(numbers from `0` thru `9`, and letters from `A` thru `F`).*

The iButton ID contains a checksum that indicates whether the number is correct or not. If any digit is wrong while typing the ID, the checksum fails and the command issues the message *parameter error(s).*

Special 'doorman' ID

There is one special ID one can use that does not correspond to any real iButton key. This ID is made of all zeros (`'0000000000000000'`) and it is an always defined system ID that is assigned to the hypothetical 'doorman' which is whoever presses the `REN` / `REX` buttons. *An actual doorman may have his/her own real key, regardless.*

Although the zero ID is always defined internally in the system, one may also define it in the actual user file.

If the zero ID is not defined in the user file, then the `REN` and `REX` commands *and their associated push-buttons (if connected)* work at all times without any restrictions. The log listing shows all Request-To-Enter and Request-To-Exit actions with a corresponding system name *without any quotes*, which isn’t searchable because it does not really exist in any file.

On the other hand, when the zero ID is actually defined in the user file *with the `AU` command*, it is *necessarily* assigned to some zone, and then it behaves like a regular user key, *except it is not actually possible to read it from the iButton readers*. In that case, the `REN` and `REX` commands obey the restrictions of the zero ID’s assigned zone. As is the normal behavior, a zero zone always allows use of these commands; zone 255 never allows use of these commands (*effectively disabling the commands and their associated push-buttons*), while all other zones behave according to their definition. So, this feature allows one to have `REN` and `REX` commands and push-buttons that are only functional for specific days and times. The name given to the zero ID user is displayed in the log listing instead of the generic system name. This name is now searchable just like any other user name.

The system must be in `LOGALL` mode for zero ID events to be recorded.

PINS ARE NOT SUPPORTED; THE FOLLOWING PARAGRAPH IS FOR COMPATIBILITY WITH PREVIOUS VERSIONS ONLY.

A PIN is made of exactly four decimal digits (`0` thru `9`). The special PIN codeword `NONE` (case-insensitive) is special in that the user is not required to enter a PIN regardless of the status of the PIN mode. Numeric PINs, on the other hand, are required verification when the system is set in PIN mode (do a `DIR` command to see current settings and modes).

A zone number is a decimal number of up to three digits. The number must be in the range `0` thru `255`, or else an error message is displayed. Remember that zones `0` and `255` are special and do not correspond to any user-defined zones. In short, zone `0` allows access at all times while zone `255` disallows all entry and exit accesses but keeps track of any such attempts in the log file (if in the `LOGALL` mode).

An optional *`StartDate`* and *`EndDate`* may be entered in `YYMMDD` format. To enter an *`EndDate`* one must also first enter a *`StartDate`*, although a *`StartDate`* does not necessarily require an *`EndDate`* to follow it. A *`StartDate`* enables the specified user’s access rights on that date. An *`EndDate`*, if defined, disables the specified user’s access rights at the end of that day. No access is allowed at all outside the provided date range. This feature is useful for temporary users with a starting and/or expiration date. To define just an expiration date, one is required to also provide a starting date, so just use any past date or today for starting date to be allowed to enter an expiration date.

The *`StartDate`* and/or *`EndDate`* may contain ‘wildcards’. This feature is 100% backwards compatible. Wildcards are entered as two dots (`..`) in place of the *`YY`*, *`MM`*, or

`DD` element of the `StartDate` or `EndDate` for the `AU` command. Wildcards effectively skip the check for that part of the date against the actual clock. Therefore, a wider selection of date ranges becomes possible. Examples using the wildcard dates are shown below:

```
AU FF00123456789A01 NONE 200 ....01 ....07 “Paper Supplier”
AZ 200 -M------ 0900 1300 AUTO
```

The above user is restricted to enter on dates between 1st and 7th of every month of every year. Because the user is further restricted by zone 200, which allows entry only on Mondays from 9:00am to 1:00pm, the user is able to enter only between those hours on the first Monday of every month of every year. *Instead of 01 to 07 which is for the 1st week, use a `DD` 08 to 14 for 2nd week, 15 to 21 for 3rd week, 22 to 28 for 4th week, and possibly 25 to 31 for last week.*

Another example: A seasonal worker in a hotel is needed for the months of May to September every year.

```
AU FF00123456789B01 NONE 201 ..05.. ..09.. “Pool cleaner”
AZ 201 –M-W-FSH 0700 1100 AUTO
```

A final example: A person is allowed only around Christmas day every year.

```
AU FF00123456789C01 NONE 202 ..1222 ..1228 “Santa Claus”
AZ 202 SMTWTFSH 2200 2359
AZ 202 SMTWTFSH 0000 0400 AUTO
```

With the current implementation, `YY` wildcard date ranges that span year changes (e.g., from December to January), or `MM` wildcard date ranges that span month changes (e.g., from 25th to 5th of next month) are not possible.

Finally, the user name is entered within double quotes (`“user name”`). Only the first 20 characters are significant (*Note: the number of significant characters may be different based on the particular version one owns*). *A null/empty name – two double quotes with nothing in between –adds and deletes the user immediately, so it is practically useless, except for testing purposes, e.g., to see the effects of a `PACK` command. To add an ID without any name use at least one space inside the double quotes for the name or a special codeword that you prefer, such as `“PRIVATE”`.*

One cannot add another user with the same iButton ID because each iButton is supposed to be given to exactly ONE user. No sharing of iButton IDs is allowed. The iButton ID can be considered the unique index of the ‘user table’ of the database. It is also strongly advised to not give a single person more than one iButton ID key. Since the same ID can be used with multiple units, there is absolutely no reason at all for people to use more than one key each, regardless of the number of access points.

Different users may share the same user name, however. The unique part of a user is the iButton ID, and only that. Nonetheless, it is recommended that users with the exact same name, be given slightly different names (an extra dot, or first-last and last-first versions of the same name, for example) to make it easier to differentiate the two in user or log listings without having to look at, or remember their iButton IDs. So, for example, if two people are named ‘John Doe’, one could be entered as `“John Doe”` and the other as `“Doe, John”`.

Since there is no *‘change user’* command, to change a user’s database record (for example, to change a user’s name), one must first delete it *if one plans on using the same iButton ID*, and then add it again using the new or modified information. To delete a user, use the `DU` (Delete User) command followed by the unique iButton ID for the user one wants to delete. *Hint: Use the `U` command followed by a name to locate the user, double-click on the ID to mark it, and then copy it (using `[CTRL-C]` in most terminal programs.) Next, give the `DU` command followed by a space and the pasted back ID (`[CTRL-V]` in most programs).*

<u>LogLock Mini only</u>

One can also quickly add or delete *‘temporary’* users by means of the small push-button *opposite the clock battery holder*.

Users added with the push-button are given the *‘mystic’* name `“?”` and assigned to the zone currently defined via the `PBZ` command (see `DIR` display). The optional start/end date will not be defined when PBZ is set to zero. For non-zero PBZ, the start date will be set to the current system clock date. This allows you to know when the ‘temporary’ user was added. If one makes the `PBZ` command point to zone `255` (OEM default) *which never allows entry*, the push-button feature is completely disabled either for adding or deleting; *no, it does not add users to zone 255.*

To use this feature for adding a user, first briefly touch the key you want to add on the outside/*primary* reader (when *Unit Location* is ‘Outside’), or the inside/*secondary* reader (when *Unit Location* is ‘Inside’). After removing the key from the reader, press the small push-button for at least one (1) second *but no more than four (4) seconds*. This will add the specific iButton key and give it the username `“?”`. *If the key already exists, it is not added a second time, nor moved to the `PBZ` zone.*

To delete all users assigned to the current `PBZ` zone, press the small push-button and keep it pressed for at least five (5) seconds. *Users assigned to all other zones will not be affected at all.*

This feature is useful for quickly adding or deleting *temporary* users, without using any PC connection and without affecting any of the *permanent* users. The rights these users have are the current rights of whatever `PBZ` zone was active at the time the user was added. In other words, the zone that was assigned to a user at the time the button was pressed remains constant even if the `PBZ` zone is later changed to another.

About the Log

The log keeps track of all user entries and exits. The log keeps the exact date and time of each successful or attempted entry or exit. By default, unsuccessful attempts *(e.g., attempting to enter outside the user's zone limits)* are not recorded to save log space for successful attempts. If you need to record both successful and unsuccessful attempts from registered users *(e.g., those attempting to enter outside their zone restrictions)*, use the `LOGALL` command to set the system in 'log all attempts' mode.

If you want to revert to keeping a log only for successful attempts, use the `NOLOGALL` command.

One can also save significant log space by using the `LOGUNIQ` command. The OEM default (`LOGSAME` command) records all actions even when the same action is quickly repeated many times within the same clock minute *for some cases indicating a possible pass back attempt*. Normally, a user may attempt multiple successive entries because s/he does not realize s/he attempting entry outside the user zone's allowed day-of-week/time combinations, and falsely assumes there is some misread of the iButton ID key, or some other temporary problem, that won't allow access. S/he will eventually give up, after having filled the log with a bunch of unsuccessful attempts *in `LOGALL` mode*. In the OEM default mode, every single attempt is recorded and in situations as the one described, there could be tens of them. With the `LOGUNIQ` command, however, only different actions are logged. It is sufficient for the clock minute alone to advance for the action to be considered different. So, one won't see more than at most a single attempt for each minute of the hour *unless another user enters or exits in between*.

If you need to record unsuccessful attempts from non-registered iButton IDs, use a terminal program with a screen capture capability, and leave LogLock into Monitor mode (M command) during times you want to collect this information. This will record all attempts to enter or exit, even for iButton IDs that aren't part of the system. The ID along with the words `ENTER`, `EXIT`, or `-----` is displayed, depending on whether the attempt was an entry, exit, or unsuccessful entry, respectively.

IMPORTANT NOTE: If one leaves the unit in Monitor mode and the network connection is either intentionally terminated or lost, or if while in Monitor mode you pause `[CTRL-S]` the terminal output, the unit may stop responding to further iButton keys (for up to 10 seconds, until the system auto-detects this situation and unblocks the blocked reader).

This is because in Monitor mode, the device must first output the collected information from the last key read before accepting another key, and if the connection is either closed/lost or paused that output is suspended until the connection is re-established or the listing is continued `[CTRL-Q]`.

It is best if one does not leave the unit in Monitor mode, when unattended. However, as a safeguard against being left in Monitor mode by oversight (or malice), please note there is a maximum time limit of up to one day (1440 minutes) for the `M` command, available only from the config mode, while the default value if no time is specified, or if issued from normal (non-config) mode is only 1 minute.

The log for a specific user can be displayed using the `L` and `LL` commands followed by a [partial] user name, but without the quotes used when creating a user. This is useful for viewing a specific user's 'in' times for a given period, say, a month. Alternatively, using a terminal's screen capture feature, one can download the complete *or within a date range* log to their computer for automatic time calculations on the PC. Additional software is needed for this task. We may be able to supply you with such software for PC based computers on an as-needed basis at extra cost. If there is a programmer in-house, they can easily write a small program to extract this information from the captured log file, and calculate total times as required by one's organization. *We can provide pre-written scripts to setup a database (such as MySQL or SQLite), and keep it updated by 'manually' or 'as scheduled task' running a couple of scripts, or so. Then, one can get summarized information for each and every user, one at a time or all together.*

Except for not displaying the username, the `LL` command is identical to the `L` command. This results in faster overall downloads of large log files.

Although the log space is rather large *(5733 records in the OEM default version)*, eventually it will become full (but not stop logging newer actions). If you're interested in keeping accurate log history for periods longer than can fit inside the device's internal memory, it is expected you retrieve the log well before it becomes full *(e.g., at the end of year, end of month, end of week, end of day, etc. depending on usage – number of users, and number of entries/exits per user per day on average)*, and then optionally clear the log completely *with the `CLEARLOG` command*.

***Hint:** To avoid the possibility of losing any actions during the short interval between the completion of the log transfer and the issuing of the `CLEARLOG` command, one can opt to not ever clear the log manually; rather, let it auto-truncate the oldest 39 actions when full, and use the Date Range (`D` command, see below) to retrieve only newer log entries. If you retrieve the new log from a specific date and time combination you will get only a minimum amount of overlaps with existing log entries from the previous log retrieval (in case you're pulling the log more than once per given period), or no overlaps if retrieving between fixed past periods (e.g., every day for the previous day up to 23:59 – last minute of day).*

Note: A database (such as MySQL or SQLite) can be indexed such that it will not allow duplicate entries in its tables. (An index based on the iButton ID, date, time, and direction is sufficiently unique. A pre-configured MySQL database script may be available on demand.)

On attempting to log an action when the log is full, the device automatically first erases a log page (i.e., 39 records) of the oldest log information to make room for the newer information. So, at any given time *unless one specifically clears the log with the `CLEARLOG` command*, the log holds at least the 5695 *(depending on version)* most recent user entries and/or exits.

To define a date range for the `L` (Log) or `LL` commands, use the `D` (Date range set) command. Pressing `D[ENTER]` shows this:

```
No Date Range, use: D YYMMDD[hhmm] [YYMMDD[hhmm]] (*=today)
```

and cancel any previous date range setting. To set the date range from Aug. 13 to Aug. 29, 2004 *(Athens 2004 Olympic Games)*, use this command:

```
D 040813 040829
```

When `[ENTER]` is pressed, the system responds with:

```
From Date YYMMDD: Fri 2004-08-13 00:00
To Date   YYMMDD: Sun 2004-08-29 23:59
```

Dates are entered in `YYMMDD` format and must be exactly 6 digits long, or entered in `YYMMDDhhmm` format and be exactly 10 digits long. If choosing the `YYMMDD` format, then the time is automatically set to the beginning of the day for the `FROM` date and to the end of the day for the `TO` date. The first date is the `FROM` date while the second date is the `TO` date. Then, the log displayed with the `L` or `LL` commands is limited to accesses during this period *(inclusive)*. One can also use the command with only a `FROM`, or only a `TO` date.

To set only a `FROM` date (to see log entries `FROM` that date onward), give only the first parameter to the command. For example,

```
D 040813
```

limits log viewing from Aug. 13, 2004 and later *(to any date)*. After pressing `[ENTER]` the system responds with:

```
From Date YYMMDD: Fri 2004-08-13 00:00
To Date   YYMMDD: Thu 2099-12-31 23:59
```

(Notice how the `TO` date is automatically set to the latest date and time possible, i.e., Dec. 31, 2099 11:59pm)

To set only the `TO` date (to see log entries from any date `TO` a specific date), give any invalid date for the `FROM` date followed by a valid `TO` date. For example,

```
D x 0408291700
```

limits log viewing from any date to Aug. 29, 2004 at 5pm *(inclusive)*. The ‘x’ acts as a ‘don’t care’ indicator. Any date that isn’t made up of valid numbers and/or doesn’t contain exactly 6 or 10 digits is invalid and, therefore, considered a ‘don’t care’ date. After pressing `[ENTER]` the system responds with:

```
From Date YYMMDD: Sat 2000-01-01 00:00
To Date   YYMMDD: Sun 2004-08-29 17:00
```

(Notice how the `FROM` date in this case is automatically set to the earliest date and time possible, i.e., Jan. 1, 2000 12:00am)

To quickly set either date to today *(based on the current clock setting)*, use a single `*` character for date (`From` and/or `To`), e.g.

```
D *
D * *
```

> **NOTE:** The system only understands dates for the years 2000 to 2099. Since the first date is already past while the second one is beyond the expected life of this device, it is a non-issue for actual use. Anywhere one is expected to enter a year, one must omit the leading 20 because the system expects all dates to be in the above range.

One can see the currently effective date range by issuing the `DIR` command. The date range remains in effect until one changes it or the system is reset.

Any log viewing commands are always restricted to within the effective date range. Even if one searches for a user name in the log (with the command `'L` *`username`*`'` or `'LL` *`username`*`'`), only those accesses that fall within the effective date range are shown.

Since the date range auto-calculates and displays the day-of-week for the given date(s), one could use this function to check on what day-of-week a specific date falls.

IMPORTANT: Don't forget to reset the date range before taking a complete log backup *or set the date range for an incremental log backup* (e.g., to use with a PC application). Press `D[ENTER]` to reset the date range to the default values of 2000/01/01 00:00 to 2099/12/31 23:59. Then, press `L` or `LL[ENTER]` to get the complete log.

Finding out who's 'in'

LogLock gives one the ability to know who's *supposedly* 'in' by checking the log for those who have registered an entry without a following exit. For accurate results, it is assumed that users have entered within the same log period (i.e., within the last 5695 transactions – *actual number depends on version*). Otherwise, there is a possibility the log gets truncated to make room for newer entries, losing the information for the oldest entries. *Under normal usage, this is highly unlikely to occur as even with a totally full user database (448 people for the default version), each and every user has to go in or out over 12 times on the same day for the log to become full and risk losing older entries.*

The `who` command examines each user's log activity. Any user who has entered but not yet exited is considered to be 'in'. Obviously, this will not be correct if people are allowed to exit bypassing LogLock (e.g., by manually opening a door, or exiting along with another person's legitimate exit, without using their own key).

Just like the `U, L, LAST,` and `LL` commands, the `WHO` command may be followed by a partial user name to limit the search to only those users whose name includes the one given.

Similarly to `WHO`, the `LAST` command allows to view the last (most recent) action of any user. Again, only actions currently in the log are considered. This command helps to quickly find when was the last time someone accessed the system for either entry or exit.

Setting the clock

To set the real-time clock of the device one must use the `C` (Clock) command. The `C` command expects the date and time in the `YYMMDDhhmmss` format (note that seconds must be given also – if one doesn't care for such accuracy the value 30 for seconds is the best guess). For security reasons, only in config mode (`#` prompt) one can change the date and time.

As an example, to set the date and time to '5:30:45pm August 15, 2004', give the command:

```
C 040815173045[ENTER]
```

One will not be allowed to enter incorrect date/time codes. The day of week does NOT need to be entered, as the unit is capable of automatically calculating it from the date.

Daylight Saving Time (DST) is automatically detected based on EU's rules for changes of time twice a year (last Sunday in October from DST to Normal, and last Sunday in March from Normal to DST, at 3:00am). When setting the time the unit automatically goes into DST or normal mode depending on the date entered (on a switch date itself, the new mode is set, regardless of time). Thereafter, the clock keeps track of the correct time even during time changes from Normal to DST or back. This makes it very convenient for the day(s) after a time change when people show up to enter based on the changed time.

The clock is protected from power failures via a small long-life lithium battery (type **CR2032** or **CR2025**) that keeps the clock running for several days of continuous power loss. If, however, the unit is left unpowered for longer periods of time, the clock battery will eventually run out and will then require replacement. The device is not serviceable by the casual user.

Please note that even with a totally drained clock battery, the unit is still usable but unless its power-supply is protected by a UPS (Uninterruptible Power Supply) system, it loses its date and time information every time there is a blackout (or even a brownout on occasion), and it must have its clock manually reset to exit the startup error condition (see box below).

IMPORTANT: When losing the date/time due to a clock battery failure, the unit reverts to midnight of January 1st of the firmware's Build year, certainly a past date, and the status LED *(for LogLock Mini)* will blink rapidly – normally, the LED blinks every 3 seconds. The `DIR` display will show the message `[INVALID]` next to the time. In this error condition, only zero zone people (including `REN/REX` events) are allowed access, since date/time cannot be trusted for zoned access. Any actions *(which in this error condition can only be accepted from 'ZeroZones')* are not logged because the date/time is known to be invalid, and logging such actions/attempts would disrupt the normal chronological sequence in the log file. Setting the clock with any date/time *(past 2008)* clears the error condition, and normal operation resumes.

Changing the LCD and username-in-listings language

LogLock is partly bilingual. For units equipped with an LCD, it shows messages on the LCD in either English or Greek. Other languages may be added (instead of Greek) in the future, if sufficient demand warrants it. Also, the user names are shown on the connected terminal in the selected language.

The device's terminal interface is always in the English language. This is because Greek or other non-Latin-alphabet languages don't use a standard character-display coding scheme among different computers (e.g., PCs, Macs, UNIX, etc.) or different countries, and the Greek or other language fonts aren't default in most systems that support these languages. This would make it very difficult to use the device if the language was set to Greek and the connected terminal didn't show it correctly.

The LCD display the user sees can be switched from English to Greek, or back. To switch to English, give the `EN` command. To switch to Greek for DOS, give the `GR` command. To switch to Greek for Windows, give the `GRW` command. *`GR` and `GRW` are only different at the terminal display, not the LCD.*

The current language setting can be seen from the `DIR` command display, and it controls all messages on the LCD, including the date and time, except for the user names.

User names on the LCD are always displayed in uppercase when Greek is selected, and mixed case when English is selected. On the terminal, however:

- If the language is English, user names are displayed exactly as entered with the `AU` command.
- If the language is Greek (for DOS), user names are displayed in uppercase Greek for DOS code page for Greek and uppercase English for English names. *Greek for Windows works like Greek for DOS except the terminal code page is different.*

Packing or 'Garbage Collection' (Technical Note – not needed for operation)

The non-volatile memory used by LogLock for keeping settings, zone, holiday, user, and log information is writable in a special way that does not allow erasing small amounts of information at a time. Erasures must be done in sizeable chunks. Also, this memory is guaranteed by its manufacturer to at least 100.000 write-erase cycles which is truly a lot but not infinite. In practice, this translates to well over 550 million accesses, which even with the heaviest possible business usage imaginable *(one access per user, per 10-minute period, per 24-hour work day)*, it is over four decades! It is theoretically possible, however, that the memory will eventually go bad for writing data to it, and it will need replacement. Special programming techniques have been utilized to extend this writing period for as long as possible, so that you can enjoy many years of service-free operation. *For most installations, this limitation is a non-issue.*

When deleting users, zones, or holidays, the unit doesn't actually delete these; it simply marks them for deletion *(yet, this is an action that cannot be revoked)*. This means that the space taken by the deleted records doesn't become available automatically. To truly remove any deleted records from memory, one must use the `PACK` command. This command skips over all records marked as deleted while copying the rest. This procedure is called 'garbage collection'. If running out of memory space (as reported by the `DIR` command's FREE column), one can use the `PACK` command to regain any blocked unused memory. Please try not to use the `PACK` command casually (for example, each time one deletes a single user, zone, or holiday).

When changing passwords or options *(such as the open-door strike time)*, the device keeps these changes in a temporary memory rather than save them immediately. This allows making these changes more than once *for testing a behavior* before committing them to memory. To make these changes 'permanent' one must use the `SAVE` command.

Because of the write-erase cycle life of the memory, it's recommended one use the `PACK` command only when truly necessary. In other words, it's not required to type the command each time one deletes a single user or zone. Give the `SAVE` command only when you must change any of the `DIR` settings or passwords, or the `PACK` command when there is no space remaining in any of the files, and you need to add data to them, or if you have a significant number of accumulated deleted records (*cleaning up the files may improve overall performance*). This helps prolong your unit's life to the maximum. (The `FROM` and `TO` search date range are never written to this special memory, so a `SAVE` or `PACK` command is never needed for accepting changes.)

Using LogLock for entry or exit

The system comes with two iButton ID readers, one for each side of the protected area. The unit is always placed on the inside with one reader placed on each side of the access point. This provides full protection from vandalism (i.e., zero hands-on access to the system from outsiders). The commands `IN` and `OUT` tell the system whether to use the LCD for displaying exits or entries, accordingly. The device firmware then knows how to behave correctly for each case.

If a Request-To-Enter or a Request-To-Exit push-button is connected, pressing the button momentarily opens the corresponding door using the defined Door Time setting. No action is logged, unless in `LOGALL` mode. This push-button is normally used by secretaries or other human operators letting visitors in or out. Visitors normally do not have their own keys and depend on someone else to open the door for them. In a more secured installation where all ‘visitors’ must be pre-validated, the Request-To-Enter and Request-To-Exit buttons may have to be left unconnected to prevent the possibility of any user entering or exiting without the use of their iButton ID (especially if the `REN` or `REX` button is placed too close to the access point, and not controlled by a security guard).

Dual strike mode

LogLock can be set to use separate strikes for entry and exit. This is useful for situations where a different path is taken for each action (e.g., garages with separate lanes for entry and exit).

The primary strike (**`LOCK1`** or **`LC1`** in the connection diagram) is used for both entry and exit, if the device is set for single strike mode (with the command `S1`).

When set in split (dual) strike mode (with the command `S2`), entries always activate the **`LOCK1`** strike, while exits always activate the **`LOCK2`** or **`LC2`** strike, regardless if the unit is set to be inside (`IN` command) or outside (`OUT` command).

The `ENTRY` command can be used to open the entry door (or garage barrier) connected at **`LOCK1`** while the `EXIT` command can be used to open the exit door (or garage barrier) connected at **`LOCK2`**, and keep it open continuously *(e.g., during rush hours one may want to raise the garage barriers for efficiency).* The iButton keys can still be used to register the requested access for time attendance purposes, but the strikes do not close after the defined timeout (`DT` command). To cancel either command, use the `NOENTRY` and `NOEXIT` commands, respectively.

If the rush hours are foreseeable and follow a specific day / time pattern, one could define a zone for them for automatic use. A zone number may follow the commands `ENTRY` and `EXIT`. If the zone number given is `255` (the OEM default), the commands are disabled. If the zone number is `0` then the original behavior of indefinite engagement is enabled. When supplying a zone number to either of these commands, the zone is set but the command may appear to not be activated immediately *(depending on the situation, if zones are to be respected).* If one gives a zone from `1` to `254`, and that zone is defined, the strike is activated on the days and times dictated by the zone, and de-activated during days and times the zone won't allow. This is very flexible in that one may have the strike(s) automatically engage during, say, business days and specific 'rush hours'. Since a different zone may be used for entry and exit, you can allow for different 'rush hours' for entry and exit.

REN and REX commands

The `REN` and `REX` commands behave exactly as if someone presses the `REN` or `REX` buttons connected to the corresponding connectors on the diagram. *When used with split strike mode,* `REX` *always applies to the exit strike.*

Battery-Low warning

If connected appropriately, LogLock can warn you when the external supply battery (e.g., UPS battery) is running low and needs replacement or other maintenance (e.g., charging). LogLock Mini shows the optional rechargeable battery's status, instead. The warning appears with the `DIR` command and, for LCD-equipped units, on the LCD in the selected language along with the date and time displays.

LogLock Mini Only: Use of an optional 9V rechargeable battery

WARNING: First and foremost, do NOT use any type of non-rechargeable battery, or there is risk of serious damage, battery explosion, and personal injury. If you connect one by mistake, disconnect it right away, as the dangers we warn about may not become apparent until some time later. When connecting the battery please observe the polarity.

LogLock Mini is capable of temporarily operating off an optional 9V rechargeable battery. We strongly recommend the use of 8.4V (rather than 7.xV) rated batteries from any reliable manufacturer. The mAh rating is up to you but, obviously, the higher the number the better the performance you get.

Do not confuse the use of this battery with the CR2032/CR2025 clock backup battery, the two are not related. The clock battery is meant to keep just the real time clock running when there is no other source of power, and the device is non-operational.

On the other hand, when the mains power is lost or disconnected, the optional 9V battery kicks in and keeps the system running for doing its primary job, access control and/or time attendance. It acts almost like a tiny UPS. The system will be able to strike the door for several times, so you won't get stuck outside waiting for the power to come back on. *On a full charge you will get several tens of strikes – the actual number depends on several factors, such as the* `DT` *strike duration setting, the strike mode (*`AC` *or* `DC`*), the strike type used, etc.*

The system keeps this battery fully charged at all times when the mains power is normal. Charging is slow and may take many hours to reach full charge. But you should not worry about it. Under normal circumstances, the main power failures are few and far between giving enough time to the battery to recharge and be ready for the next one. *Unlike with some general-purpose chargers, there is no risk of overcharge. The battery remains in stand-by for when it's needed.*

To save power for the primary job of the device (*access control*), other functions have to be shut down when the system runs off the 9V battery. Therefore, the Ethernet module as well as the LCD (if connected) will be powered down. When the mains power returns to normal, the Ethernet module (and LCD) will be re-initialized. If a telnet connection was active before the power failure, it must be re-established.

Charging is fully automatic. There are no options or settings to adjust. Whenever a battery is installed, it is under the control of the built-in charger. You can see the `DIR` display to check the battery status and charging state. If the battery fails to charge for very long (*while charging the voltage remains constant and far below normal*), it may be time to replace it with a new one.

Mass-erase actions

Some commands are meant to completely erase single files, or all files. All delete commands (e.g., `DU` for delete user) can optionally be followed by the word `ALL` to delete all records in that file with a single command. A verification of the action is required to prevent mistakes. If you are certain you want to proceed with the action, enter `Y` (for *Yes*). The command for erasing all log entries is `CLEARLOG` while the command for erasing all files *(including the log, but not the system settings, or passwords)* in a single step is `CLEARALLFILES`. All these actions can only be performed in `PASS` mode.

Contact information

The command `INFO` displays our company’s contact information (address, phone numbers, etc.). Use it whenever you need to contact us. This information should be up to date according to the purchase date (or latest firmware upgrade, if applicable) of your unit. Should you require a firmware upgrade (e.g., to take advantage of added features in later versions), please contact us. Firmware upgrades (command `UPGRADE`) consist of loading an ASCII file via a telnet connection (e.g., HyperTerm – recommended because of its ‘File Send’ capability), and unless the update is performed to fix a possible remaining bug in the system, it may be not free (at our discretion).

Firmware Upgrade

By ‘firmware’ we refer only to the *application firmware* of the device, which is user upgradeable, and which runs on top of another fixed ROM (Read Only Memory) firmware which contains a BIOS, our OS8 real-time multitasking operating system, and upgrade related functions.

From time to time, we may provide free firmware upgrades. We highly recommend you update your device(s) as soon as possible to take advantage of improvements, or added features.

The ROM portion is not upgradeable by the end user. A ROM upgrade is normally not required, as we provide various firmware versions to match your specific ROM BIOS version. Nevertheless, earlier ROM versions may be upgraded to the latest version at no cost (other than possible round-trip shipping charges) by returning the unit to us.

Note1: BIOS bOS8 v1.70+ will not allow sibling product firmware use. Only a compatible BIOS (bOS8) version and LogLock model firmware image can be used.

Note2: BIOS versions which differ only in the final digit can accept the same firmware image as the base version. For example, for all BIOS bOS8 v1.7x devices, you must select the BIOS v1.70 firmware version, regardless of the actual value of x in your device.

Note3: After upgrading to a new firmware version, issue the `CLEAR` *command to zero all counters, as the values shown may be random.*

Begin by downloading the correct firmware for your device from our website: http://www.aspisys.com/firmware/ adding the appropriate filename as described below. *Note: All filenames are case-sensitive. Please observe the correct case when typing. Specifically, the word BIOS is uppercase, everything else is lowercase.*

To locate the correct firmware file for your device, please follow these instructions:

1. Identify the type of device you own (`INFO` command), e.g., *LogLock 3000* or *LogLock Mini*.
2. Identify the BIOS version you have (`INFO` command). *You can also ‘guess’ the version by looking at the Revision History, if you know the purchase date.* If a BIOS version isn’t shown, your BIOS version is v1.0
3. Download the correct firmware from **http://www.aspisys.com/firmware/** by adding the filename `loglock_`***`MODEL`***`_firmware_`***`NNN`***`_[BIOSv`***`?_?`***`].s` replacing ***`MODEL`*** with your unit’s model (e.g. ‘3000’ for LogLock 3000, ‘mini’ for LogLock Mini, etc.), ***`NNN`*** with the 3-digit firmware version (e.g., for v3.41 NNN should be 341), and finally ***`?_?`*** with the BIOS version (e.g., for BIOS v1.4x, use 1_4). They’re no spaces in the link, only underscores. As an example, for the 3.41 Mini version for BIOS v1.40, the correct firmware is: `http://aspisys.com/firmware/loglock_mini_firmware_341_BIOSv1_4.s`

Please see the revision history section later on for details on version changes.

WARNING: Sending the wrong firmware file to your device may make it completely inoperable as an access control system until the correct firmware file is loaded. Some firmware versions are closely related, and although they may appear to work even when loaded into a different system from the one for which they were intended, correct operation should not be assumed under all situations.

Updating is both simple and fast; *it normally takes less than one minute to complete.* It can be done over the network from anywhere you have allowed access to your device, even over the Internet[7], if you have set up your router to allow access to your LogLock from the outside. Of course, you need to know the `PASS` password to enter `#` mode before commencing.

If you happen to encounter undocumented incompatibility issues or other problems with a newer firmware, please let us know immediately. In such cases, you may re-load an older firmware version until a newer version is provided.

If unsure, please issue the `INFO` command to see the current version of your system. If the latest version of this manual (http://www.aspisys.com/loglock_mini.pdf) refers to a later version than the one you have, please contact us to obtain the latest firmware file. *If you have purchased the system directly from us, you may receive email notifications for possible upgrades as they become available.*

To send a firmware file to the device, follow these steps:

1. Make sure you have the required firmware file readily available before continuing.
2. Connect to your device using HyperTerm or similar application.
3. If upgrading to the same user/log ratio version, the data files are not affected. But to be safe against possible user errors, it's advised to make a backup of the device configuration, at this point. Following a firmware upgrade, all device settings *(including the passwords)* are restored to their OEM default. Make a backup with the `BACKUP` command, if you want to make it easier to restore the previous settings.
4. Initiate the firmware upgrade procedure by issuing the `UPGRADE` command from the # (config) mode.
5. Answer `'Y'` to the confirmation prompt. ***WARNING: This action is not reversible. Once you press 'Y' the old firmware is erased. (Press [ESC] to cancel, if you changed your mind. The system will restart.)***

[7] IMPORTANT NOTE: Access over the Internet should be very carefully considered. When typing your password, it's possible for anyone *with the necessary skills* between you and your LogLock device to intercept your communication and copy your password. Then they may be able to gain access to your system (specially if the system has a static IP address). For this reason, we strongly advise against entering # mode over the Internet, but only do so from your local network for which it is assumed you have administrator control and feel confident about how it is used. If you don't understand the risks involved, please do not make your LogLock accessible from outside your local network. *If you have doubts even about your own local network, use a direct connection from your PC to your LogLock using a cross UTP patch cable.*

6. Using HyperTerm *(or similar application)*, send the firmware file to the device using the 'Send Text File' *(or similar)* option. While the file is being transferred, a series of dots appears. If there are any errors, the dot(s) are replaced with special character(s) indicating the type of error that occurred. If all goes well, the dots will terminate with an exclamation point (!) and the message `'Loaded'`. The system will auto-restart with the new firmware.
7. Re-establish the telnet connection that was lost due to the previous restart.
8. If you had made a backup before the upgrade, send the backup file to the device to restore it to its previous configuration state. *If loading an earlier firmware, you may encounter compatibility issues trying to send the backup file to the device. Newer versions are backwards compatible, so sending a backup file created from a previous firmware should be recognized without problems (unless specifically noted otherwise).*

If the upgrade procedure fails for whatever reason *(e.g., power-failure half-way during the process)*, the system will re-start to the bOS8 monitor application and a slightly different procedure is required to load the new firmware. If when the device starts, instead of the usual welcome screen you see the bOS8 welcome screen, then follow these instructions:

- Give the `LOAD` command
- Answer `'Y'` to the prompt, if asked.
- Go to Step 6 of the normal upgrade procedure.

Under some rare conditions, and following an incomplete firmware upgrade, it is still possible that this second method can't be used. There is still a third method to recover. This is slightly more involved as it requires a few extra steps of changing a specific DS Manager parameter, and detailed instructions will be provided on an as-needed basis.

About the Alarm feature

The alarm feature is not meant to replace a regular alarm system, as it currently does not have all the needed features normally found in such systems. Its purpose is somewhat different; it is there to help notice when people enter or exit without using their keys, or if someone left the door open after using it. As an example, it can alert an office security guard or doorman that someone is trying to enter or exit without the correct procedure *(using their key)*, or that the door was left open after last being use. With an active alarm the guard does not need to have his/her full attention at the door, but only when the alarm sounds.

An external alarm device *(either the actual siren/buzzer, or an input to the controller of a separate dedicated alarm system)* and a door-left-open detection switch must be connected at the corresponding pins for this feature to work.

When the alarm feature is enabled *(i.e., `ALARM` On delay not zero)*, the alarm sounds either immediately if the door is opened without a key, or after the specified delay if using a key. The alarm delay starts counting from the moment the door strike is activated, not from the time the door strike is again deactivated at the end of the `DT` time. In other words, it runs concurrently with the `DT` time. If the alarm timeout is set to anything less than the `DT` time *(and provided the door is still open)*, the alarm will start before the strike stops.

While the alarm is active *(i.e., sounding)*, the `DIR` screen shows the message `[ACTIVE]` next to the alarm time setting. This allows you to know from a distance if there is currently an alarm event.

The alarm stops as soon as the door closes, or a valid key is used for entry or exit, or a `REN/REX` command is issued. To stop the alarm event *for the specified alarm time*, the key must be both registered in the system and allowed for the specific time zone. In other words, it must able to open the door at that specific moment in time. An Off delay is possible with the `ALARM` command. The Off delay is zero by default *(for compatibility with previous versions)*. If the Off delay is non-zero, the alarm will not stop until after this much time has elapsed from the moment the alarm condition stopped, *e.g., by closing the door*. So, a quick open/close of the door *without using a key* sounds the alarm for at least that many seconds. You can stop the alarm by presenting a valid key or issuing a `REN/REX` command *(an easy way to temporarily suspend the alarm)*.

A single alarm is used both for entry and exit *(in case you are using the `S2` mode)* and all door-left-open detection switches must be connected in series.

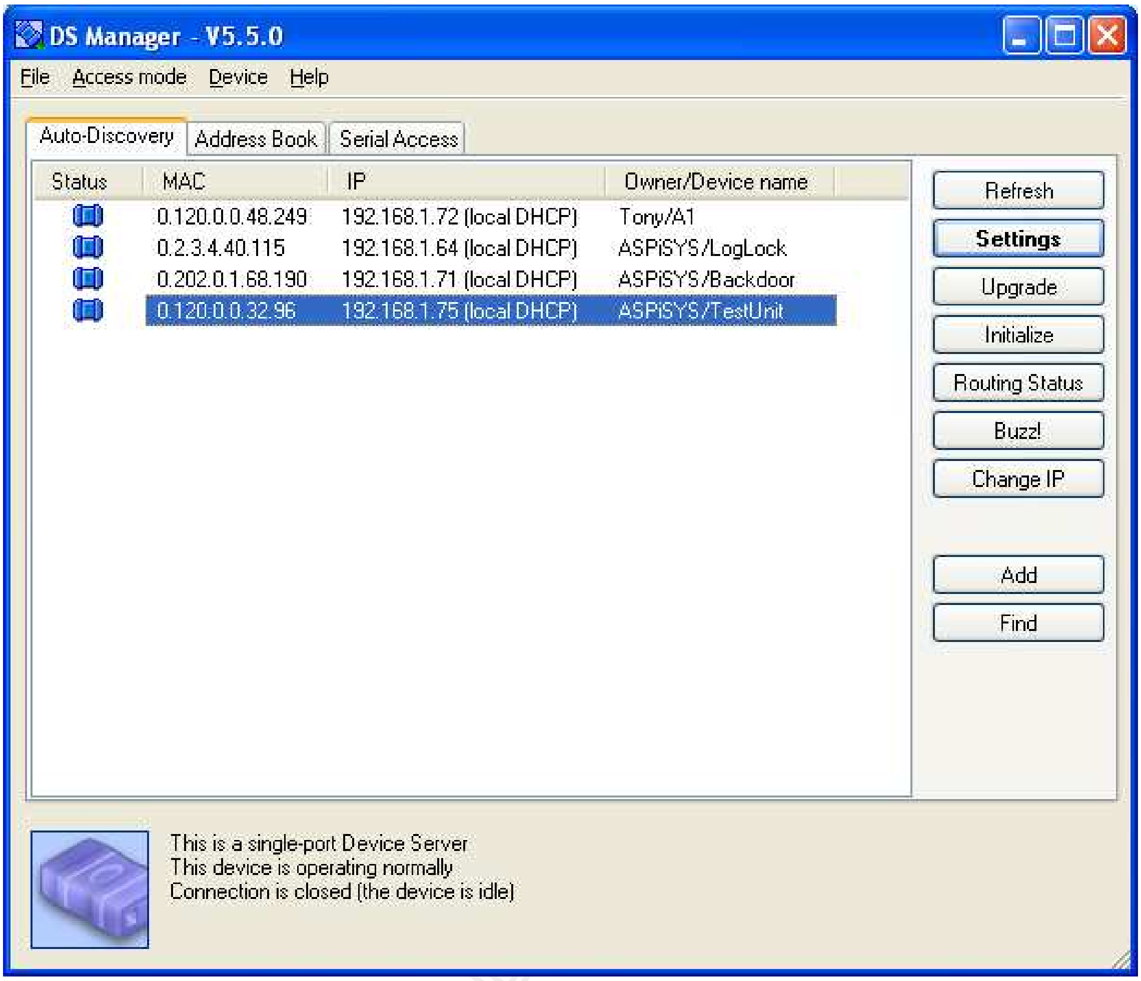
The alarm is not active during manual or automatic `ENTRY` and/or `EXIT` commands *(unless the Off delay from a previous alarm has not run out yet)*, or during `REN/REX` commands *(which cancel any active alarm immediately)*. *For the LogLock Mini version, the RX pin is used for the door switch, and the TX pin is used for the alarm signal. These are located on a separate header. An appropriate driver must be used on the TX pin to drive the external alarm or relay.* ***WARNING: Do NOT connect the TX***

***pin directly, or you will cause irreparable damage to the device.** Both the door-left-open switch (RX) and alarm (TX) pins are active high.*

IMPORTANT: ONLY a qualified person (someone experienced in bare electronic PCB handling) must perform the installation of LogLock. Do not attempt installation yourself unless you know what you are doing, or else there is increased probability of damage to the device due to wrong connections.

Custom units may have different installation requirements. Select the location on the wall or door casing you want to install the readers. It must be somewhere near the door, and at a height such that all users can easily access without having to either stand on their toe tips or bend down. The unit can be placed anywhere inside the protected area, at a distance not exceeding 100m (using UTP CAT5 cable) or shorter (plain twisted pair.)

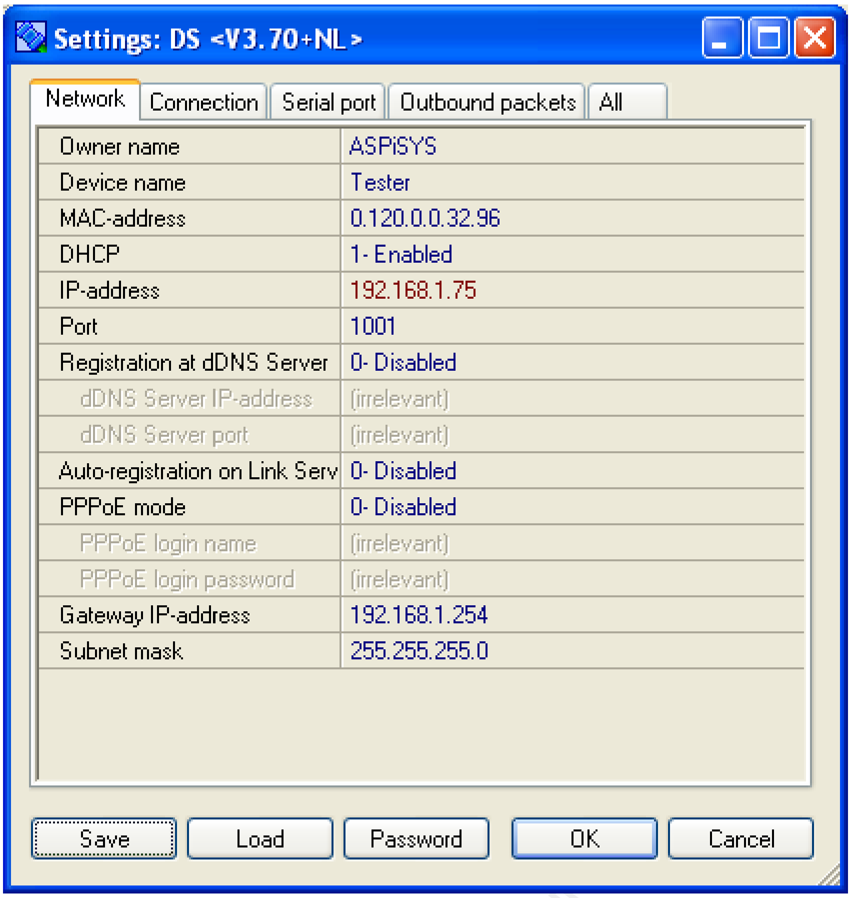
All LogLock units come with a 10/100Mbps Ethernet adapter. Connect it to a hub/switch or PC using standard Ethernet UTP cable. *Use cross cable for direct PC connection*. From the **`tdst-5-05-00-x86.exe`** file on the accompanying CD (or Internet download as instructed, if a CD was not provided), install only the “DS Manager” application and run it. Your “DS Manager Settings” should be similar to the following pictures (but certain parameters, such as the IP address, may be different depending on your specific network setup):



Status	MAC	IP	Owner/Device name
●	0.120.0.0.48.249	192.168.1.72 (local DHCP)	Tony/A1
●	0.2.3.4.40.115	192.168.1.64 (local DHCP)	ASPiSYS/LogLock
●	0.202.0.1.68.190	192.168.1.71 (local DHCP)	ASPiSYS/Backdoor
●	0.120.0.0.32.96	192.168.1.75 (local DHCP)	ASPiSYS/TestUnit

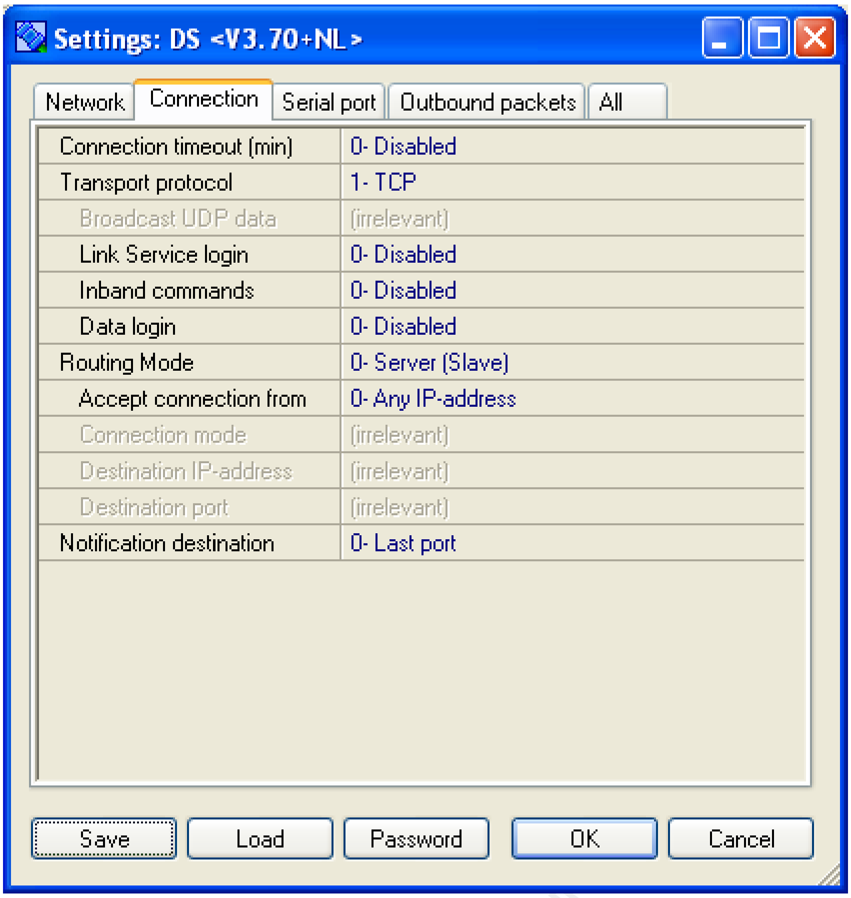
This is a single-port Device Server
This device is operating normally
Connection is closed (the device is idle)

Multiple devices may be showing. Double-click on the specific device you want to change.



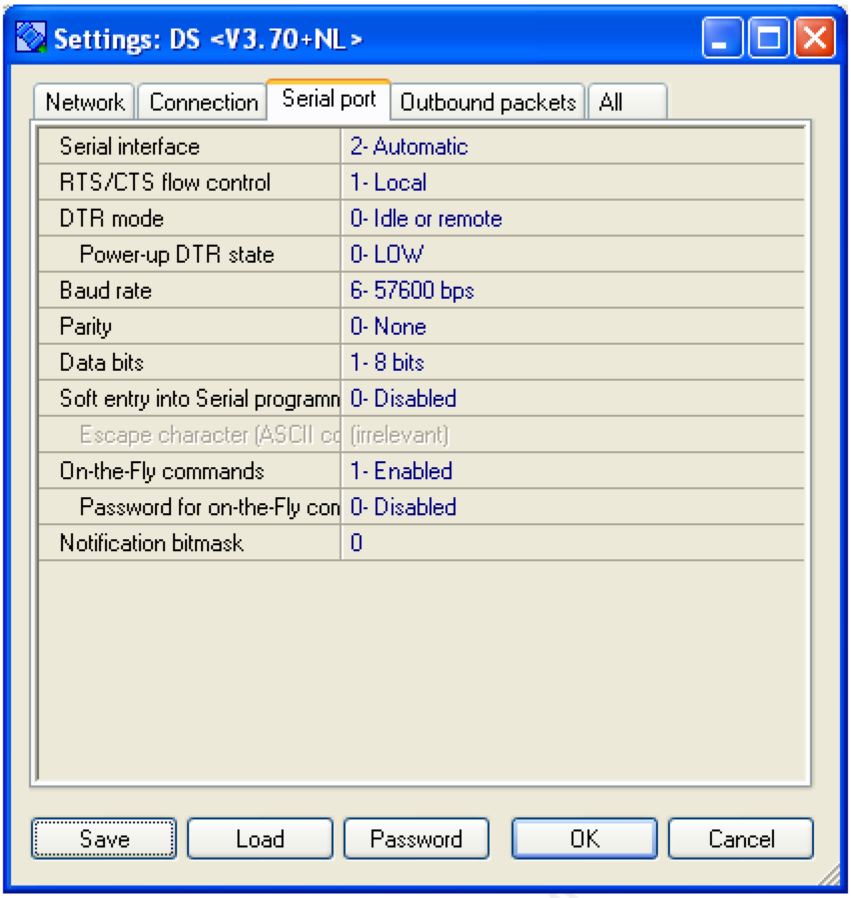
Owner name	ASPiSYS
Device name	Tester
MAC-address	0.120.0.0.32.96
DHCP	1- Enabled
IP-address	192.168.1.75
Port	1001
Registration at dDNS Server	0- Disabled
dDNS Server IP-address	(irrelevant)
dDNS Server port	(irrelevant)
Auto-registration on Link Serv	0- Disabled
PPPoE mode	0- Disabled
PPPoE login name	(irrelevant)
PPPoE login password	(irrelevant)
Gateway IP-address	192.168.1.254
Subnet mask	255.255.255.0

Owner name and device name are optional and can be set to your liking. The device name can indicate which access point it controls *(e.g., CompRoom)*.
MAC address is changeable but should be unique. *Do not change unless you really know why*.
DHCP can be enabled or disabled depending on whether you want your device to obtain an IP address dynamically from the network's DHCP server, or manually.
Port should be any valid port number *(i.e., a number from 1 to 65534)*, and there is really no reason to change it from the default (**1001**).
Gateway is your network's router IP address, *or PC address, if connected directly through a cross cable.*
Subnet mask is again network specific. If you're unsure what to use for gateway and mask, issue the IPCONFIG command from the command console, and use the same numbers as your PC's.



Connection timeout (min)	0- Disabled
Transport protocol	1- TCP
Broadcast UDP data	(irrelevant)
Link Service login	0- Disabled
Inband commands	0- Disabled
Data login	0- Disabled
Routing Mode	0- Server (Slave)
Accept connection from	0- Any IP-address
Connection mode	(irrelevant)
Destination IP-address	(irrelevant)
Destination port	(irrelevant)
Notification destination	0- Last port

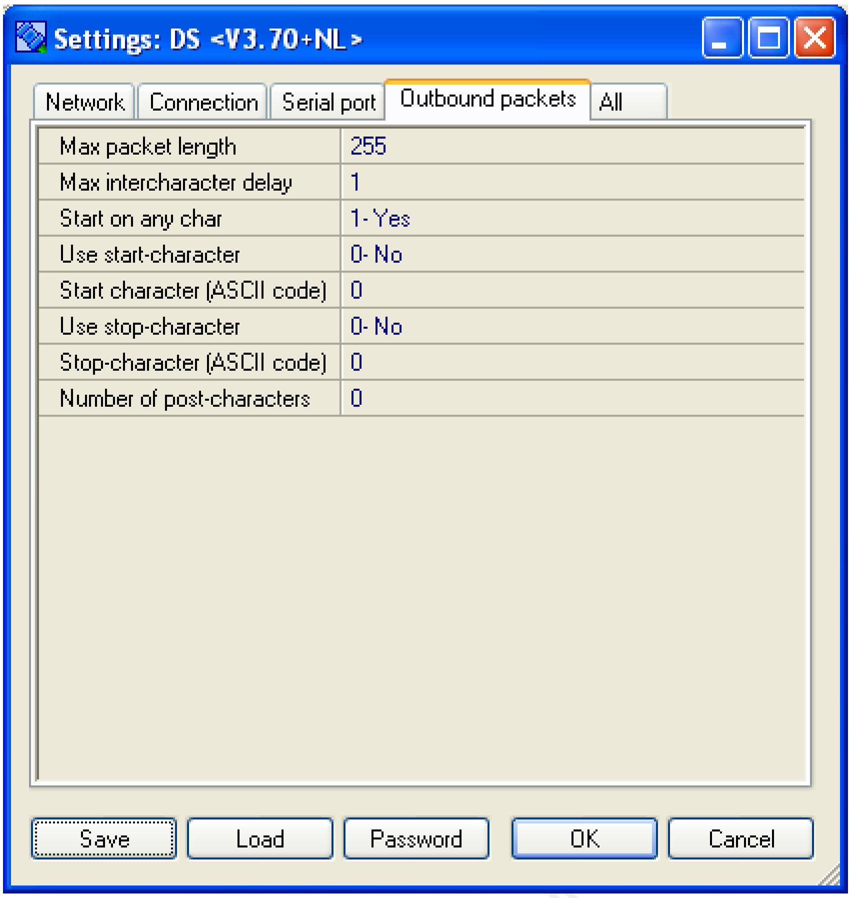
In the connection Tab, it's important to set the Transport protocol to **TCP**. Connection timeout is up to you, depending on your application (a zero disables timeout). Routing Mode should be "**0-Server (Slave)**". Unless you want to accept connections from only a single IP address, leave the 'Accept connection from' box to 'Any IP-address'.



Serial interface	2- Automatic
RTS/CTS flow control	1- Local
DTR mode	0- Idle or remote
Power-up DTR state	0- LOW
Baud rate	6- 57600 bps
Parity	0- None
Data bits	1- 8 bits
Soft entry into Serial programn	0- Disabled
Escape character (ASCII cc	(irrelevant)
On-the-Fly commands	1- Enabled
Password for on-the-Fly con	0- Disabled
Notification bitmask	0

In the Serial port Tab, it’s important that you make the following settings the same as shown above:

Serial interface, RTS/CTS flow control, DTR mode, Power-up DTR state, Baud rate, Parity, and Data bits. *These should already have the correct settings but if you inadvertently changed them you can restore them to the ones shown above.*



Max packet length	255
Max intercharacter delay	1
Start on any char	1- Yes
Use start-character	0- No
Start character (ASCII code)	0
Use stop-character	0- No
Stop-character (ASCII code)	0
Number of post-characters	0

In the Outbound Packets Tab, use the above preferred settings. ‘Start on any char’ should always be set to 1-Yes. *Various settings in this tab may work, but the ones shown work best.*

Press Save if you want to make a backup file of this configuration on your PC (to load perhaps into another device). Finally, press OK to send the configuration to the device. Changes sent to the device are remembered across power cycling. *Any active connection is lost.*

IMPORTANT: DS Manager cannot auto-detect devices across a router. Your devices must be in the same network segment.

Restarting the unit, you should see the LCD light up *(if an appropriate LCD is connected)* and the terminal screen welcome you with a copyright message and the firmware version of your unit. You're done! *Because the Ethernet module itself is reset, your connection is lost and it must be re-established.*

Press `?[ENTER]` on the terminal to see the unit's command help screen. If nothing appears check your connections and settings.

Hint: To connect using HyperTerm, press the Connection Properties button, select TCP/IP connection (rather than a COM port), and enter the corresponding IP or domain name and port number (default 1001).

For any questions or first-time programming of the unit please write or call us.

REVISION HISTORY *(most recent at the top) [earliest purchase date in brackets]*

v3.53: bOS8 v1.80 [2010.07.29]

1. Fixed issue with showing “Searching” when in LCD2 mode, if exit iButton is not allowed (zone 255).

v3.52: bOS8 v1.80 [2010.05.06]

1. Internal optimizations.

v3.51: bOS8 v1.80 [2010.04.16]

2. Added manual command (DZU) to delete users assigned to specific zone.
3. Added password delay on wrong MASTER_RESET codes.
4. Push Button records date of addition for non-zero zones.
5. PBZ command now defaults to zero zone.

v3.50: bOS8 v1.80 [2010.04.10]

1. Optimized log wrap-around method (which occurs every time the log becomes full) to make it practically instantaneous. ***Major Internal Change.***
2. Improved long-term log memory durability by using fewer overall memory writes.
3. Made Date Range restricted log display’s response time practically instantaneous.
4. Internal optimizations.

v3.45: bOS8 v1.80 [2010.03.12]

1. Removed “Low Battery” warning during name display on the LCD.
2. Internal optimizations.

v3.44: bOS8 v1.80 [2010.03.09]

1. Added bi-directional LCD capability (mostly, for use as time-attendance only).
2. Added `LCD1` and `LCD2` commands to control [1] above.
3. Added auto-clearing of username from LCD after several (10) seconds.
4. Internal optimizations.

v3.44: bOS8 v1.80 [2010.03.09]

1. Added bi-directional LCD capability (mostly, for use as time-attendance only).
2. Added `LCD1` and `LCD2` commands to control [1] above.
3. Added auto-clearing of username from LCD after several (10) seconds.
4. Internal optimizations.

v3.43: bOS8 v1.80 [2010.03.05]

1. Fixed "Low Battery" warning so it goes away.
2. Internal optimizations.

v3.42: bOS8 v1.71 [2009.11.14]

1. Setting a wrong clock will display the word "incorrectly".
2. Added "Build" date on copyright message.

v3.41: bOS8 v1.71 [2009.10.01]

1. Bug fix: Disallowed zone 255 from manual `AUTO` command (which caused a system stall due to the impossibility of the situation).

v3.40: bOS8 v1.70 [2009.08.27]

1. Disallowed zone 255 exits.
2. Increased device name length to 60 characters.
3. Internal optimizations.

v3.39: bOS8 v1.6x [2009.05.25]

1. Added manual auto-exit for specific zone *including zero zone*. To use, follow the command `AUTO` with a zone number. This works regardless if the auto-exit mode is currently enabled or disabled.
2. `Z` command now prints `ERROR` on wrong zone number.
3. Added *PASS Attempts* counter in `DIR` screen.
4. Added *Resets* counter in `DIR` screen.

v3.38: bOS8 v1.50/1.40 [2009.05.20]

1. Added 5-second delay after each failed password attempt. This severely inhibits brute force attack methods *as it takes more than 3.33E48 years to go through just half of all possible codes.* [Regardless, it's wise to define long passwords using a wide variety of characters, spaces, letters, numbers, and punctuation marks.]

v3.37: bOS8 v1.50/1.40 [2009.05.19]

1. Internal optimizations.
2. Several changes in various informational messages (help screens, etc.)
3. Provided the `LOCK` and `PASS` passwords are different, giving the `PASS` password from locked mode takes you straight to config mode, bypassing normal mode. This means you can still enter config mode, even if the `LOCK` password is forgotten. *For best security, the `LOCK` and `PASS` passwords should be different, especially if more than one person uses the LogLock terminal.*

v3.36: bOS8 v1.50/1.40 [2009.05.18]

1. Added ‘wildcard’ Starting/Ending dates in `AU` command. The `YY`, `MM`, `DD` or a combination of these date elements may be wildcarded *(using `..` instead of the corresponding number)* for a much wider range of possibilities, such as entry every first Monday of every month *(in combination with appropriate zone entry)*, only Februaries every year, from March to May every year, etc.

v3.35: bOS8 v1.50/1.40 [2009.05.13]

1. The `WHO` command no longer shows attempted entries, only successful ones. Use the `LAST` command, instead, if you need to look at attempted entries.
2. On a similar note, auto-exit will not apply to attempted entries, only true entries.

v3.34: bOS8 v1.50/1.40 [2009.05.12]

1. Bug fix for v3.33 addition. The auto-exit would only do one person at a time even when several people should be exited together.

v3.33: bOS8 v1.50/1.40 [2009.05.11]

1. Internal optimizations
2. Added capability for auto-exit for selected zone entries. Added new commands `AUTO` and `NOAUTO` as well as `AUTO` parameter to `AZ` command.

v3.32: bOS8 v1.50/1.40 [2009.05.05]

1. Internal optimizations
2. `DEVICE` command works in `LOCK` mode to help identify the machine for using appropriate password. (`INFO` showed the string, already, but `DEVICE` command was not accepted.)
3. Zones can now be set with just the holiday bit to define a holiday-only schedule, e.g.,
   ```
   AH 20 -MTWTF-- 0900 1700
   AH 20 -------H 0900 1700
   ```
   will allow those in zone 20 to enter on any holiday from 09:00 to 17:00 regardless of day-of-week *(i.e., even Saturdays and Sundays in this example, provided these fall on defined holidays)*, and weekdays from 09:00 to 17:00. This is different from
   ```
   AH 20 -MTWTF-H 0900 1700
   ```
   which allows entry on Mon-Fri from 09:00 to 17:00 regardless if the day is a holiday or not, but which will never allow access on Saturdays and Sundays.

v3.31: bOS8 v1.50/1.40 [2009.05.04]

1. Invalid clock condition is immediate *(even when setting clock)* when year is anything < 9.

2. When truncating a full Log, automatically re-apply the current `D` command date range.
3. Count number of alarm events *(up to 255)* and show counter in `DIR` screen.
4. Added `CLEAR` command to zero the alarm counter.
5. Added `DEVICE` command to show, change, or remove device name / comment. Use `?` for name to remove. The `DEVICE` string, if defined, is also shown in the `INFO` screen.
6. `D` command now interprets the symbol `*` as today's date, e.g., use: `D *` for quickly setting the range From Date to today.

v3.30: bOS8 v1.50/1.40 [2009.04.28]

1. When the clock is invalid *(see v3.29 details)* logging is disabled.
2. Improved `REN/REX` debounce.
3. Disallowed stuck `REN/REX` switch from opening the door continuously. The `REN/REX` switch must be released before another `REN/REX` switch event is accepted. A stuck switch no longer affects the manual `REN/REX` commands.
4. Monitor mode did not show username in `HIDE` mode. `HIDE` mode should only hide the username from the LCD, besides hiding user IDs in user mode.

v3.29: bOS8 v1.50/1.40 [2009.04.28]

1. When the clock information is lost due to a power-on reset with a failed clock backup battery, the status LED will blink rapidly, and the `DIR` display will show `[INVALID]` next to the time. When in this error condition only zero zone people will be allowed access since date/time cannot be trusted for zoned access. Setting the clock clears the error condition.

v3.28: bOS8 v1.50/1.40 [2009.04.20]

1. Added optional delay for stopping an alarm event. Once the alarm goes off it won't stop until this delay expires, or a successful access occurs (valid key or allowed `REN/REX` command).

v3.27: bOS8 v1.50 [2009.04.10]

1. Added Serial Number display for units based on bOS8 v1.50 *(which is otherwise 100% compatible to bOS8 v1.40)*

v3.26: bOS8 v1.40 [2009.04.09]

1. Removed the implicit `HELP` command (pressing `[ENTER]` on a blank line). To display the help screen, one of the two explicit commands, `?` or `HELP` must be used. This little change helps some telnet terminals that send extra characters on Linefeed from not choking due to unexpected repeated help messages on receiving a file (such as a backup) via a Paste operation.

2. `LOCK` command is now completely ignored in user mode (as it didn't do anything, anyway). It's only active in locked mode (for entering user mode) and config mode (for changing the `LOCK` password).

v3.25: bOS8 v1.40 [2009.04.08]

1. Made `PASS` a synonym for `LOCK` when in terminal locked mode.

v3.24: bOS8 v1.40 [2009.04.06]

1. Added display of username in Monitor mode.
2. Made `LOCK` command visible only in config mode help.

v3.23: bOS8 v1.40 [2009.04.04]

1. Improvement on a privacy issue. Added the new command `LOCK` for defining an optional password for terminal access *(which may be different from the config password)*. A `NOPASS` command from the `[>]` mode will go into locked mode *indicated by the prompt `[!]`*. In locked mode, only the following *harmless* commands are available: `ANSI`, `CLS`, `INFO`, `REM`, `LOCK`, and `MASTER-RESET`. [`MASTER_RESET` is available in all modes in case one is ever locked out by forgotten password(s).] Only the `INFO` command is shown in the help screen, however. Locked mode protects from casual browsing of settings or the user and log lists by chance visitors (e.g., if the unit is accessible over the Internet). Only in config mode, one can [re-]define the `LOCK` password.
2. `MASTER-RESET` updated to clear both passwords (`PASS` and `LOCK`).

v3.22: bOS8 v1.40 [2009.03.26]

1. Fixed minor bug with not being able to add the 256th holiday.

v3.21: bOS8 v1.40 [2009.03.24]

1. Zoned `EXIT` in `S1` mode is now auxiliary output *(i.e., not for exit)*.
2. `NOENTRY` and `NOEXIT` no longer attempt to close on non-zero `ENTRY` or `EXIT`, respectively.

v3.20: bOS8 v1.40 [2009.03.19]

1. Added command `MU` to Move User to another zone.
2. Added current alarm status in `DIR` screen.

v3.19: bOS8 v1.40 [2009.03.19]

1. Added command `LAST`. Similar to `WHO` but shows any action, not just entries.
2. `REM` command no longer prints the message that follows it.

v3.18: bOS8 v1.40 [2009.03.09]

1. Fixed a small bug with the alarm sounding even during a `REN/REX` event.
2. Minor cosmetic change in backup files.
3. Manual `ENTRY` & `EXIT` now print `'ERROR'` if set for automatic use *(zone <> zero)*.

v3.17: bOS8 v1.40 [2009.03.04]

1. Improved battery charging.

v3.16: bOS8 v1.40 [2009.02.26]

1. Added Push Button capability.

v3.15: bOS8 v1.40 [2009.01.26]

1. Added `REM` command.
2. Fixed first time alarm to use defined alarm time.

v3.14: bOS8 v1.40 [2009.01.24]

1. Alarm no longer sounds during `ENTRY/EXIT` commands (manual/automatic).

v3.13: bOS8 v1.40 [2009.01.22]

1. Added `ALARM` command and door-open detection.

v3.12: bOS8 v1.40 [2009.01.09]

1. Added "I'm alive" pulse to main LED.

v3.11: bOS8 v1.40 [2008.12.29]

1. Internal optimizations.

v3.10: bOS8 v1.40 [2008.12.28]

1. Zero `DT` does not attempt to open door (short pulse eliminated).

v3.09: bOS8 v1.40 [2008.12.28]

1. Internal optimizations.

v3.08: bOS8 v1.40 [2008.12.28]

1. Added automatic reset of iButton readers when losing connection in Monitor mode.

v3.07: bOS8 v1.40 [2008.12.28]

1. Monitor mode has 1 min limit in normal mode, 24 hour limit in config mode.

v3.06: bOS8 v1.40 [2008.12.28]

1. Hide username from LCD in `HIDE` mode.

v3.05: bOS8 v1.40 [2008.12.28]

1. Internal optimizations.

v3.04: bOS8 v1.40 [2008.12.28]

1. Added brief LED blink when reading iButton keys.

v3.03: bOS8 v1.30 [2008.12.02]

1. Added half-sec delay after iButton before opening door.

v3.02: bOS8 v1.20 [2008.12.01]

1. Added `TEMP` command *(for OEM use, mostly).*

v3.01: bOS8 v1.10 [2008.11.20]

1. Added full Greek alphabet conversion.
2. Added `HIDE` command.
3. Added separate `DT` delays for entry and exit.
4. Added separate `AC/DC` mode for entry and exit.

v3.00: bOS8 v1.00 [2008.10.01]

Original LogLock 3000/Mini firmware based on LogLock 2000 v2.54.

Possible compatibility issues with older LogLock 2000 versions.

1. The `ENTRY` and `EXIT` commands are more powerful, and a zone number may follow them. The OEM default is 255, which practically disables the commands. To make the system behave the same, as with original firmware, you must first assign zone 0 (zero) to both `ENTRY` and `EXIT` and save the changes using the `SAVE` command (if they must survive a `RESET`).

2. Lines in original firmware ended with `CR|LF` pairs but used single `LF` characters to advance additional lines (e.g., the sequence `CR|LF|LF` was possible). Current firmware uses a `CR|LF` pair for each new line (e.g., `CR|LF|CR|LF`). This should not cause a problem unless your custom software specifically expects a sequence of consecutive `LF` characters based on previous observations of the actual data stream.

3. Inputs were accepted on lines ending with either `CR` or `LF`. Now, only `CR` can be used to end an input line, LF is ignored. This change offers better telnet behavior with applications other than HyperTerm. If the command you sent from your custom application ended with just an `LF`, you must change it to a `CR` character, *which will work both with current and previous versions.*

4. The `DIR` and `HELP` output screens may change slightly from version to version to accommodate new commands or options. If your software expects a specific output from the `DIR` screen in particular, you'll have to allow for the changes by examining the new `DIR` output.

CONNECTIVITY DETAILS

The following table shows the pin out for the PCB *(shown simulated on the next page)*. **If you need assistance, please contact us before attempting to make possibly incorrect connections, which may damage the device.**

Name	Description
i1	iButton Reader #1 (primary – entry) gray reader cable
iB	Common iButton Reader Ground (black reader cable)
i2	iButton Reader #2 (secondary – exit) gray reader cable
+V	Power Supply 9-12VDC positive (3 Amps max, depends on strike)
GND	Common Ground
LC1+	Primary door strike [entries] (positive lead)
LC1-	Primary door strike [entries] (negative lead)
LC2+	Secondary door strike [exits] (positive lead)
LC2-	Secondary door strike [exits] (negative lead)
REN	Optional Request-to-Enter push-button (same as `REN` command)
REX	Optional Request-to-Exit push-button (same as `REX` command)
BUTTON	Push-Button for adding ‘guest’ users (optionally enabled)
Ethernet	Standard Ethernet connectivity jack RJ45 - **10/100Mbps**
TX	Alarm output (High=Alarm). **Use appropriate FET/transistor to drive external siren.**
GND	Common Ground for TX / RX pins
RX	Door-left-open switch (Low=door is closed)

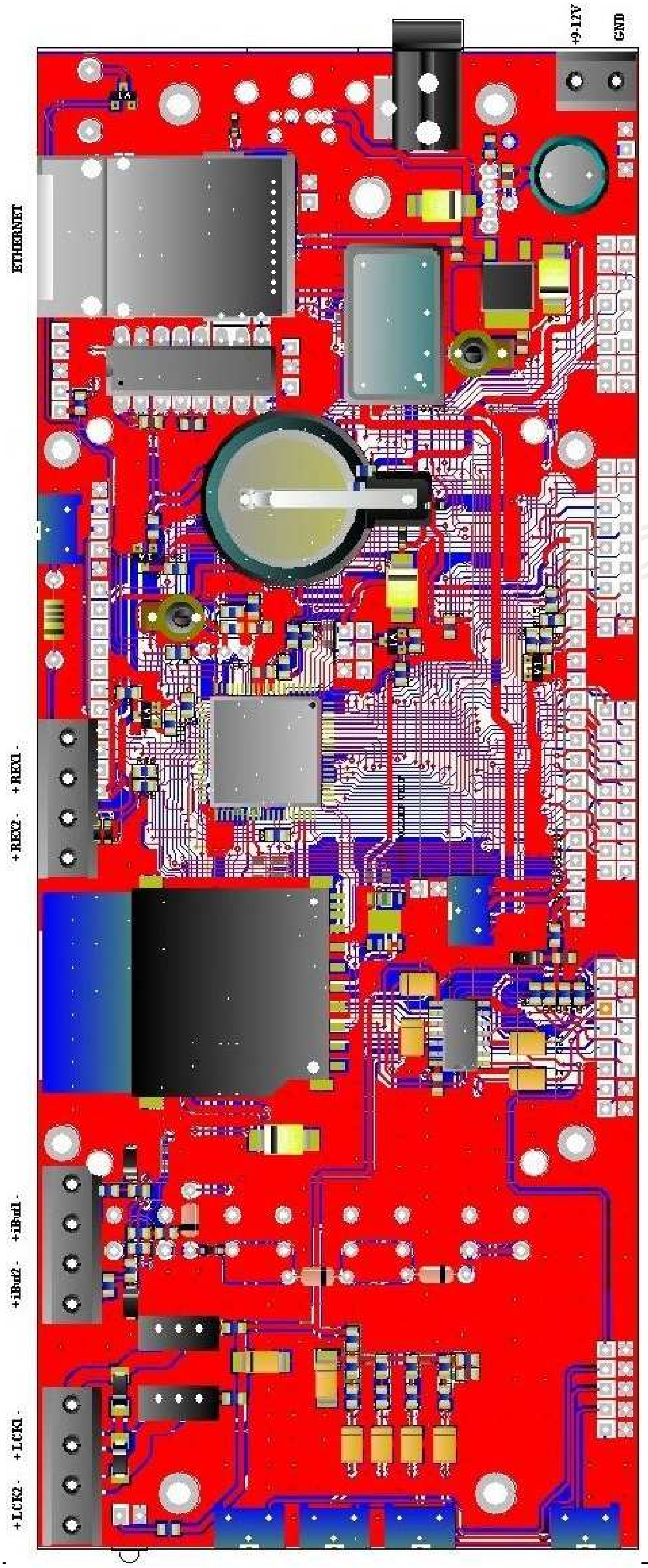
Note: LC1/LC2 polarity is not significant for AC strikes. It is important for relays, however.

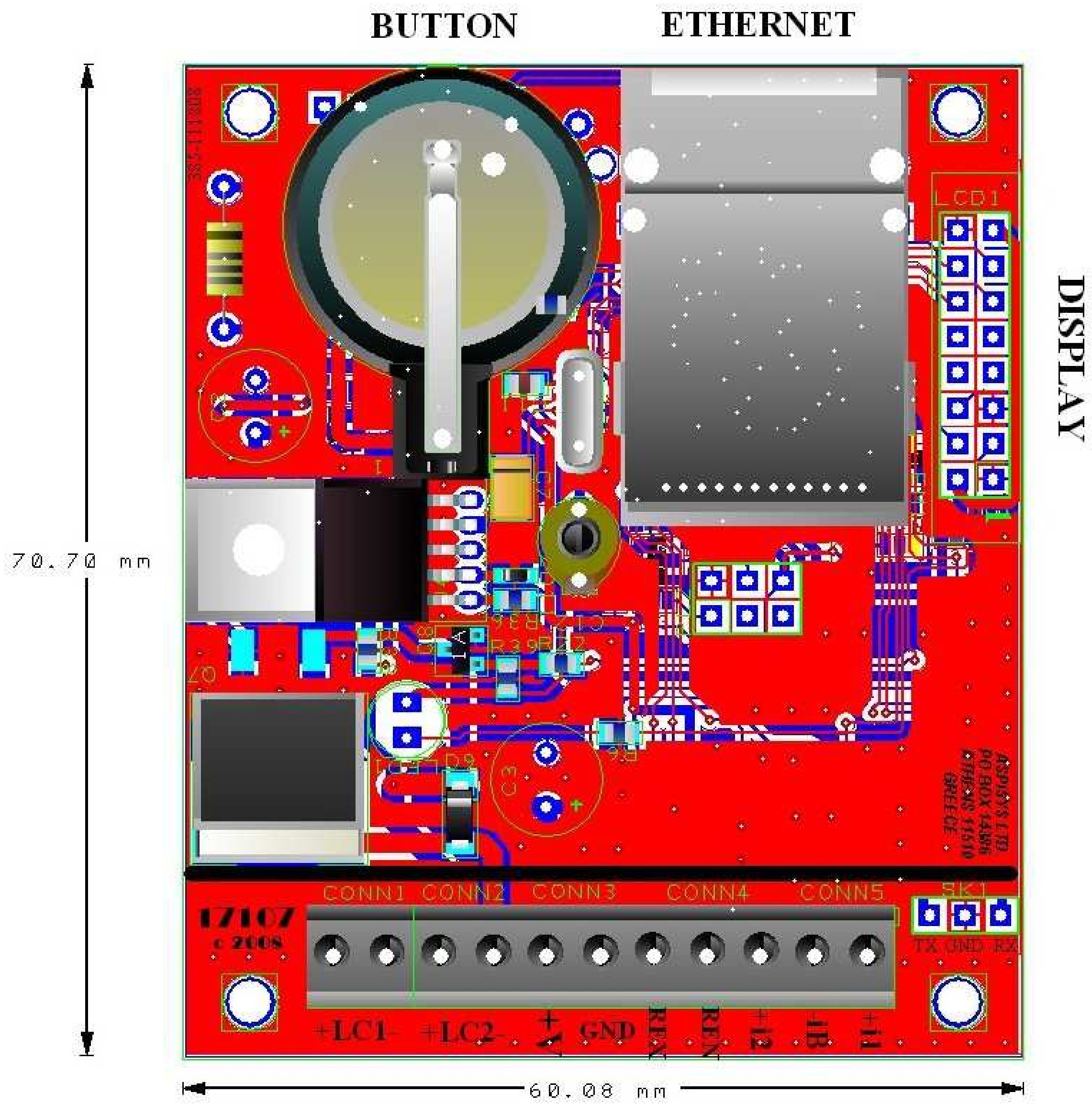
LogLock Mini LCD pin-out.

For correct operation *(if adding the LCD yourself)*, please use only a 20x4 (20 characters per line, 4 line) LCD with a compatible pin out.

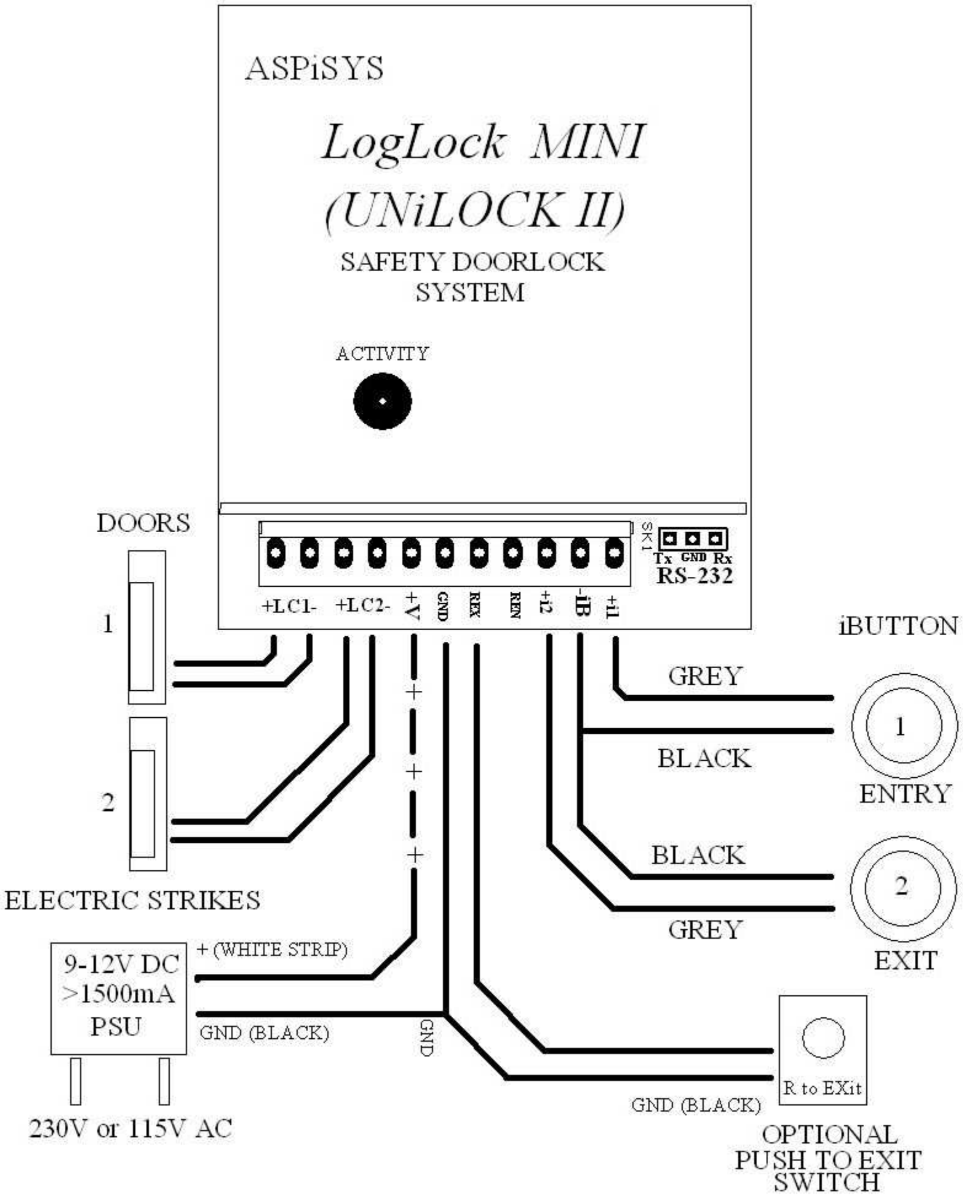
PIN Number	Pin Description
1	GND *(This pin is clearly marked on the LCD header with “1”)*
2	+5V
3	Contrast
4	RS = Register Select
5	R/W = Read /Write
6	E = Enable
7-14	D0..D7 = Data0 .. Data7
15	Backlight +
16	Backlight -

LogLock 3000 PCB





LogLock Mini PCB



LogLock MINI - CONNECTION DIAGRAM