Engineering
2232 Northmont Parkway
Duluth, Georgia 30096
USA

Original Date:	2010/03/03	Document:	ICD_PP.doc
Project Number:	2036	Page:	Page 1 of 44
Dwg. /Part Number /Id:	N/A		

Interface Control Document (ICD)

Portable Programmer

DISTRIBUTION: Per document OPDP00003

ORIGINAL APPROVAL:

Prepared by (Last, First Initial)	Signature & Date (Use Italics)	Approved by (Last, First Initial)	Signature & Date (Use Italics)
Leyva, S	*Silvia B. Leyva (2010/03/10)*	Vahalia, K	*Ketki Vahalia (2010/03/10)*

REVISION APPROVAL RECORD (Revision history on next page):

Revision Number	Revision Date (yyyy/mm/dd)	Prepared by (Last, First Initial)	Approved by (Last, First Initial)	Signature & Date (Use Italics)

REVISION HISTORY:

Revision Number	Revision Date (yyyy/mm/dd)	Prepared by (Last, First Initial)	Description of Changes (reference section or page numbers)

Table of Contents

List of Tables

1 Scope

This document explains the interface between the LMS and the Portable Programmer. The Portable Programmer is made up of a PDA, PDA Adaptor and Portable Programmer Application. To transfer information between LMS and Portable programmer the system uses a CSV files and Audits.

1.1 Definitions, Abbreviation and Acronyms

The terms in use in the document are explained below:

Acronym	Description
ACF	Access Control Format
ACU	Access Control Unit
ADA	Americans with Disabilities Act
AFC	Alternate Fire Code
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
CM	Control Module
CSV	Comma Separated Value
DST	Daylight Savings Time
EEPROM	Electrically Erasable Programmable Read Only Memory
HEX	Hexadecimal
ILS	Intelligent Lock System
Issue Code	The sequence number of the card
LED	Light Emitting Diode
LMS	Lock Management System
LSB	Least Significant Bit
MSB	Most Significant Bit
NA	Not Applicable
PDA	Personal Digital Assistant
PP	Portable Programmer
RTC	Real Time Clock
SCF	Smart Card Format
WLM	Wireless Lock Module

Table 1: References

1.2 References

Ref	Number	Title	Version
A	ORP_OA	ORP Document	B

Table 2: References

2 Portable Programmer Application Overview

The Portable Programmer Application is used to configure the locks with various configurations. To load the PP Application with the required data a CSV file is used. The CSV File is in ANSI encoding format and the contents are extracted for use by the PP Application.

This document describes the parameters expected in the CSV file. These parameters shall be generated by the LMS.

2.1 CSV file Format

The CSV file has the following sections. Each section is indicated by a corresponding numeric in the range 1-11.The integer mapping is given below.

- 1 – Door Details
- 2 – Application Configuration
- 3 – Site Configuration
- 4 – Operator Details
- 5 – DST details
- 6 – Holidays information
- 7 – Time zone information
- 8 – Automatic Changes information
- 9 – User Details
- 10 – ACF
- 11 – SCF
- 12 – Priority Events

Each section begins with the numeric value corresponding to the section and is followed by parameter values specific to that section. Every parameter value in the section is separated by a comma. The end of a section is indicated by using a semicolon.

Each section along with the parameters is described in the section 3.

Each CSV file shall contain at least one entry for each of the following sections:

- 1 – Door Details
- 2 – Application Configuration
- 3 – Site Configuration
- 4 – Operator Details

If a section is present in the CSV file, then all the fields in that section are mandatory. Blank spaces are not allowed.

2.2 File Transfer between PDA and LMS

2.2.1 Downloading the Lock Configuration File onto PDA

The LMS application shall generate the PP Application configuration data file named “Ppdata.txt” using the details described in the section 3. When a new lock configuration file has to be loaded to the PDA the following steps are required

1) The system operator shall connect the PDA to the system via ActiveSync.
2) Select relevant option in the LMS software that shall download and transfer the CSV file (Ppdata.txt) into the PDA’s **My Document** folder (\My Document).

2.2.2 Uploading PP and Lock Audits onto the LMS

Upon executing upload operation by the PP Application operator, the PP Application shall generate either a PP or Lock audits file in the **My Document** folder (\My Document).

The LMS shall automatically read the audit files from the PDA. The PP audit file shall be named “PPAudits.txt” and Lock audit file shall be named as “LockAudits.txt”. The LMS shall delete the files, “PPAudits.txt” and “LockAudits.txt”, from the PDA upon a successful upload operation. This will avoid the possibility of uploading the same audit files again.

3 CSV File Description

3.1 Door Details

This section outlines the parameters for the door details section of the CSV File. They are described in the order in which they appear in the CSV file.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to door details. Please refer to Section 3.1.1 for an example	Format: Decimal Range: NA Fixed Value: 1
LOCKID	The LMS generated unique number for door.	Format: HEX Range:1- FFFFFFFF Default Value: NA
LOCK NAME	A user defined lock name, max of 40 characters.	Format: String (ASCII) Range: Max 40 Characters Default Value: NA
STD OPEN TIME (in seconds)	This specifies the time the door should remain open after the door is unlocked using a card or PIN or both.	Format: Decimal Range: 1- 255 Default Value: 6
EXTD OPEN TIME (in seconds)	This specifies the time the door should remain open when unlocked by an ADA user. This is always longer than the normal door unlock/std open time duration.	Format: Decimal Range: 1- 255 Default Value: 15
ENABLE KEYPAD	This parameter states whether the keypad function is enabled or not in the lock	Format: Decimal Range: 0 -1 Default Value: 0 0 - Disable keypad 1 - Enable keypad
ENABLE BLOCK WITH CARD	If this parameter is enabled and a valid blocking card is presented, the lock will change the mode into block mode	Format: Decimal Range: 0 - 1 Default Value: 1 0 – Disable Block mode. 1 – Enable Block mode.
ENABLE PRIVACY	This parameter states if the Privacy mode of the door is enabled or disabled	Format: Decimal Range: 0 - 1 Default Value: 1 0 – Disable privacy feature. 1 – Enable privacy feature.

Parameter Name	Description	Values
ENABLE BUZZER	This parameter states whether the buzzer should beep The beep that is enabled can be for conditions such as access denied and door held open alarm.	Format: Decimal Range: 0 - 1 Default Value: 1 0 – Disable buzzer. 1 – Enable buzzer.
ENABLE LATCHMONITOR	Enabling this option allows the user to enable the latch monitoring feature.	Format: Decimal Range: 0 - 1 Default Value: 0 0 – Disable Latch Monitor feature. 1 – Enable Latch Monitor feature.
ENABLE DOOR SENSOR	This parameter indicates enables/disables the use of the door sensor switch.	Format: Decimal Range: 0 - 1 Default Value: 1 0 – Disable door sensor feature. 1 – Enable door sensor feature.
ENABLE OFFICE WITH CARD	When enabled, this option allows the lock owner to put the lock into Office Mode by swiping the owner card twice within ‘unlock timer’ interval. This function shall also govern taking lock out of Office Mode with Owner card.	Format: Decimal Range: 0 -1 Default Value: 0 0- Disable OFFICE WITH CARD feature. 1 – Enable OFFICE WITH CARD feature.
DEADBOLT ENDS AFC MODE	When this option is enabled, the activation of the deadbolt relocks the lock that was left unlocked under AFC settings.	Format: Decimal Range: 0 -1 Default Value: 0 0 – Disable DEADBOLT ENDS AFC MODE feature. 1 – Enable DEADBOLT ENDS AFC feature.
AFC ON EXIT	When enabled, lock unlocks and does not relock as it would normally after door is opened from the inside.	Format: Decimal Range: 0 -1 Default Value: 0 0 – Disable 1 – Enable
AFC ON ENTER	When enabled, lock does not relock as it would normally after door is opened from the outside following access granted.	Format: Decimal Range: 0 -1 Default Value: 0 0 – Disable 1 – Enable

Parameter Name	Description	Values
ENABLE RELOCK TIMER	Selecting this option enables the relocking timer to relock the door after a specific amount of time after the door is unlocked under AFC settings.	Format: Decimal Range: 0 – 1 Default Value: 0 0- Disable RELOCK TIMER feature. 1 – Enable RELOCK TIMER feature.
RELOCK TIMER	The value in this field indicates the duration the door will remain unlocked under AFC conditions before relocking automatically. The value may be set in minutes or seconds. This field is and 8 bit value with 2 parts. The MSB bit denotes whether duration is in minutes or seconds. The remaining 7 bits represents relock timer value	Format: Decimal (1byte) Range: 0 – 1 (MSB bit) and 1 – 99 (remaining 7 bits) Default Value: 1 MSB (1 Bit) 0 – indicates unit is in minutes 1 – indicates unit is in seconds Remaining 7 bits: timer duration Examples: If the relock timer value is 5 minutes then this field will have value 5. in bit format: 0000 0101 If the relock timer value is 5 seconds then this field will have value 133. in bit format: 1000 0101
Reserved	Reserved	This value shall be 0 at a times
STD DOOR HELD OPEN	Time duration after which the lock shall raise a door open alarm, if the door is still in open state.	Format: Decimal Range: 5 - 255 Default Value: NA

Parameter Name	Description	Values
EXT DOOR HELD OPEN	Time duration for ADA user after which the lock shall raise a door open alarm if the door is still in open state.	Format: Decimal Range: 5 - 255 Default Value: NA
LOCK AUTHORIZATION	Authorization filter is the authorization level set in the door configuration which will be matched with the user authorization to provide access to the door.	Format: Decimal Range: 0-40 Default Value: 0
LOOK AHEAD MAX	Determines the range of issue codes accepted by the lock. The lock accepts issues codes in the range of current issue code to current issue code + look ahead	Format: Decimal Range: 0 -99 Default Value: 1
ENABLE DOOR HELD OPEN ALARM	If enabled, the alarm will be triggered if the door held open duration is exceeded	Format: Decimal Range: 0 -1 Default Value: 1 0 – Disabled 1 - Enabled
DOOR HELD OPEN ALARM DURATION	Door Held Open Alarm Duration	Format: Decimal Range: 1 -255 Default Value: 30
PRIORITY CARD_USER	This option determines the precedence of the data that is present on both the card and the lock If it is 0, the data from the card is considered for data validation. If it is 1, then the data from the lock is considered for the validation.	Format: Decimal Range: 0 -1 Default Value: 1
IDF_ DATE	This parameter indicates whether the Activation/Deactivation date has to be used in Access control decisions	Format: Decimal Range: 0 -2 Default Value: 0 0 = None 1 = Date 2 = Date and Time

Parameter Name	Description	Values
LOCK_MODE	Different modes in which the lock can be operated	Format: Decimal Range: 1 - 10 Default Value: 4 1 = Office 2 = Office 1st 4 = Standard 7 = Blocked 8 = Emergency Lock mode 9 = Emergency Unlock mode 10= Foyer Mode
LOCK_ON_RELEASE	Relocks door on handle release if enabled. Else lock relocks after open time has expired	Format: Binary Range:0-1 Default Value: 1 0 – Disable Lock on release feature. 1 – Enable Lock on release feature.
Reserved	Reserved	Default Value:3
CARD NUM SIZE	Size of card number (Badge ID) in bytes	Format: Decimal Range: 2-8 Default Value: NA
ISSUECODE SIZE	Size of issue code in bytes	Format: Decimal Range: 1-4 Default Value: NA
ACU_LMS_COM TIMEOUT (in seconds)	This field specifies the ACU to LMS communication timeout.	Format: Decimal Range: 1 -10 seconds Default Value: 6 seconds
ACU_LMS_COM_ RETRY	This field specifies the ACU to LMS communication retry count.	Format: Decimal Range: 1 -10 Default Value: 3
HEART_BEAT_RATE (in seconds)	This field is a Wireless Operational Parameter that specifies the time between transmissions from the lock to the WAP.	Format: Decimal Range: 60 - 86400 Default Value: 300

Parameter Name	Description	Values
RF_OUTPUT_ POWER	This field is a Wireless Operational Parameter that specifies the lock output power.	Format: Decimal Range: 1 -4 Default Value: 3
CHANNEL_ID	This field is a Wireless Operational Parameter that specifies the lock channel id.	Format: Decimal Range: 1 -26 Default Value: 1
FREQUENCY_ AGILITY_MODE	This field is a Wireless Operational Parameter that specifies the lock frequency agility mode. This is part of the Wireless Operational Parameters – between WLM and WAP. When WAP & WLMs are in this mode, they automatically jump to a new channel when interference is detected on the existing operating channel.	Format: Decimal Range: 0-1 Default Value: 1
CM_WLM_COM TIMEOUT	This field specifies the CM to WLM communication timeout.	Format: Decimal Range: 5 -50 Default Value: 5 (implies 500 milliseconds) Example: Value 5 indicates 500 milliseconds for Lock
CM_WLM_COM_ RETRY	This field specifies the CM to WLM communication retry count.	Format: Decimal Range: 1 -10 Default Value: 3

Table 3 : Door Details

3.1.1 Door Detail Example

1,001E,Test123,6,15,0,1,1,1,0,1,0,0,0,0,1,133,1111,5,10,10,1,1,10,1,2,4,1,10,4,4,6,3,100,3,4,1,5,3;

1,6D12,Sanity,6,15,0,1,1,1,1,1,0,1,0,0,1,133,1111,6,15,10,1,1,10,1,2,4,1,10,4,4,6,6,100,4,10,0,10,7;

3.2 Application Configuration

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to application configuration details. Please refer to Example in Section 3.2.1 below.	Format: Decimal Range: NA Fixed Value: 2
SYSTEM CODE	The System Code is a numeric identifier used for the installation site; it must be supplied by the system provider.	Format: HEX Range: 1 - FFFFFFFF Default Value: NA
ENABLE AUTOLOGOUT	This parameter enables the auto logout feature of the PP Application.	Format: Decimal Range: 0 -1 Default Value: 0 0 - Disable Auto Log Off feature. 1 – Enable Auto Log Off feature.
PP IDLE TIME (in minutes)	If the ENABLE AUTOLOGOUT feature is enabled then PDA application automatically logs out after the specified PP IDLE TIME	Format: Decimal Range: 1 - 120 Default Value: 5
ENABLE DEACTIVATEDATA	This parameter enables the auto Deactivate data feature. If this feature is enabled and if the application is not used for DEACTIVATE DURATION days then database will be deleted after the specified duration.	Format: Decimal Range: 0 -1 Default Value: 0 0 - Disable deactivate data feature. 1 – Enable deactivate data feature.
DEACTIVATE DURATION (in days)	This parameter provides the time after which the application database shall be deleted automatically, provided user has not used the system for the time specified.	Format: Decimal Range: 1 -120 Default Value: 2
DATE	System generated Date. The date when the CSV file is created	Format: mm-dd-yyyy Range: NA Default Value: System Date
MAX LOGIN ATTEMPT	Maximum number of invalid login attempts allowed for PDA application After the Max Login Attempts, the application clears the locking plan data. Audit records are kept.	Format: Decimal Range: 1 - 5 Default Value: 4

Parameter Name	Description	Values
MAX AUTO CHANGE	Maximum number of Automatic changes allowed per door in the system	Format: Decimal Range: 1- 50 Default Value: 50
MAX HOLIDAYS	Maximum number of Holidays allowed in the system	Format: Decimal Range: 1 - 100 Default Value: 100
MAX TIMEZONE	Maximum number of Time Zone allowed in the system	Format: Decimal Range: 1- 64 Default Value: 64
MAX USERS	Maximum number of users allowed per door in the system	Format: Decimal Range: 1 - 5000 Default Value: 5000
MAX DST	Maximum number of DST allowed in the system	Format: Decimal Range: 1 - 10 Default Value: 10
LOG LEVEL	Level of error logging for the PP application 0- No data recorded 1- Print Module Name 2- Print Stack Trace of the Exception (Class, Function and code line number details)	Format: Decimal Range: 0 - 2 Default Value: 1

Table 4 : Application Configuration

3.2.1 Application Configuration Data Example

2,11A5C3B8,1,10,1,30,07-30-2008,5,30,30,30,5000,10;

3.3 Site Configuration

This section outlines configuration information about the site in the order in which it appears in the CSV file.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to site configuration details. Please refer to Section 3.2.1 for an example.	Format: Decimal Range: NA Fixed Value: 3
ENABLE DST	This parameter specifies whether DST is to be used in the site	Format: Decimal Range: 0 - 1 Default Value: 1 0 - Disable DST. 1 - Enable DST.
GENERAL NUMBER OF AUTHORIZATIONS	This number applies to Standard Users. An authorization limits access after a locking plan has already been created and implemented. The maximum number of authorizations is 40.	Format: Decimal Range: 1 - 40 Default Value: 40

Table 5 : Site Configuration

3.3.1 Site Configuration Example

3, 1, 4;

3.4 PDA Operators

This section outlines configuration information about the PDA operators in the order in which it appears in the CSV file.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to PDA operator details. Please refer to Section 3.4.1 for an example.	Format: Decimal Range: NA Fixed Value: 4
OPERATOR ID	The LMS generates a unique number for operators	Format: Decimal Range: 1 - 65535 Default Value: NA
OPERATOR NAME	A user defined name for individual operators	Format: String (ASCII) Range: Max 15 Characters Default Value: NA Alphanumeric characters. Note: no special characters allowed
OPERATOR LOGIN NAME	A user defined login name for individual operators	Format: String (ASCII) Range: Max 10 Characters Default Value: NA Alphanumeric characters. Note: no special characters allowed
OPERATOR PASSWORD	A user defined password for individual operators	Format: String (ASCII) Range: 6 – 12 Characters Default Value: NA Alphanumeric characters with at least 1 number. Note: no special characters allowed
OPERATOR PRIVILEGES	See below for details	Format: Binary (13 bits) Range: NA Default Value: NA

Table 6 : PDA Operators

OPERATOR PRIVILEGES

Describes the permissions and access rights for each operator
There are 13 operations on PDA application and for each; the operators may or may not have privilege.

Following are the list of privileges that an a PP operator can have

1. Initalize
2. Update/Set CM WLM timeout/Set ACU LMS Timeout/Set Wireless Operational Parameters
3. Open
4. ChangeMode
5. PowerUp
6. Diagnostics/Read Lock Cycles
7. Upload Lock Audits
8. Upload PP audits
9. WLM Diagnostics
10. Read Lock Audits/Read Debug Info
11. View Lock Audits
12. View PP Audits
13. Firmware Upgrade

If the Diagnostics/Read Lock Cycles bit is enabled then the following privileges are also set for the operator

- Battery Test
- Buzzer Test
- LED Test
- Switch Test
- View Lock Info
- Read Lock Cycles

If the WLM Diagnostics bit is enabled then the following privileges are also set for the operator

- Network Join

3.4.1 Site Configuration Example

4,1,operator1,operator1,operatorpsw,1111111111110;
4,2,operator2,operator2,operatorpsw2,1011011111110;
4,3456,operator3,operator3,operatorpsw3,1111111110000;

Note: The OPERATOR ID should be unique

3.5 DST

This section outlines configuration information about the DST in the order in which it appears in the CSV file.

Note: DST settings are applicable to all the doors

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to DST details. Please refer to Section 3.5.1 for an example.	Format: Decimal Range: NA Fixed Value: 5
DATE	DST Date	Format: mm-dd-yyyy Range: NA Default Value: NA
TIME	DST Time	Format: hh:mm Range: 00:00 – 23:59 Default Value: NA
CHANGE	This field indicates whether the DST change moves the clock forward or backward	Format: Decimal Range: 0 – 1 0 - Backward 1 - Forward Default Value: 1

Table 7 : DST Details

3.5.1 DST Example

4,1,operator1,operator1,operatorpsw,1111111111110;
4,2,operator2,operator2,operatorpsw2,1011011111110;
4,3456,operator3,operator3,operatorpsw3,1111111110000;

Note: The OPERATOR ID should be unique

3.6 Holidays

This section outlines configuration information about the Holidays in the order in which it appears in the CSV file.

Note: Holidays are applicable to all the doors.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to Holidays details. Please refer to Section 3.6.1 for examples.	Format: Decimal Range: NA Fixed Value: 6
STARTDATETIME	The date and time at which the Holiday starts	Format: MM-dd-yyyy HH:mm Range: NA Default Value: NA
ENDDATETIME	The date and time at which the Holiday ends	Format: MM-dd-yyyy HH:mm Range: NA Default Value: NA

3.6.1 Holiday Examples

3 Holiday details:

6, 09-07-2008 00:00, 09-07-2008 00:00;
6, 12-07-2008 00:00, 12-08-2008 00:00;
6, 12-17-2008 00:00, 12-17-2008 00:00;

Note: The Holiday “Start Date and Time” should be unique

3.7 Time Zone

This section outlines configuration information about the Time Zones. Each valid time zone the information is required; ‘Start time’, ‘End time’ and ‘Days of the week’. Each time zone can have up to 5 sub-time zones containing similar information.

Note: Time zones are applicable to all the doors. Each user is assigned a time zone index. If a user is given access in TIME_ZONE_ALWAYS time zone, then the user shall be able to access the lock regardless of any Time zones that are specified (user can access the lock without time restriction). If a user is given access in TIME_ZONE_NEVER time zone, then the user shall not be able to access the lock in any of the time zones.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to Time Zone details. Please refer to Section 3.7.1 for examples.	Format: Decimal Range: NA Fixed Value: 7
INDEX	The time zone index that identifies each sub-time zone to be part of the same time zone. If a time zone has 3 sub-time zones then all 3 of them would have the same time zone index.	Format: Decimal Range: 0 - 63 Default Value: NA TIME_ZONE_NEVER = 0 and TIME_ZONE_ALWAYS = 63
START TIME	The time at which the Time Zone starts	Format: hh:mm Range: 00:00 – 23:59 Default Value: NA
END TIME	The time at which the Time Zone ends	Format: hh:mm Range: 00:00 – 23:59 Default Value: NA
DAYS	Specifies which days of the week the time zone is valid. MSB bit represents Holiday and the rest represent one day of the week in the following order: Saturday, Friday, Thursday, Wednesday, Tuesday, Monday, and Sunday. If a bit is set, then the time zone is valid on that day. Example: 10111111 (BF)	Format: HEX Range: 1 - FF Default Value: NA

3.7.1 Time Zone Examples

4 Time zone details:

7,1,01:00,03:00,FF;
7,2,01:00,02:00,C0;
7,3,02:00,03:00,E0;
7,4,04:00,05:00,68;

Note: The Time Zone “Index” should be unique

3.8 Automatic Changes

This section outlines the configuration information about Automatic.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to Automatic changes details. Please refer to Section 3.81 for examples.	Format: Decimal Range: NA Fixed Value: 8
LOCK ID	The Lock ID for which the Automatic Changes are assigned	Format: HEX Range: 1-FFFFFFFF Default Value: NA
TIME	The time at which the Automatic Change starts	Format: HH:mm Range: 00:00 – 23:59 Default Value: NA
STATE	This parameter defines the Lock state- OFFICE_MODE OFFICE_FIRST_MODE, STANDARD_MODE, SECURITY_MODE, BLOCKED_MODE, EMERGENCY_LOCK, EMERGENCY_UNLOCK, FACILITY_CODE/ FOYER_MODE	Format: Decimal Range: 1 - 10 Default Value: 4 OFFICE_MODE = 1 OFFICE_FIRST_MODE =2, STANDARD_MODE = 4, BLOCKED_MODE = 7, EMERGENCY_LOCK = 8, EMERGENCY_UNLOCK = 9, FACILITY_CODE/ FOYER_MODE = 10,
DAYS	Specifies the day(s) of the week where the automatic change is valid. The MSB represents Holidays and the rest represent one day of the week in the following order; Saturday, Friday, Thursday, Wednesday, Tuesday, Monday, and Sunday. If the holiday bit is set then the automatic change is valid on a holiday. Example: 11111011(FB)	Format: HEX Range: 1 - FF Default Value: NA

Table 8: Automatic Changes

3.8.1 Automatic Changes

The following line shows 2 automatic changes details.

8, 6D12, 00:00, 04, FF;
8, 6D12, 01:00, 04, 1E;

Note: The Automatic Change “TIME” should be unique, for the given door.

3.9 User Details

This section outlines configuration information about users.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to Users details. For examples see Section 3.9.1.	Format: Decimal Range: NA Fixed Value: 9
LOCKID	The Lock ID assigned to a User. There is a single Lock ID per user record.	Format: HEX Range: 1-FFFFFFFF Default Value: NA
CARD_NUMBER	A unique identifier for each user in the system	Format: HEX Range: 1-FFFFFFFFFFFFFFFF (8 bytes) Default Value: NA
ISSUE_CODE	A number which is incremented every time a new card is created for the same user.	Format: HEX Range: 0- FFFFFFFF (4 Bytes) Default Value: NA
ACT_DATE	Activation date and time	Format: MM-dd-yyyy HH:mm Range: NA Default Value: NA [0 if no activation date is present]
DEACT_DATE	Deactivation date and time	Format: MM-dd-yyyy HH:mm Range: NA Default Value: NA [0 if no activation date is present]
OWNER/PRIVACY/ OFFICE	Owner / Office / Privacy	Format: Decimal Range: 0-1 Default Value: NA
BLOCKING OVERRIDE	Blocking override	Format: Decimal Range: 0-1 Default Value: NA
ADA	Specifies whether user is an ADA user	Format: Decimal Range: 0-1 Default Value: NA

Parameter Name	Description	Values
USER TYPE	Specifies whether user is a standard or special user. 0 – Standard 1 – Blocking 2 – Network Join 3 – Test Key 4 – Emergency Lock 5 – Emergency Unlock	Format: Decimal Range: 0-5 Default Value: NA
TIMEZONE	Time zone applicable to the particular user 0 - TIMEZONE NEVER 63 - TIMEZONE ALWAYS	Format: Decimal Range: 0-63 Default Value: NA

Table 9: User Details

3.9.1 User Details Examples

The following line shows 2 User details.

9, 6D12, 15001, 10, 12-07-2009 00:00, 12-08-2009 00:00, 1, 1, 0, 0, 63;
9, 6D12, 15002, 1, 15-07-2009 00:00, 19-09-2009 00:00, 1, 1, 0, 0, 33;

Note: The “CARD_NUMBER” should be unique, for the given door

3.10 ACF: Access Control Format

This section outlines configuration information about the Access Control Format.

Note: Maximum number of ACF details that can be present per door is 4.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to ACF details. For examples, please refer to Section 3.10.1.	Format: Decimal Range: NA Fixed Value: 10
LOCKID	The Lock ID for which the user is assigned	Format: HEX Range: 1-FFFFFFFF Default Value: NA

Parameter Name	Description	Values
PRIORITY NUMBER	Assigned by the LMS, it determines the order of the ACFs. It determines which ACF has to be used first to validate the card data	Format: Decimal Range: 1-4 Default Value:1
TYPE	Tells the lock how the type of data to interpret (Wiegand, Integra Magnetic)	Format: Decimal Range: 0-1 1 – Integra Format 0 – Wiegand Format Default Value:1
TOTALBITCOUNT	The number of bits supported in this format	Format: Decimal Range: 0-256 Default Value: NA
PARITY_TYPE	Used to check the validity of the data bits received from the Access Control Card. There are three possible parity types: PARITY_ NONE, PARITY_STANDARD, PARITY _HID1000	Format: Decimal Range: 0-2 Default Value: NA PARITY_ NONE = 0 PARITY_STANDARD = 1 PARITY _HID1000 =2
FACILITYCODE_ ACF	Value of Facility Code stored with each Access Control Card Format	Format: Decimal Range: 0-4294967295 Default Value: NA
FACILITYCODE _ STARTBITS	Start bit of the Facility Code. This field is not used in writable cards	Format: Decimal Range: 0-255 Default Value: NA
FACILITYCODE _ NBITS	Number of bits in Facility Code	Format: Decimal Range: 0-32 Default Value: NA
CARDNUMBER_ STARTBITS	Start bit of the Card Number. This field will be used as “USER_ID” in writable cards	Format: Decimal Range: 0-255 Default Value: NA
CARDNUMBER_ NBITS	Number of bits in Card Number	Format: Decimal Range: 0-64 Default Value: NA
ISSUECODE_ STARTBITS	Start bit of Issue code This field will be used as “USER_SEQUENC” in writable cards	Format: Decimal Range: 0-255 Default Value: NA

Parameter Name	Description	Values
ISSUECODE_ NBITS	Number of bits in Issue code	Format: Decimal Range: 0-32 Default Value: NA
ACT_ STARTBITS	Start bit of Activation Date and time	Format: Decimal Range: 0-215 Default Value: NA
ACT_ NBITS	Number of bits in Activation Date and time	Format: Decimal Range: 0-40 Default Value: NA
DEACT_ STARTBITS	Start bit of De-Activation Date and time	Format: Decimal Range: 0-215 Default Value: NA
DEACT_ NBITS	Number of bits in De-Activation Date and time	Format: Decimal Range: 0-40 Default Value: NA
ADA_ STARTBITS	Start bit of ADA	Format: Decimal Range: 0-215 Default Value: NA
ADA_ NBITS	Number of bits associated with the ADA attribute	Format: Decimal Range: 0-1 Default Value: NA
AUTHORIZATION _ STARTBITS	Start bit of Authorization	Format: Decimal Range: 0-215 Default Value: NA
AUTHORIZATION_ NBITS	Number of bits associated with Authorization	Format: Decimal Range: 0-40 Default Value: NA
EVEN PARITY INFO	Even Parity Information	Format: Decimal Range: 0-256 Default Value: NA
ODD PARITY INFO	Odd Parity Information	Format: Decimal Range: 0-256 Default Value: NA

Table 10: ACF Details

3.10.1 ACF Examples

3 Wiegand type ACFs and 1 Integra type ACF

10,001E,1,0,256,1,4294967295,10,32,40,64,100,24,130,40,170,40,210,1,215,40,200,200;
10,001E,2,0,200,1,7295,10,32,40,32,80,16,0,0,0,0,150,1,160,40,215,215;
10,001E,3,1;
10,001E,4,0,160,1,4294995,10,32,40,64,100,24,0,0,130,10,0,0,0,0,200,200;

Note: The “PRIORITY NUMBER” should be unique, for the given door

3.11 SCF: Smart Card Format

This section outlines configuration information about the Smart Card Format.

Note: Maximum number SFC’s per door is 4.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to SCF details. Please refer to Section 3.11.1.	Format: Decimal Range: NA Fixed Value: 11
LOCKID	The Lock ID for which the user is assigned	Format: HEX Range: 1-FFFFFFFF Default Value: NA
PRIORITY NUMBER	The LMS assigns a priority for each SCF to define the order of processing. The lock should use the load order provided by the LMS. The Format ID’s are processed in ascending order	Format: Decimal Range: 1-4 Default Value: 1
FORMAT TYPE	Based on Format Type, the Lock makes a decision on how to retrieve data from the card. A Unique number is given to each format type, this will determine the requirements of the Application location and key information	Format: Decimal Range: 0 - 1 Default Value: 1

Parameter Name	Description	Values
APPLICATION LOCATION	Application Location will specify the location of access control data in terms of book, page and application or sector and block	Format: Decimal Range: 0 - 255 Default Value: NA
APPLICATION KEY	Provides the key information to authenticate and retrieve the access control data	Format: HEX Range: 0 – FFFFFFFFFFFFFFFF (8 Bytes) Default Value: NA

Table 11: SCF Details

3.11.1 SFC Examples

The following lines show several SCF details.

11, 001E, 1, 1, 200, 987654321;
11, 001E, 2, 1, 64, 9875633452;
11, 001E, 3, 1, 100, 35235342;
11, 001E, 4, 1, 128, 6834347;

Note: The “PRIORITY NUMBER” should be unique, for the given door

3.12 Priority Events

This section outlines configuration information about Priority.

Note: Maximum number of Priority events that can be present in a door is 20.

Parameter Name	Description	Values
CONFIGURE PARAMETER	This parameter indicates that the data following this parameter corresponds to Priority Event details. Please refer to Section 3.12.1 for examples	Format: Decimal Range: NA Fixed Value: 12
LOCKID	The Lock ID for which the user is assigned	Format: HEX Range: 1-FFFFFFFF Default Value: NA
PRIORITY_EVENT_ID1	Provide the id for event 1	Format: Decimal Range: 0 - 255 Default Value: NA

Parameter Name	Description	Values
PRIORITY_EVENT_ID2	Provide the id for event 2	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID3	Provide the id for event 3	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID4	Provide the id for event 4	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID5	Provide the id for event 5	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID6	Provide the id for event 6	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID7	Provide the id for event 7	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID8	Provide the id for event 8	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID9	Provide the id for event 9	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID10	Provide the id for event 10	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID11	Provide the id for event 11	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID12	Provide the id for event 12	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID13	Provide the id for event 13	Format: Decimal Range: 0 - 255 Default Value: NA

Parameter Name	Description	Values
PRIORITY_EVENT_ID14	Provide the id for event 14	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID15	Provide the id for event 15	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID16	Provide the id for event 16	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID17	Provide the id for event 17	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID18	Provide the id for event 18	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID19	Provide the id for event 19	Format: Decimal Range: 0 - 255 Default Value: NA
PRIORITY_EVENT_ID20	Provide the id for event 20	Format: Decimal Range: 0 - 255 Default Value: NA

Table 12: Priority Events

3.12.1 Priority Events Examples

Examples with 2 different number of priority events.

20 priority events: 12, 001E, 1, 2,3,4,10,15,23,45,46,50,55,61,65,68,69,73,89,92,97,98;
2 priority events: 12, 001E, 1, 2;

Note: Priority Event ID's should be unique, for the given door

4 Portable Programmer Application Audits

The PP Application is used to configure a lock and to perform diagnostics. The application is also used to move data to and from the Lock to the LMS. There are 2 types of Audits that are recorded by the PP Application for this information transfer: PP Application Audits and Lock Audits

The PP Application records an audit for each operation performed by the user on the PDA. This information is stored in the internal PP database. The audit data can be exported to a text file in CSV format and can be uploaded to the LMS application.

The PP Application can read the audits from the lock and store them in the PP database. The data can be exported to a text file in CSV format and uploaded to the LMS application.

This document gives a brief description of the PP application audit format, lock audit format, as well as, PP and lock audit events and their description.

4.1 PP Application Audits

Each PP application audit shall contain 6 fields in the order as mentioned below

- Serial number
- Event ID
- Date time
- Lock ID
- Battery status
- Operator ID

4.1.1 PP Audit Fields

This section describes the fields in application audit section.

PP Audit ID – An integer (4 bytes), which is auto generated by the Application database to identify each Audit

Event ID – Event ID is an integer (2 bytes) to identify the event that is logged. The PP audit event ID starts with 0.

Date Time – Date and time of the event. Format: mm-dd-yyyy dd:mm:ss.

Lock ID – Lock ID is a 4 byte integer in hexadecimal format which indicates the ID of the Lock on which user has performed an operation. If a user has performed only application related operations (e.g. Load database, Login etc.), then lock ID field shall contain invalid lock ID (0).

Battery Level – Battery level field is a 1 byte integer value. For each lock related operation, the application should record the battery level of the lock. This field contains the battery level of the lock when the user has performed that particular operation. If a user has performed only application related operations (e.g. Load database, Login etc.), then the battery level field shall contain invalid battery level (-1).

Operator ID – Operator id is a 2 byte integer. The Operator ID identifies the operator who logged in to the application and performed the operations.

For Example:

2 audits for successful initialization and for battery level test would be as follows:

1,3,07-31-2008 12:00:00,6d12,81,1;2,25, 07-31-2008 12:02:00,6d12,81,1;

4.1.2 PP Audit Events

The below list shows the PP audit events and their description:

Event ID	Event Name	Description	Message Displayed in View Audits
0	LOGIN_TAMPERED	This audit shall be recorded after maximum failed login attempts (3-5) to the PP application	Login Tampered
1	LOGGED_IN_SUCCESS	This audit shall be recorded for successful login to the PP application	Login Successful
2	LOGGEDOUT_SUCCESS	This audit shall be recorded for successful logout from the PP application	Logged out Successfully
3	INITIALIZE_SUCCESS	This audit shall be recorded when lock is initialized successfully.	Lock Initialized Successfully
4	INITIALIZE_FAILED	This audit shall be recorded when lock initialization failed.	Lock Initialization Failed
5	GET_LOCK_MODE_SUCCESS	This audit shall be recorded when get lock mode operation is successful	Lock Mode Read Successfully
6	GET_MODE_FAILED	This audit shall be recorded when get lock mode operation failed.	Reading Lock Mode Failed

Event ID	Event Name	Description	Message Displayed in View Audits
7	CHANGE_LOCK_MODE	This audit shall be recorded when a change lock mode operation is successful.	Lock Mode Change is Successful
8	CHANGE_MODE_DENIED	This audit shall be recorded when a change lock mode operation is denied/failed.	Change Mode Denied
9	OPEN_LOCK_SUCCESS	This audit shall be recorded when a lock is opened successfully with open lock command. This event is also used when batteries are low and the lock is opened with power-up	Lock Opening Successful
10	OPEN_LOCK_FAILED_ EVENT_ID	This audit shall be recorded when lock opening failed with open lock command.	Lock Opening Failure
11	UPDATE_LOCK_SUCCESS_ EVT_ID	This audit shall be recorded when lock is updated successfully.	Update Lock Successful
12	UPDATE_LOCK_FAILURE_ EVT_ID	This audit shall be recorded when lock update failed.	Update Lock Failure
13	POWERUP_LOCK_SUCCESS	This audit shall be recorded when lock is powered up successfully with power up command.	Lock Power up Successful
15	CLEAR_LOCKINGPLAN_ SUCCESS_EVT_ID	This audit shall be recorded when all the lock related data is cleared successfully from the PP database.	Clear Locking Plan successful
16	CLEAR_LOCKINGPLAN_ FAILED_EVT_ID	This audit shall be recorded when clear locking plan operation failed.	Unable to clear the locking plan
17	READ_LOCK_AUDITS_ EVENT_ID	This audit shall be recorded when audits are read successfully from the lock with Read lock audits command.	Read Lock Audit Successful
18	READ_LOCK_AUDITS_ FAILURE_EVENT_ID	This audit shall be recorded when reading lock audits fails with Read lock audits command.	Read Lock Audit Failure

Event ID	Event Name	Description	Message Displayed in View Audits
19	VIEW_LOCK_AUDITS_ EVENT_ID	This audit shall be recorded when lock audits from PP application database are viewed successfully in the application.	View Lock Audits Successful
20	VIEW_LOCK_AUDITS_ FAILURE_EVENT_ID	This audit shall be recorded when view lock audits operation in PP application fails.	View Lock Audits Failure
21	SWITCH_TEST_SUCCESS_ EVENT_ID	This audit shall be recorded for the follow scenarios: 1)If switch test is started and the user opts not to press any switch or 2) switch test is started and the user press cancel button	Switch Test Successful
22	SWITCH_TEST_FAILED_ EVENT_ID	This audit shall be recorded if execution of Switch Test fails.	Switch Test Failed
23	BATTERY_LEVEL_TEST_ SUCCESS_EVENT_ID	This audit shall be recorded on successful retrieval of the battery level from lock.	Battery Level Test Successful
24	BATTERY_LEVEL_TEST_ FAILURE_EVENT_ID	This audit shall be recorded if Battery level test execution fails	Battery Level Test Failure
25	VIEW_LOCK_INFO_ SUCCESS_EVENT_ID	This audit shall be recorded on successful retrieval of the View Lock information from the lock.	View Lock Information Successful
26	VIEW_LOCK_INFO_ FAILURE_EVENT_ID	This audit shall be recorded if View lock info command execution fails	View Lock Information Failure
27	VIEW_PP_AUDITS_ SUCCESS_EVENT_ID	This audit shall be recorded when PP audits from PP application database are viewed successfully in the application.	View PP Audits Successful
28	VIEW_PP_AUDITS_ FAILURE_EVENT_ID	This audit shall be recorded when view PP audits operation in PP application fails.	View PP Audits Failure

Event ID	Event Name	Description	Message Displayed in View Audits
29	CHANGE_LANGUAGE	This audit shall be recorded when the language is changed successfully in the PP application.	Language Change Successful
31	LOAD_DATABASE_ SUCCESS	This audit shall be recorded when the PP application database is loaded successfully from the PPData CSV file.	Database Loading successful
32	LOAD_DATABASE_FAILURE	This audit shall be recorded when the PP application database fail to load from the PPData CSV file.	Failed to load the database
33	UPDATE_LOCK_CLOCK_ SUCCESS_EVT_ID	This audit shall be recorded on successful execution of Update lock clock command thereby updating the lock RTC with PP application configured time.	Update lock clock successful
34	UPDATE_LOCK_CLOCK_ FAILURE_EVT_ID	This audit shall be recorded if Update lock clock command execution fails.	Failed to update lock clock
35	UPLOAD_PPAUDITS_ SUCCESS_EVENT_ID	This audit shall be recorded when the PP audits CSV file is successfully created by the PP application from the PP database, for upload to the LMS.	Upload PP Audit Successful
36	UPLOAD_PPAUDITS_ FAILURE_EVENT_ID	This audit shall be recorded when the PP audits CSV file creation by the PP application failed.	Upload PP Audit Failure
37	UPLOAD_LOCKAUDITS_ SUCCESS_EVENT_ID	This audit shall be recorded when the lock audits CSV file is successfully created by the PP application from the PP database, for upload to the LMS.	Upload Lock Audit Successful

Event ID	Event Name	Description	Message Displayed in View Audits
38	UPLOAD_LOCKAUDITS_ FAILURE_EVENT_ID	This audit shall be recorded when the lock audits CSV file creation by the PP application failed.	Upload Lock Audit Failure
39	CHANGE_LANGUAGE_ FAILURE	This audit shall be recorded when the change language operation failed.	Unable to change the language
40	LED_TEST_FAILURE_ EVENT_ID	This audit shall be recorded if execution of LED Test fails. Failure condition can occur when there is communication break, low batteries, or timeout.	Failed to test the LED
41	LED_TEST_SUCCESS_ EVENT_ID	This audit shall be recorded on successful execution of LED Test.	LED test successful
42	BUZZER_TEST_FAILURE_ EVENT_ID	This audit shall be recorded if execution of Buzzer Test fails. Failure condition can occur when there is communication break, low batteries, or timeout.	Failed to test the BUZZER
43	BUZZER_TEST_SUCCESS_ EVENT_ID	This audit shall be recorded on successful execution of Buzzer Test. This does not mean that the Buzzer successfully worked.	BUZZER test successful
44	TEST_KEY_FAILURE_ EVENT_ID	This audit shall be recorded if execution of Test Key command fails.	Failed to initiate Test Key
45	TEST_KEY_SUCCESS_ EVENT_ID	This audit shall be recorded on successful execution of Test Key command.	Test key Successfully executed
46	NETWORKJOIN_FAILURE_ EVENT_ID	This audit shall be recorded if execution of Network Join command fails.	Network Join Failed
47	NETWORKJOIN_SUCCESS_ EVENT_ID	This audit shall be recorded on successful execution of Network Join command.	Network Join Successful
48	GET_LOCK_CLOCK_ FAILURE_EVT_ID	This audit shall be recorded when getting lock clock failed	Get lock clock Failed

Event ID	Event Name	Description	Message Displayed in View Audits
49	GET_LOCK_CLOCK_ SUCCESS_EVT_ID	This audit shall be recorded when getting lock clock operation is success.	Get lock clock Successful
52	SERIAL_PORT_ CONFIGURATION_SAVED_ FAILURE	This audit shall be recorded when serial port configurations update fails.	Serial port configuration failure
53	SERIAL_PORT_ CONFIGURATION_SAVED_ SUCCESS	This audit shall be recorded when serial port configurations update is successful.	Serial port configuration success
54	CM_FIRMWARE_ UPGRADE_FAILURE	This audit shall be recorded when ACU/CM firmware upgrade fails.	ACUCM Firmware upgrade failure
55	CM_FIRMWARE_ UPGRADE_SUCCESS	This audit shall be recorded when ACU/CM firmware upgrade is successful.	ACU/CM Firmware upgrade success
58	ICLASS_FIRMWARE_ UPGRADE_FAILURE	This audit shall be recorded when iCLASS reader upgrade fails.	ICLASS Firmware Upgrade failure
59	ICLASS_FIRMWARE_ UPGRADE_ SUCCESS	This audit shall be recorded when iCLASS reader upgrade is successful.	ICLASS Firmware Upgrade Success
60	MIFARE_FIRMWARE_ UPGRADE_FAILURE	This audit shall be recorded when MiFARE reader upgrade fails.	MIFARE Firmware Upgrade failure
61	MIFARE_FIRMWARE_ UPGRADE_ SUCCESS	This audit shall be recorded when MiFARE reader upgrade is successful.	MIFARE Firmware Upgrade Success
62	AWID_FIRMWARE_ UPGRADE_FAILURE	This audit shall be recorded when AWID reader upgrade fails.	AWID Firmware Upgrade failure
63	AWID_FIRMWARE_ UPGRADE_SUCCESS	This audit shall be recorded when AWID reader upgrade is successful.	AWID Firmware Upgrade Success

Event ID	Event Name	Description	Message Displayed in View Audits
64	WLM_FIRMWARE_ UPGRADE_FAILURE	This audit shall be recorded when WLM upgrade fails.	WLM Firmware Upgrade Failure
65	WLM_FIRMWARE_ UPGRADE_SUCCESS	This audit shall be recorded when WLM upgrade is successful.	WLM Firmware Upgrade Success
66	READ_LOCK_CYCLE_ FAILURE_EVENT_ID	This audit shall be recorded when Read Lock Cycle operation fails.	Read Lock Cycle Failure
67	READ_LOCK_CYCLE_ SUCCESS_EVENT_ID	This audit shall be recorded when Read Lock Cycle operation is successful.	Read Lock Cycle Success

Table 13: PP Audits Event List

4.2 Lock Audits

The Lock audits shall contain 7 fields in the following order:

- Serial number
- Lock ID
- Event ID
- User ID
- Sequence number
- Date time
- Old date time

4.2.1 Lock Audit Fields

This section describes the fields in application audit section.

Loc Audit ID – An integer (4 bytes), which is auto generated by the Application database to identify each Audit

Lock ID – – Lock ID is a 4 byte integer filed that shall contain the ID of the Lock on which user has performed an operation. This value shall be in hexadecimal format.

Event ID – – Event ID is an integer (2 bytes) to identify the event that is logged on the lock. Lock event IDs start with 1.

User code – A 4-byte integer value that shall uniquely identify every user in a system. This parameter shall contain the user code of the user that performed an operation in the lock. For an operation performed by the PP application this field shall contain the operator ID of the operator who performed the event. In case of automatic changes, where there is no user associated with the event, this field shall be -1.

Sequence number – A 2-byte value that indicates how many times a card has been created for a user. This value is incremented by 1 whenever a new card is created for a particular user. When a copy card is created the sequence number is not incremented.

Date time – Date and time of the event. Format MM-dd-yyyy HH:mm:ss.

Old Date time – Old date time of the Lock. This parameter shall exist only for RTC updated event (RTC_UPDATED). Format MM-dd-yyyy HH:mm:ss. For other events this parameter shall be 0.

For example:

Audit for initialization of lock by PP Application

1, 6d12, 54, 1, 0, 07-31-2008 12:00:00, 0;

4.2.2 Lock Audit Events

Event ID	Event Name	Description
1	GRANTED_ACCESS	Access Granted, (latch monitoring and door sensor not enabled)
2	GRANTED_ACCESS_DOOR_ OPENED	Access Granted and Door Opened,; used when either latch monitoring or door sensor are enabled
3	GRANTED_ACCESS_DOOR_ NOT_OPENED	Access Granted but Door Not Opened; used when either latch monitoring or door sensor are enabled.
4	EMERGENCY_OPENING	Lock opened through PP or LMS
5	DOOR_OPENED_INTERIOR	Door opened from inside; Only used when office mode is not enabled

Event ID	Event Name	Description
6	MECHANICAL_KEY_OVERRIDE	Mechanical key override
7	DEADBOLT_PROJECTED_ FROM_INSIDE	Privacy knob turned (enabled) from inside
8	DEADBOLT_WITHDRAWN_ FROM_INTERIOR	Privacy knob turned back (disabled) from inside
9	DOOR_HELD_OPEN	Alarm when door is left open; used when latch monitoring or door sensor enabled
10	DOOR_FORCED_OPEN	Alarm when door is forced open
11	CARD_NOT_ACTIVE	Card not active
12	CARD_EXPIRED	Card has expired
13	INVALID_BADGE	User information is not on the lock
14	INVALID_AUTHORIZATION	Authorization for access is missing
15	INVALID_ISSUE_CODE	Card is cancelled
16	ACCESS_DENIED_INVALID_ TIMEZONE	User is not enabled at this time/timezone.
17	ACCESS_DENIED_PRIVACY	User does not have Privacy Override privilege
18	ACCESS_DENIED_ EMERGENCY_LOCK	Lock is in Emergency Lock Mode no users allowed access
19	ACCESS_DENIED_BLOCKED	User does not have Blocked Override privilege
20	ACCESS_DENIED_LOW_ BATTERY	Door open/close failed because of low batteries
21	LOCK_UNLOCKED_UNDER_ OFFICE_FIRST	office first unlock
22	LOCK_LOCKED_UNDER_ OFFICE_FIRST	office first relock
23	LOCK_UNLOCKED_ UNDER_AFC	Lock entered AFC mode
24	LOCK_LOCKED_UNDER_AFC	End of AFC mode
25	ENTERED_STANDARD_MODE	Lock entered Standard mode

Event ID	Event Name	Description
26	ENTERED_OFFICE_FIRST_ MODE	Lock entered Office first mode
27	ENTERED_OFFICE_MODE	Lock entered Office mode
28	ENTERED_BLOCKED_MODE	Lock entered Blocked mode
29	ENTERED_EMERGENCY_LOCK	Lock entered Emergency unlock mode
30	ENTERED_EMERGENCY_ UNLOCK	Lock entered Emergency lock mode
31	ENTERED_FOYER_MODE	Lock entered Foyer mode
32	AUTOMATIC_STANDARD_ DENIED_BLOCKED_MODE	Automatic change to standard mode denied because lock is in blocked mode
33	AUTOMATIC_OFFICE_DENIED_ BLOCKED_MODE	Automatic change to office mode denied because lock is in blocked mode
34	AUTOMATIC_OFFICEFIRST_ DENIED_BLOCKED_MODE	Automatic change to office first mode denied because lock is in blocked mode
35	AUTOMATIC_FOYER_DENIED_ BLOCKED_MODE	Automatic change to foyer mode denied because lock is in blocked mode
36	AUTOMATIC_STANDARD_ DENIED_EMERGENCY_MODE	Automatic change to standard mode denied because lock is in emergency mode
37	AUTOMATIC_OFFICEFIRST_ DENIED_EMERGENCY_MODE	Automatic change to office mode denied because lock is in emergency mode
38	AUTOMATIC_OFFICE_DENIED_ EMERGENCY_MODE	Automatic change to office first mode denied because lock is in emergency mode
39	AUTOMATIC_FOYER_DENIED_ EMERGENCY_MODE	Automatic change to foyer mode denied because lock is in emergency mode
40	OFFICE_DENIED_LOW_BATTE RY	Lock cannot go to office mode due to low battery
41	UPDATE_OF_LOCK	Lock was updated
42	UPDATE_FIRMWARE_READER	Reader firmware update
43	UPDATE_FIRMWARE_CM	Lock firmware update
44	UPDATE_FIRMWARE_WLM	Radio Module Firmware Updated

Event ID	Event Name	Description
45	UPDATE_RTC	Real Time Clock Updates
46	DAYLIGHT_SAVINGS_EVENT	DST start or DST end occurred
47	LOW_BATTERY_EVENT	Lock has reached voltage level of 18%of usable range.
48	AUDIT_TRAIL_CLEARED	Recorded when audit trail is cleared
49	AUDIT_TRIAL_LIMIT	Inform LMS about audit log getting full and about to be overwritten
50	LOCK_POWER_UP_PP	Recorded after power up by Portable programmer
51	INITIALIZATION_OF_LOCK_ BY_PP	Lock initialized through PP Application
52	DOOR_HELD_OPEN_ RESTORED	Clear state to Door Held Open
53	DOOR_FORCED_OPEN_ RESTORED	Clear state to Door Forced Open
54	LOW_BATTERY_EVENT_R ESTORED	Clear state to Low Battery Event
ACF Events		
52	ACF_INVALID_DATA	Failed to Process Integra Card Data
53	ACF_INVALID_FACILITY_CODE	Facility Code for selected ACF did not match facility code retrieved from the card
54	ACF_INVALID_PARITY	Parity Calculations for retrieved data failed for Selected ACF
55	ACF_INVALID_DATA_LENGTH	Length of retrieved data did not match length specified in selected ACF
56	ACF_INVALID_TYPE	The type of retrieved data (Wiegand/Integra) did not match ACF Type
57	ACF_NOT_FOUND	No ACFs stored at the lock.

Event ID	Event Name	Description
SCF Events		
58	SCF_INVALID_DATA	Invalid header, invalid data length, filed to retrieve HID App data...
59	SCF_INVALID_ AUTHENTICATION	Failed to authenticate to Application specified by selected SCF
60	SCF_INVALID_LOCATION	Application Data could not be located on the card based on selected SCF
61	SCF_INVALID_CARD	Either card was not found in the field, or a card failed to respond to the requested RF protocol.
62	SCF_NOT_FOUND	No SCFs stored at the lock

Table 14: Lock Audits Event List