	The GPP ini File Explained J. Gleave

Introduction

This document details all GuardPointPro.ini file entries for the GuardPoint Pro version 2.3. Most of these entries are included in the “Tools>Options” screens of the application but these screens do not contain all of them.

If changes are made to entries in the “Tools>Options” screens, then, on clicking OK, the GuardPointPro.ini file is re-built according to the current definitions.

To change any entry of the GuardPointPro.ini file, open the GuardPointPro.ini file located in the GuardPoint Pro folder, with Notepad. The GuardPointPro.ini file is structured in categories, indicated with ‘[ ]’ symbols. Search for the required entry in the corresponding category.

Unless additional values are specified, setting an option is done by manually setting the value of the corresponding entry to ‘1’ and disabling an option is done by setting the value to ‘0’. When all changes are done, save the GuardPointPro.ini file and restart GuardPoint Pro.

Note: Changes are only recognized after restarting GuardPoint Pro, as the GuardPointPro.ini file is only read at program start.

GuardPointPro.ini entries

[Background]

- **Background File Name**: Graphic file of application background; the file should be located in the application folder.
- **Background Stretch**: if =1, the application background image is stretched.

[Database]

- **DbsFolder**: Full path of main application folder on GuardPoint Pro server machine.
- **DBType**: if =1, the application database is MS-Access type, if =2, the database is MS-SQL type (required SQL module on the dongle).
- **SQL_Connect**: Connection string to main SQL database
- **SQL_Connect_Backup**: Connection string to alternative SQL database (see also the notes regarding the entries *AutoFailover, SwapPrimaryDB* and *ServerRedundancy*).

- **SQLRestoreTimeout**: 600sec by default (range 0-60000). Time out (seconds) when attempting to restore a saved SQL database under GuardPoint Pro from .bak file or when deleting old events. Note that the default value of 600 (i.e., 10 minutes) is not enough when the history contains more 700k events (approx.).
- **DatabaseTimeout**: 0sec by default (range 0-60000). Timeout used when executing view queries into SQL. If =0, GuardPoint Pro waits for the end of the query execution without time limit.
- **AutoFailover**: if =1, when connection to the main database is lost, GuardPoint Pro automatically switches to the alternative SQL database.
- **SwapPrimaryDB**: 5min by default (range 1-1440). Frequency (in minutes) in which GuardPoint Pro checks whether the main database is operational again when the alternative SQL database defined at SQL_Connect_Backup option is in use.
- **WaitDBcancel**: if =1, the 'Cancel' button is displayed on the little screen which appears when the database is not found or when the workstation cannot see the server. Since these screens wait for the database or the server, clicking ‘Cancel’ in fact prevents the application from starting. So setting this entry to 0 avoids user mistake on sites where the auto start of GuardPoint Pro is critical.
- **NetHasp**: if =1, the license dongle is of special kind (called ‘NetHasp’, its physical color is red) that may be installed on any PC on the LAN. That PC should run the Aladdin utility ‘License Manager’. Such dongle can be used, for instance, in Terminal-Server environment. On such environment users may run GuardPoint Pro each time from a different terminal client while leaving the dongle connected to one specific machine.
- **SQLServerDateFormat**: Date/time format (i.e. yyyy\-mm\-dd hh\:nn\:ss) to use when saving date related records in the SQL database. SQL date/time settings may be different according to Windows regional settings and/or user preferences during SQL Server installation. User should edit the value of this entry according to the format used on their SQL Server. Consult the system SQL administrator. This entry is used when the entry MotorComNet=0 only.
- **SQLServerDateFormatNet**: Same as above when the entry MotorComNet=1.

[Communications]

- **IsWS**: if =1, GuardPoint Pro works as Workstation. If =0, GuardPoint Proworks as Server.
- **myServerName**: PC name of the server to which this workstation belongs. This entry is mandatory for workstations when using GuardPoint Pro in a MultiServer/MultiPolling installation in Multi Site installation (when the entries MultiSite=1).
- **DontCreateConf**: if =1, GuardPoint Pro does NOT recreate the Spread configuration file (Spread.conf) on each startup. If =0, this file is re-built at startup with the data defined in the Computer screen.
- **SpreadDeamon**: =4803@localhost, by default. This option uses the centralized spread, a way that allows multiple PCs to connect to a single Spread instance (deamon), by using a single executable 'spread.exe' (i.e. spread application located on the server), thus avoiding communication difficulties between GuardPoint Pro server and its workstations (due to firewalls, anti-virus, or when the remote computers are only allowed to be connected to the server but not to each other,etc.). 4803 is the port used and localhost is the current PC, that can be changed either with IP address of the PC or with the PC name

(i.e.4803@192.168.168.141 or 4803@SERVER). The Centralized spread configuration is described in the document '10TE512 Connecting multiple computers to a single Spread deamon'.

- **SpreadDeamonBackup**: Same option than SpreadDeamon for using the Centralized Spread with environment of redundant servers, i.e. this option defines the 'SpreadDeamon' option of the Redundant Server. For example: SpreadDeamonBackup=4803@<NAME_OF_REDUNDANT_SERVER>. Then, when workstations do not succeed to connect to the Main Server Spread and if the delay before swapping to the Redundant Server is reached, the workstations try to connect to the second server. When the Main Server is started, they try to connect to the Main Server again. Note that the 'Spread.conf' file should contain both servers (and should be the same in both servers). In addition, the ini option 'DontCreateConf=1' should be set on both servers.
- **SpreadDeamonWaitBeforeSwapSec**: 60, by default. When using the option 'SpreadDeamonBackup', delay in seconds before swapping to the Redundant Server.
- **SpreadTestEvery:** 60sec by default (range 1-3600). Frequency (in seconds) in which the Server/Workstation checks its connection to the Spread daemon. If the connection fails, it signals a flag that communication had failed. If this is a Workstation, once TestMinute function is called, it brings up a modal screen, which displays that the server is disconnected. In all cases if connection is lost, AME message appears. The option 'SpreadReconnect' does not influence the functionality of this feature.
- **SpreadTestTimeout**: 5sec by default (range 1-3600). Timeout (in seconds) in which the Server/Workstation checks its connection to the Spread daemon. Server/Workstation sends Server with Daemon a "Hi" message and waits for a "Bye" answer.
- **SpreadMulticast**: if =239.0.0.60:4803, the broadcast mode of the Spread is disabled. By default, this entry is empty allowing the Spread working on the Spread_Segment defined at the Subnet Mask field of the Computer screen. If filled, this entry should be filled for all PC of the installation. The advantage of using Multicast on broadcast was due to the fact that on certain system Tibbo would get confused from the broadcast communication.
- **SpreadGroup**: Virtual PC name for 'Cluster' environment. By default, this entry is empty. When one or more PC are seen from the outside world as one virtual PC (i.e. ADMIN), the Computer screen should contain the name of all the PC including the virtual PC (it requires a Workstation license for each one in GuardPoint Pro dongle). In addition, on each PC, this entry should have the name of the virtual PC (i.e. SpreadGroup = ADMIN).
- **CloseSpreadonExit**: = 1 by default, for kill the spread.exe process on application exit.
- **DoPolling**: = 1 by default, for starting controllers polling on application start.
- **NbRetry**: 3 by default (range 0-10). Number of retries to resend the data in case the controller does not answer to a command. Either polling or data download.
- **GAPNbRetry**: 3 by default (range 0-10). Number of times to resend the Global Anti Passback commands. When Global Anti Passback is managed by the application (i.e., when entry GlobalAPBwoPC=0), controllers does not answer to the Global Anti Passback commands because these commands are broadcasted.

- **Daily Program 4 Zones**: if =1, each daily program can have up to 4 active ('green') periods. If =0, up to 2 active periods only.
- **SpecialDays**: if =1, application has three holiday types: Holiday, Special Day 1, Special Day 2. Weekly programs consist of 7 weekdays + holiday + two special days. If =0, only one holiday type.
- **Show Commands**: if =1, the commands to the controller(s) are shown on the main screen event log.
- **ComErrorSeconds**: 30sec by default (range 1-300). Duration (seconds) since the first detection of communication error with a controller till changing the polling icon on the main toolbar to red X.
- **Com_PollingPriorityDuringDownload**: 1 by default (range 1-10). Number of polling commands sent between two definition parameters commands. Obviously, the definitions download process slows down as much as the value is higher. To ensure at least one polling command to each controller between two download commands, the value should be equal to the number of controllers in the largest controller network in the system, if not refreshing input/output status in the background (i.e., when entry NoIO=1). If refreshing IO status (i.e., when entry NoIO=0), multiply this value by 3.
- **Com_DownloadEmployeeDuringProcessing**: if=1, on controller initialization, downloading all cardholders' definitions starts, simultaneously whilst preparing the commands in the PC RAM. If =0, updating the controllers starts only after preparing all the commands in the PC RAM.
- **MotorComNet**: if =1, the communication DLL file (UC.dll) developed on VB.NET is used allowing to free GuardPoint ProGUI even during heavy communication consuming operations such as: importing large HR files, controllers initializations, reading thousands of events. Also GuardPoint Pro can start normally and run freely while many controllers are not communicating at all (supported only with VB.NET enhancement using the setup file: UCDotNet_Setup.exe). Please contact us before setting this entry.
- **MotorComDebugLevel**: if =1 or 3, when the entry MotorComNet=1, debug information is written on the DBMON.exe application (the value '3' is the highest level). If =0, no information is written.
- **Graphic+**: if=1, support for Graphic plus module (required G+ on dongle or in DEMO mode, Microsoft .Net framework and G+ setup file: graphic_plus_setup.exe).
- **EventModeKeepAliveYesNo**: if =1, GuardPoint Pro will close and reopen the communication port used for second Alarm Priority buses, with the frequency specified at EventModeKeepAlive entry. This is especially important when the connection is TCP, since the TCP socket might be shut down automatically after a certain period of communication silence.
- **EventModeKeepAlive**: 60sec by default (range 1-300). Frequency (in seconds) in which to close & reopen the communication port for second Alarm Priority busses, when the entry EventModeKeepAliveYesNo=1.
- **SwapBackDelay**: 5min by default (range 1-1440). Frequency (in minutes) in which GuardPoint Pro checks whether the main bus is back to live when a second bus is used as a redundant communication bus. After a communication error on the main bus, GuardPoint Pro swaps immediately to the second bus and waits this delay to check via which bus it can talk to more controllers.

- **Minilock**: if =1, support for Minilock controllers (relay commands are sent with command 10 instead of command 40). It is recommended to use only if one of the controllers is Minilock. In this case, do not use '4 states' inputs and set the entry OldRelayCmd=1.
- **Resent Definition on Deny**: if =1, when a cardholder is denied, GuardPoint Pro immediately downloads his/her definition to the controller. During controller initialization, some cardholders can be denied. By sending immediately updates to the controller, another pass attempt would be successful.
- **NoIO**: if =1, automatic refresh of the inputs/outputs status is disabled in the Active Alarm screen in order to save controller communication time. This setting is recommended in large installations. Manual refresh is still possible with the 'Refresh' button on the Active Alarm screen toolbar.
- **Lift per Reader**: if =1, the screen 'Lift Authorization Group' is enabled, allowing to define different Lift Program for each reader of a same Lift controllers. If =0, cardholder can only activate one 'Lift Program' for a Lift controller, no matter which one of its readers he used.
- **DoorOpenByMinute**: Future use. Not supported by hardware yet.
- **OldRelayCmd**: if =1, support for old controllers (having firmware before the year 2000). It is recommended to use only if one of the controllers is old. Please contact us before setting this entry. When this entry is set, old relay commands are sent (10 instead of 40), no special days commands (76) and no crisis level commands (0E) are sent, new 'Input Group' actions are not supported.
- **RelayAsync**: if =1, when using actions for activating relays, no feedback is expected, thus preventing the possibility to stuck the application when two or more operations involving communication take place simultaneously. E.g., 'Activate relay' during Cardholder Import.
- **RelayAsyncImmediate**: if =1, any relay command is executed almost immediately, right after the current command, instead of after all the existing commands of the operational queue (e.g., initializing a controller with thousands of cardholders). This setting ensures the immediate execution of the relay action, but contain the risk of inverting the designed order. E.g., when a process contains two successive actions: 'relay on' then 'relay off', the program might randomly reverse the order and leave the relay on. Therefore, if the order is critical, this entry should be disabled.
- **ResetTibbo**: if =1, when one or more controllers using TCP networks do not answer, GuardPoint Pro sends a reset command to the Tibbo TCP converter.
- **Resend Pendings**: 30min by default (range 1-1440). Frequency (in minutes) of sending the pending commands to controllers. The pending commands are commands that were not received by controllers due to communication error or other problems.
- **Validation Cardholders**: 30min by default (range 1-1440). Frequency (in minutes) when GuardPoint Pro scans the cardholder database to see whether there are cardholders that need to be added/deleted from controllers in accordance with cardholders' time related definitions (From date / To date / Scheduled AG / Exceptions).

- **WaitFirstPing**: 5sec by default (range 1-254). Duration (in seconds) from the first detection of communication problems till testing the TCP socket via PING command, when one or more controllers using TCP networks do not answer. If the PING fails, GuardPoint Pro won't try to reach to the controller itself.
- **WaitNextPing**: 20sec by default (range 2-300). Duration (in seconds) between PING commands, when one or more controllers using TCP networks do not answer and when TCP socket did not answer to the first PING.
- **Ping Timeout**: 1000ms by default (range 50-60000). Timeout (in milliseconds) in which GuardPoint Pro waits for an answer to a PING command, when one or more controllers using TCP networks do not answer.
- **Controller Second**: if =1, all events reported by controllers include also seconds (controllers need to be initialized after changing the value of this entry). Supported by controllers having firmware later than 01/06/2004. Not supported by NSL controllers.
- **AlarmZones**: if =1, support for allocating weekly program to input groups. An option to select input groups is displayed in the 'Event handling program>Alarms' screen. In case of conflict, the individual input weekly program definition prevails. This entry should be set to '1' when using 'Input Group Activation/Deactivation during…' actions and/or Terminal reader.
- **ControllerInputGroup**: if =1, support for Input Group commands (43). This entry should be set to '1' when using 'Input Group Activation/Deactivation during…' actions and/or Terminal reader.
- **SkipCheckTables**: if =1, will not check if the database should be updated at the application start. This option is not recommended. Please contact us before setting this entry.
- **Refresh IO Period**: 500ms by default (range 0-60000). Frequency (in milliseconds) of refreshing the inputs/outputs status, when the entry NoIO=0.
- **SleepingDelay**: 2ms by default (range 1-5). Minimum duration (in milliseconds) between sending of two successive commands. This entry affects the whole communication process thus should not exceed a value of about 3ms (unless directed otherwise by the manufacturer). Note that the 'Waiting Delay' option in the 'Controller Network' screen, defines the delay between two polling commands (including refresh input/output status) for each individual controller network, while this entry concerns both polling / refresh I/O as well as other commands for the whole system.
- **Allow57k**: if =1, allow using the baud rates: 57600 and 115200 bps. Note that these baud rates are supported on all MEGA and on TPL controllers having firmware version dated 02/07/04 and later.
- **Baud Rate**: 1 by default (range 0-5). Controller communication baud rate (0 for 4800; 1 for 9600; 2 for 19200; 3 for 38400; 4 for 57600; 5 for 115200).
- **Baud Rate Biometrics**: 3 by default (range 0-5). Biometrics reader communication baud rate (0 for 4800; 1 for 9600; 2 for 19200; 3 for 38400; 4 for 57600; 5 for 115200).
- **BiometricOptimize**: if =1, fingerprints are sent only to the relevant biometrics readers according to the access group definitions. If =0, all the fingerprints are sent to all active biometrics readers.
- **BioCreateBadge**: if =1, card is automatically created and allocated to the relevant cardholder during fingerprint enrollement.

- **DisableDesign**: if =1, report layouts designing is disabled (the ‘design’ tab of the report preview is hidden).
- **WoSetBaudRate**: if =1, GuardPoint Pro never sends a command to switch to the current baud rate, when creating a new controller or when activating a non-active one.
- **doLockOnDoEvents**: Used for debbugging. If =1, the function SendCardholder1 will be locked for reentrant through DoEvents.
- **countDepthDoEvents**: Used for debbugging. When >0, all over the application DoEvents will be in depth allowed (calling DoEvents in Doevents) of countDepthDoEvents.
- **DoPauseonReportViewer**: 0 by default (range: 0 - 5). Delay of the little pause before previewing a report in order to let the application the time to fill all the data in the report before editing, avoiding some missing data (e.g. Total hours in Time and Attendance report).

[Parking]

- **Auto Reset**: if =1, all the parking lots are automatically cleared at the time given by the entries ‘Reset Hour’ and ‘Reset Minute’.
- **Reset Hour**: 0 by default (range 0-23). Hour of the parking lots auto reset, when the entry Auto Reset=1.
- **Reset Minute**: 0 by default (range 0-59). Minute of the parking lots auto reset, when the entry Auto Reset=1.

[Log]

- **View Log Windows At Startup**: if =1, the real time event log is shown on the application main screen on GuardPoint Pro start.
- **Log Windows Height**: Height of the real-time event log window.
- **Log Windows Width**: Width of the real-time event log window.
- **Log Windows Top**: Top position of the real-time event log window on the main screen.
- **Log Windows Left**: Left position of the real-time event log window on the main screen.
- **NewLog**: if =1, the event log runs as Rich log, RTF text allowing to show camera icons for relevant event and right click options. However, copying text is not possible. If =0, the event log runs as Simple log, a simple text allowing copying with [Ctrl]+[C] keys.
- **ScrollLogs**: if =1, after writing new event, the event log cursor returns to its previous location in the log text allowing the user to read the log text while getting new events. If =0, the event log cursor auto jumps to the end of the log text every time a new event is received.
- **LogScrollControl**: if =1, a control button is displayed just above the top left side of the event log window allowing to set on/off scrolling of the event log. Note that the entry ScrollLogs controls the default scroll status on application start only.
- **LogInsertEventsControl**: if =1, a control button is displayed just above the top right side of the event log window allowing to set on/off displaying newly received events on the event log.

- **2Logs**: if =1, the event log window is divided into two windows: one for access events, the other for alarms instead of having both access & alarm events on the same window.
- **LogOptimized**: if =1, newly received events are not added at the end of the log text but wherever the cursor is, allowing to save processing time when a large amount of events is received in a very short time. However, it may be confusing to the user: if clicking in the middle of the log text when new event is coming, the data is written in the middle, thus 'pushing' the half of the old text downwards. Therefore this value is suggested only on unmanned PCs.
- **LogCleanFrequency**: 100 events by default (range 10-5000). Frequency (in transactions number) in which GuardPoint Pro checks for event log clean up. By default each 100 transactions, the application checks if the log text has reached the maximum value specified for the entry LogMaxCharacters (if the entry NewLog=0) or LogMaxLines (if the entry NewLog=1). Note that reducing this value can have a negative effect on the application performance.
- **LogMaxCharacters**: 100000 by default (range 3000-450000). If the entry NewLog=0, maximum number of characters stored in the event log (1 event is about 100 characters). At each LogCleanFrequency, if the LogMaxCharacters is reached, all the transactions are deleted from the log except a number of characters equals to LogMaxCharacters. The most recent characters are kept.
- **LogMaxLines**: 1000 by default (range 100-5000). If the entry NewLog=1, maximum number of lines stored in the event log. At each LogCleanFrequency, if the LogMaxLines is reached, all the transactions are deleted from the log except a number of lines equals to LogMaxLines. The most recent lines are kept.
- **DisplayAndSaveOnlyGrantWithPin**: if =1, Access Granted events are stored and displayed on the log screen only if the cardholder has presented both badge+PIN code. The reader definition should have the options 'With Card AND Keypad' and 'Door Controlled'.
- **Process_DisplayImageAndText**: if =1, when adding process buttons to the main toolbar, the process name is displayed next to the icon. If =0, the process name is not displayed allowing more place on the toolbar. The tool tip text of the button contains the process name or the process description when it is filled.

[ActiveAlarm]

- **ActiveAlarm_IconWithoutLabel**: if =1, when the entry Graphic+=0, icons on the active alarm maps are shown with text label containing their name. If =0, icons are shown without any text label.
- **ActiveAlarm_IconSize**: if =16, when the entry Graphic+=0, icons size on the active alarm maps is 16X16 pixels. If =32, icons size is 32X32 pixels.
- **BalloonToolTips**: if =1, when the entry Graphic+=0, balloon shaped tool tips are shown when moving the mouse over the icons on the active alarm map.
- **AlarmSoundInterval**: 25sec by default (range 0-3600). Duration (in seconds) between sounds of "OnAlarm.wav". If =0, there would be not sound in case of alarm.

[Time and Attendance]

- **TA+**: if=1, support for Time&Attendance plus module (required T+ on dongle or in DEMO mode).
- **TA_Correction**: Maximum delay (in seconds). In Time & Attendance plus module (i.e., when entry TA+=1), if two successive transactions are from the same reader and the same cardholder, only the second one will be taken into account (i.e. the first one will be ignored) if the delay between the two transactions is less than this 'correction' delay. This feature allows a cardholder to immediately re-punch if he discovers that his first transaction was wrong.
- **TA_LateArrivalCountBeforeShift**: if=1, in Time & Attendance plus module (i.e., when entry TA+=1), the report of late arrival cardholders (i.e. arrived later than the scheduled entrance time (+ the grace delay) in their Personal Contract) will also include cardholders who arrived before their scheduled entrance time, leaved and then came back later than the start of their shift.
- **TA_MaxGraceInMinutes**: 20min by default (range 0-1440). Maximum value (in minutes) allowed for the Grace period when creating Daily Shift in Time & Attendance plus module (i.e., when entry TA+=1).
- **TA_useLOG**: Set by default. If=1, when opening the Time and Attendance screen, the cardholder list and the reader list is filled following to the existing events in the Journal. If=0, when opening the Time and Attendance screen, the reader list is filled with all the readers of the database. This last value improves the speed of screen opening.

[Language]

- **Language**: Application language. The available values are ARA (Arabic), CAT (Catalan), CL (Spanish-Chile), DEU (German), EN (English), ES (Spanish-Spain), FIN (Finnish), FR (French), GRK (Greek), HEB (Hebrew), HGR (Hungarian), ITA (Italian), KOR (Korean) (Not translated yet), NL (Dutch), PL (Polish), POR (Portuguese), RU (Russian), SIC (Chinese simplified), SK (Slovak), SWE (Swedish), TUR (Turkish).

[Font]

- **FontName**: Application font
- **CharSet**: The character set relevant for the selected language. It is needed since the application menu does not use Unicode. The available values are 0 (ENGLISH, FRENCH), 136 (CHINESE), 161 (GREEK), 162 (TURKISH), 163 (VIETNAMESE), 177 (HEBREW), 178 (ARABIC), 186 (BALTIC), 204 (RUSSIAN), 222 (THAI), 238 (EASTEUROPE). Windows should have the local regional settings set as default.

[General]

- **SoftwareDongle**: If=1, the license is held in secure software file. If=0, the software runs with physical dongle.
- **KeepAliveEvery**: 5ms by default (range 1-1440). Frequency (in minutes) in which GuardPoint Pro writes "KeepAlive" in the AME file. In addition, in Multi Site installation (when the entries MultiSite=1), at this interval, the server also writes in the

database that it is currently running for updating the Diagnostic screen (text reported that the server was alive at <date and time of last keep Alive>).

- **CheckBackupEVTEvery**: Frequency (in minutes) in which the server treats the BackupEVT files if any. These files are temporary files where events are stored in case of database disconnection. In addition, these files are also treated at each application startup and every day at 00:05.
- **FileSavingFormat**: Date format (i.e. ddmmmyyyy) to use for AME, database and Journal files name.
- **CloseWithoutMessage**: if =1, when closing the application, no confirmation message is displayed.
- **NoMessageBox**: if =1, all GuardPoint Pro messages that usually wait for user click on OK button are disabled in order to prevent these messages from blocking the application, when the application server is configured to run as a Windows service. This option must be set ONLY on a server that runs the application as service, without any user interface.
- **PassPass: if =1,** a checkbox 'Pass Everywhere' appears in the Cardholders screen, allowing to give access (i.e. for fire fighters) on all the doors (not depending on Access Group, Exceptions, Schedule AG). Only the Validation option is stronger. In Multi Company/Multi Site applications, only 'Super users' can see this checkbox.
- **ImportParamInSQL**: if =1, the application reads the translation strings from the Param.mdb file upon each startup. If =0, the application does not read it, saving 10-20 seconds when starting. In this case, if modifications were made to the translation or after updating the application, the modified/new strings are not updated into the system.
- **Multi Company**: if =1, support for Multi Company application (required M on dongle).
- **MultiSite**: if =1, support for Multi Site application (required xMS on dongle). Note that it works only with database SQL type (DBType=2) and with Multiple access groups (ForceMultipleAG=1).
- **SQLReplication**: if =1, in Multi Site installation (when the entries MultiSite=1) the SQL database is replicated and the application knows that the data sent to the other servers could have a latency.
- **CheckQueueMSGEvery**: 60sec by default (range 0-3600). Frequency (in seconds) in which the GuardPoint Pro server checks in the database table called Qu eueMSG if it has received some transactions from other servers, in Multi Site installation (when the entries MultiSite=1).
- **QueueMsgTOP**: 80 by default (range 10-500). Number of transactions to read in QueueMSG table in 'QueueMsgMaxTimeProcessing' seconds at each iteration defined by 'QueueMsgLoadInterval', in Multi Site installation (when the entries MultiSite=1).
- **QueueMsgLoadInterval**: 8sec by default (range 1-60). Pause (in seconds) until the next iteration, when there are pending transaction in the QueueMSG table, in Multi Site installation (when the entries MultiSite=1). If there are no pending transaction , the next iteration will occur by the value set in 'CheckQueueMSGEvery' option.
- **QueueMsgMaxTimeProcessing**: 1sec by default (range 1-10). Maximum number of seconds to allow processing the QueueMSG table at each iteration defined by 'QueueMsgLoadInterval', in Multi Site installation (when the entries MultiSite=1).
- **DebugMSMQSend**: if =1, the GuardPoint Pro server writes in AME files all messages sent to the other servers, in Multi Site installation (when the entries MultiSite=1).

- **DebugMSMQRecv**: if =1, the GuardPoint Pro server writes in AME files all messages received from the other servers, in Multi Site installation (when the entries MultiSite=1).
- **HelpFile**: For special projects only. File name of a customized help file in .pdf format to open by clicking on "Help" menu. The .pdf file should have been set into the application folder previously. Note that PDF reader must be installed in order to open a PDF file.
- **woColMemNum**: if =1, at the startup the application does not upload the cardholders' details to PC RAM. This setting can save a lot of time in GuardPoint Pro startup, especially when using DynamicNumBadge option.
- **CardholderLoadOnSearch**: if =1, the Cardholder screen opens directly in "Search" mode, like when the "Search" button is clicked.
- **CardholderSelectTop**: Maximal number of cardholders (the first ones) to display in the Cardholder screen. This setting can save a lot of time in this screen when a lot of cardholders are managed. If =0, all the cardholders are displayed. Note that in case of search, only the first found cardholders are displayed if the result reaches the maximal value.
- **ReportFolder**: Full path of the report folder. If nothing is specified, GuardPoint Pro(server or workstation) uses the default folder 'Reports' under the server application folder.
- **ReportShowDeleted**: if =1, 'Door Pass' report shows also events from deleted cardholders and 'All Cardholders' report shows also the details of deleted cardholders. These reports can be filtered according to deleted people or not.
- **FileChecker**: Not used.
- **ShowErrors**: if =1, errors that application receives from Windows and which are generally saved in the AME file are displayed on main screen log (in addition to writing them on the AME file).
- **Region**: For special projects only.
- **isPollingToFile**: Option for placing within files all events waiting to be processed by GuardPoint Pro in order to preserve the controller buffers against loss of data due to a server crash or due to a restart operation during event uploading. The buffer files are located into the folder '\polEvt'.
- **doSavePollingFiles**: When the entry 'IsPollingToFile=1', option for saving the files after treatment into the folder '\polEvt\Done' in separate folders per day and per hour (if =0, the files are deleted after treatment).
- **sendCtlWithPriority**: Option to set up a priority order in the controllers download. For each controller, the field (sendPriority) in the Controller table in the database should be set with a priority number (0 - 9999). The higher is the number, the greater is the priority. Note that special priority number '9999' is reserved for adding a second queue of download. In this case, the commands are sent alternatively to controllers having '9999' as priority number and to the other controllers from the regular queue.
- **sendMaxCrdHcommandsPriorityAtOnce**: When the entry 'sendCtlWithPriority=1', option to send more than one command in '9999' queue, at each timer (up to 3, default is 1).
- **sendMaxCrdHcommandsRegularAtOnce**: When the entry 'sendCtlWithPriority=1', option to send more than one command in regular queue, at each timer (up to 3, default is 1).

[Cardholder / Visitor]

- **AllowDuplicateName**: if =1, GuardPoint Pro allows saving people having the same first & last name. In this mode cardholders' names are displayed along with their 'Number' (as typed in Number field on the cardholder screen). Therefore, in order to force the duplicates to have a unique Number, it is recommended to set the option CardholdersNumberUnique.
- **SavePhotoByField**: Option for saving the captured photos with specific file name. If="Num", the cardholder photo files will have the cardholder Number as file name. If="ID" it will be the cardholder ID as defined in the database. If empty, the file name is "photo" & cardholder ID & "_" & Cardholder Last Name. Note that "Num" only works if the option CardholdersNumberUnique=1.
- **CardholdersEraseMsg**: if =1, when deleting a cardholder, a confirmation message "Do you want to delete?" is displayed.
- **CardholdersNumberUnique**: if =1, when creating new cardholders, the system forces the user to enter a unique value in the Number field on the cardholder screen.
- **CardholderDefaultAccessGroup**: Default Access Group allocated automatically at Cardholder creation (i.e. CardholderDefaultAccessGroup = Anytime Anywhere). Note that if the Access Group does not exist, a message is written in the AME file.
- **DepartmentAG**: If = 1 (set by default), Department screen allows Access Group/s to be defined as the default for new cardholders being assigned that Department. Note that this feature is not available when using simple Access Groups (when the INI entries "MultiSite=0" and "ForceMultipleAG=0"). This option is stronger than the entries 'VisitorDefaultAccessGroup' and 'CardholderDefaultAccessGroup'. This feature is stronger than the option 'Also for Visitor screen' in the Access Group screen.
- **ForceMultipleAG**: if =1, the user is forced to work with Multiple access groups only. In addition, if Simple access groups were allocated to existing cardholders, they are automatically transformed into Multiple access groups at application startup.
- **CardholderDefaultBadgePrintingLayout**: Default Badge printing layout allocated automatically at Cardholder creation (i.e. CardholderDefaultBadgePrintingLayout = badge1.rpx).
- **VisitorDefaultAccessGroup**: Same option as 'CardholderDefaultAccessGroup' at Visitor creation.
- **VisitorDefaultBadgePrintingLayout**: Same option as 'CardholderDefaultBadgePrintingLayout' at Visitor creation.
- **VisitorEndDay**: Default end time allocated automatically at Visitor creation (i.e. VisitorEndDay = 17:00). The card will be valid during the day of its creation, till the max. 30 minutes (by default) after the hour/minute specified at this entry hour.
- **CardholderSpecialSearch**: if =1, the Search function in the Cardholder screen allows searching on special characters, like the Turkish character <İ>.
- **MinCardholders**: 1 by default (range 1-266000). Minimum value for the NumBadge, the cardholder unique index on the controller(s) memory. When giving a card to a cardholder, a new NumBadge (last given value + 1) is allocated to him. The cardholder NumBadge can be seen on the lower right corner of cardholder screen when pressing Shift+F12. By default, the minimum value is 1 and it should not be changed in standard installations. Only in Multi Site installations, where two or more

polling servers are used, this entry (and MaxCardholders) allows to allocate each server with a different array of cardholders' indexes (E.g. Server 1: from 1 to 1000, Server 2: from 1001 to 2000, etc…)

- **MaxCardholders**: 5000 by default (range 1-266000). Minimum value for the NumBadge (see explanation for MinCardholders). The value should be equal to the highest allowed NumBadge of the controller. For example, the highest NumBadge allowed for TPL with 128K RAM is 6552 (with 4 doors) or 8934 (with 2 doors). The TPL with 512k RAM can accept up to NumBadge of 32760 (with 4 doors) or 44760 (with 2 doors). If controllers have different RAM sizes, this entry should match the highest NumBadge on the lowest RAM controller. When all the available NumBadge are occupied (i.e., according to the limits as defined by MinCardholders & MaxCardholders) GuardPoint Pro gives the error message: "Controller Memory Full".
- **DynamicNumBadge**: if =1, each controller may have different NumBadge (cardholder unique index on the controller memory) for a same cardholder, allowing controller memory optimization. NumBadge array of each controller is based only on known cardholders according to their access group. If =0, NumBadge array is the same for all the controllers in the system. Example: in a system of 20k cardholders, one of the controllers needs to grant access just two cardholders – the ones that was last to be added to the system. If DynamicNumBadge=0, their NumBadge would be 19999 & 20000 (which means a TPL with 128K RAM cannot accept them). If DynamicNumBadge=1, their NumBadge on this controller would be 1 & 2. Note that Global Anti Passback is not supported when DynamicNumBadge=1.
- **Timeout Log Off**: Range 0-1440. Duration (in minutes) after which GuardPoint Pro automatically logs off. The program continues to work in the background. If =0, there is no automatic log off (highly recommended when performing long server procedures, like cardholders import, controller initialization, etc.).
- **Automatic Inhibition**: 0day by default (range 0-365). Duration (in days) after which GuardPoint Pro automatically invalidates all the cards that were not used on this period. GuardPoint Pro checks each night between 00:45 and 00:46. If =0, there is no automatic cardholder inhibition.
- **BioSmart_SiteKeyMode**: Value corresponding to the 4 options of Bio Smart Security in the Tools>Options>SQL/BIO screen. The available values are 0 (asking the Site code once per session), 1 (asking the Site code once), 2 (asking the Site code at each Bio Smart use), 3 (disabled).
- **BioSmartWaitingCardTimeout**: 10sec by default (range 0-300). Timeout (in seconds) in which GuardPoint Pro waits for smart card after clicking 'Read Smart Card'.
- **SendBioPending**: if =1, Bio template pending are sent during startup. If =0, skipping the 'send pending' commands of Bio template readers upon application startup.
- **DebugBIO**: if =1, all messages relating to Biometric readers are written into AME files (and in DBMon).
- **Default Badge Code**: Value of default card prefix for all new cards. The prefix would be auto created as the card code for each new card, but users can freely edit it. If no value is specified, there is no default badge code prefix.
- **Default Technology**: Default technology for new cards and new readers. The available values are 1 (Magnetic card), 2 (Barcode), 3 (Wiegand), 4 (Wiegand 2), 5 (Wiegand Keypad), 6 (Bio Smart Card), 7 (Touch), 8 (Radio).

- **UseWorkstationTech**: if =1, each workstation uses the ‘Default Technology’ option from its GuardPointPro.ini file (useful in MultiCompany/Multisite applications) instead of using the one of the server GuardPointPro.ini file.
- **UseUSBReader**: if =1, support USB reader for enrollment. Clicking on the 'Get from card' button and passing a card at this reader displays the card code on the 'Get from card' screen.
- **USBReaderFormat**: Card format supported by the USB reader when the entry UseUSBReader=1. The available values are: USBReaderFormat = 0 (hexadecimal, the 8 MSB digits). For example, for a card having the code 1234567890, the screen shows 12345678.

USBReaderFormat = 1 (16 bit decimal for Paxton USB reader)

USBReaderFormat = 3 (24 bit decimal for Paxton USB reader)

USBReaderFormat = 108 (the 8 LSB digits). For example, for a card having the code 1234567890, the screen shows 34567890.

USBReaderFormat = 109 (the 9 LSB digits). For example, for a card having the code 1234567890, the screen shows 234567890.

USBReaderFormat = 110 (the 10 LSB digits)

USBReaderFormat = 111 (the 11 LSB digits)

USBReaderFormat = 112 (the 12 LSB digits)

- **GetFromCardReaderID**: If the reader list is used in the 'Get From Card' screen for filtering cards enrolment on a single enrolment reader, and a specific reader selected, the Reader ID is stored at this location (when exiting the screen), and subsequent accesses to GetCardFromReader will pre-select this reader in the dropdown. By default the value is 0 (<Any Reader>).
- **MultipleViewPhoto**: if =1, more than one ‘Display Photo’ screen can be opened allowing to match several readers simultaneously. On each request to open this screen, a new instance is opened. If =0, only one instance of this screen is allowed.
- **DisplayPhotoDuring**: 0sec by default (range 0-60). Minimum duration (in seconds) to show an image on the Display Photo screen, avoiding too fast photo swapping while many successive access events are received. If =0, the screen shows each image until the next access event is received.
- **PhotoSize**: Default photo size when capturing a photo through the cardholder screen. The available values are 100, 150, 200, 250, 300, 350, 400.
- **PhotoSizeType**: Additional photo sizes to the entry 'PhotoSize' for having different photo ratios (i.e. 4x3, 4x3.25). The available values are 1 (100 X 75), 2 (100 x 81), 3 (100 x 100), 4 (150 x 150), 5 (200 x 150), 6 (200 x 162), 7 (200 x 200), 8 (250 x 250). If =0, the 'PhotoSize' option is used.
- UseAGoptimization: Option to prevent download to controllers any changes on Access Group if no cardholder belongs to this Access Group.

- **TerminalReader**: Allow to display the transactions made using the Terminal into TA or TA+ reports by associating them to a reader. If =1/2/3/4, all the Terminal transactions will be considered as being passed from reader no.1/2/3/4 of the controller which the Terminal is connected to. Note that in the log event screen, the transactions are still attributed to the relevant Terminal. If =0, the Terminal transactions will have no attribution to any reader.
- **PhotoFormat**: Default photo file format in the cardholder screen. The available values are JPG, BMP.
- **LocationRefresh**: Period (in seconds) of the automatic refresh for the Location screen. If =0, there is no automatic refresh for the Location screen.
- **ConfirmOnlyNotOnAlarm**: Value corresponding to the 3 options of Alarm Confirmation in the Tools>Options>General screen. The available values are 0 (allowing to confirm all alarms), 1 (restricted to OFF inputs) and 2 (displaying warning message before confirming).
- **NightShiftHours**: Maximum allowed work time (in hours) for Roll Call supporting overnight work. If =0, overnight work is not supported by the Roll Call (the advanced T&A report which checks entry/exit readers only).
- **Distant_ConnectOnPending**: if =1, GuardPoint Pro automatically updates dial up controllers (via modem) when pending should be sent to these controllers.
- **StartMinimized**: if =1, GuardPoint Pro starts with minimized window.
- **ImportDB_LogOnlyError**: if =1, when importing cardholders, the log file (import.log by default) contains only errors. If =0, the log file contains all the actions, including successful imports. It is recommended to set this entry at 1 if frequent imports are realized to avoid having big log files.
- **ImportwoDownload**: if =1, when importing cardholders, the controllers are not updated, saving process time (recommended for large databases). It is highly advised to initialize the controllers once the import is done.
- KeepUnallocatedBadgeAfterImport: When someone has to change his card for any reason, it may be useful to keep his old card in the system as 'free' card. If=1, the cards replaced by the Import function are still stored in the database as 'free' cards. If=0, when updating existing cardholders with new card via the Import function, the replaced cards are automatically removed from the database.

- **AMEFileMaxSize**: 5Mega by default (range 1-100). Maximum size (in Mbytes) of the daily error files (.ame) on the AME folder. When growing bigger GuardPoint Pro rename the file and open a new one, up to the value of the entry AMERotation.
- **AMERotation**: 3 by default (range 1-254). Maximum number of AME files per day. In case GuardPoint Pro needs to write more AME files in one day, the new file would override the last. For example, if 7 files needed to be created in a certain day, and the entry is equal to 3, the folder would finally contain the 1st, 2nd and the 7th file. Their total size would be AMEFileMaxSize X AMERotation (i.e. 5 X 3 = 15MB).
- **Light**: if =1, when no dongle is installed, the application just supports the basic modules and limited functionality on many screens. If =0, when no dongle is installed, the application supports all the modules with DEMO configuration for demonstrations.

- **EmailServerAddress**: SMTP Server Address, defined in the Tools>Options>General>E-mail options screen, for sending e-mail via an action.
- **EmailSenderAddress**: Sender E-mail Address, defined in the Tools>Options>General>E-mail options screen, for sending e-mail via an action.
- **EmailUser**: User account, defined in the Tools>Options>General>E-mail options screen.
- **EmailPassword**: E-mail Password, defined in the Tools>Options>General>E-mail options screen.

[APB]

- **SoftAPB**: For special projects only. If =1 and if special firmware on controllers, when a cardholder requests to access a second time from a same reader which has the local Anti-Passback mode, the controller grants the access and reports the event as “Access Denied - Anti-Passback”.
- **GlobalAPBwoPC**: if =1, Global Anti Passback is managed by the application and also through the 2nd bus of the controllers, even when the application is down. If =0, it is managed only by the application. Modifying this entry should be followed by controllers initialization.
- **DontUpdateAPBLevel**: if =1, Global Anti Passback is not managed by the application. Usually used when the entry GlobalAPBwoPC=1.
- **UpdateEscortAPB**: if =1, when GuardPoint Pro manages Global Anti Passback, the Anti Passback level of the escort (i.e. the 2nd person to pass on an Escort reader), is also updated.
- **EnableStopPolling**: if =1, the ‘Communication>Stop/Resume polling’ menu is available. In Multi Company/Multi Site applications, only ‘Super users’ can see this menu.

[User]

- **LimitUserAG**: if =1, ‘Access groups’ tab is enable in the User screen allowing to limit each user to be able to add/remove only specific access groups. In this mode, the check box 'Also for visitor' in Access Group screen is disabled because the LimitUserAG option has higher priority. As this option only affects multiple Access Groups, it works only with the entry ‘ForceMultipleAG=1’.
- **PasswordExpireAfter_Days**: 0day by default (range 0-365). Number of validation days of the user password. If =15, it means that the user password expires after 15 days. If =0, there is no expiration. Note that if the password has expired and the user is still logged, GuardPoint Pro will not log him off but will inform him that he should change the password because the period expired.
- **AllowReuseUserPassword**: if =0, the user can't set the same password twice.
- **PasswordMinLength:** Minimum number of characters for the authentication password, including numerals or special characters. (=1 by default).

- **PasswordMixNumber**: Minimum number of letters and digits for the authentication password (=0 by default). A value of 2 would require at least 2 letters and two digits in the password.

[LPR]

- **LPRType**: if =1, support for Sony License Plate Recognition Camera model XCI-NPR. It requires the LPR module on the dongle.

[Video]

- **ViewerPath:** Defines location of custom DVR viewer program (if required). Example: ViewerPath = C:\Program Files\Avigilon\AvigilonViewer.exe. By default the option is empty, which means that the viewer is installed in the application folder.

[External integration]

- **OpenScreenOnTop**: if =1, when opening a screen, it stays above all the other screens for 0.5 second.
- **OpenScreenConstantOnTop**: if =1 and if the entry OpenScreenOnTop=1, when opening a screen, it stays above all the other screens constantly.
- **NoTask_ActiveAlarm**: For special projects only. If =1, when the entry Graphic+=0, no command can be realized from the Active Alarm screen. Usually used with SCADA.
- **ExternalEvents**: For special projects only. If =1, the application receives events from external applications.
- **ExternalEventsTestMin**: For special projects only. 1min by default (range 1-1440). Frequency (in minutes) in which the application should check events from external applications, when the entryExternalEvents=1.
- **Dual Confirmation**: if =1, two types of users can be defined: ‘Maker’, who makes access data changes that affect cardholders and ‘Checker’ who approves or rejects these changes. Once the changes are approved there are automatically downloaded to the respective controllers. This feature is limited to changes in the cardholders’ screen.
- **UseDBforacAPI**: Option for using the table QueueMSGAP of the database for communicating with the Web Interface. This table contains Status and Result of requests.
- CheckacAPIEachSec: 5sec by default (range 1-60). When the entry 'UseDBforacAPI=1', frequency (in seconds) in which the Web Interface checks Status and Result of requests.
- NslTdtAddToAscii: Option for using Ticket Dispenser Terminal controller (belongs to the NSL family), which in addition to its standard security features, is able to print programmable tickets on a serial printer for ticket printing applications (e.g. cafeteria meal tickets). If=1 (0 by default), the “Send Cardholder Names” option is added in the controller screen when selecting the controller type ‘OPEN/NSL4’, for storing in the controller memory, the last name and first name of each

cardholder (11th characters maximum). Note that after a controller is set to 'Send Cardholder Names', GuardPoint Pro server and workstations must be restarted. This feature is supported only for SQL database.

[OPC]

- **OPC Server**: if =1, support for OPC server. It requires the OPC module on the dongle.
- **OPCServerTagUseIdOnly**: if =1, when the entry OPC Server=1, OPC tag names include the ID number of the relevant records in the database. If =0, some OPC tag names include the text inserted in the Description field of the relevant records (e.g., inputs).
- **OPCWaitingDelay**: 0ms by default (range 0-5000). Delay (in milliseconds) between start and end of alarm events in OPC, when the entry OPC Server=1. This is helpful when the external OPC client application might miss successive quick changes in OPC tags. The recommended value is around 100.
- OPCConfirmEventReception: Option for allowing GuardPoint Pro server to wait for OPC client confirmation, in order to be sure that the OPC client receives every event. Then, only when the OPC client has confirmed the event reception by setting the tag '_EVENTS_RECEIVED' to 1, GuardPoint Pro can send the next event and immediately reset the tag value to 0. Events that are waiting to be sent to OPC client are stored in the 'OPCEvents.xml' file.

[ModbusTCP]

- **ModbusTCP**: if =1, support for ModbusTCP. In this mode GuardPoint Pro answers to ModbusTCP commands and each controller is seen as a virtual ModbusTCP device that can accept the relevant read/write supported commands. It requires the Modbus module on the dongle.
- **ModbusTCPObject**: if =1, when the entry ModbusTCP=1, ModbusTCP support is done by the external program 'TCP_MDB_OBJ.exe' (recommended). If =0, ModbusTCP support is done by GuardPointPro
- **ModbusTCP_LogRead**: if =1, when the entry ModbusTCP_LogServer=1, GuardPoint Pro writes in the AME file, the events occurred on Read type data.
- **ModbusTCP_LogWrite**: if =1, ModbusTCP_LogServer=1, GuardPoint Pro writes in the AME file, the events occurred on Write type data.
- **ModbusTCP_LogServer**: if =1, GuardPoint Pro writes in the AME file, the communication operations realized via ModbusTCP.
- ModbusTCP_UseDescriptionForActionProcessID: Option for executing Actions and Processes of GuardPoint Pro via TCPModbus by using customized ID. The customized ID must be numbers only and must be set in the 'Description' field of the corresponding Actions and Processes.

[Telemaque]

- **Telemaque_Table**: For special projects only. Support for an integration with an advanced visitors management system by Safeware (www.safeware.fr).
- **Telemaque_SupprimeVisitor**: For special projects only. Support for an integration with an advanced visitors management system by Safeware (www.safeware.fr).

[JOURNAL]

- **doAskToJournalOnStartUp**: if =1, when the database is MS-Access type (DBType=1), GuardPoint Pro will prompt at startup with the question suggesting the backup when the journal contains more than 3 months data.
- **doAutoJournalEveryMonth**: if =1, when the database is MS-Access type (DBType=1), GuardPoint Pro checks every month, if the journal contains more than 3 months data. If it is true and if GuardPoint Pro is running, it launches the auto backup. The checking operation happens on the day specified at the 'dayOfMonthToAutoJournal' entry and at time specified at the hourToAutoJournal and minuteToAutoJournal entries.
- **dayOfMonthToAutoJournal**: 2 by default (range 1-31). Day of the month (eg. on 2nd day of the month) when GuardPoint Pro checks if the journal contains more than 3 months data and if yes, it launches the auto backup. Only when the entry 'doAutoJournalEveryMonth=1' and the database is MS-Access type (DBType=1).
- **hourToAutoJournal**: 0 by default (range 0-23). Hour of the auto backup (see the 'dayOfMonthToAutoJournal' entry).
- **minuteToAutoJournal**: 57min by default (range 0-59). Minute of the auto backup (see the 'dayOfMonthToAutoJournal' entry).

[Wizcon]

- **Wizcon Integration**: if =1, support for Wizcon Integration.
- **WizconInputTagReset**: For special projects only, when the entry Wizcon Integration=1.
- **WizconReaderTagReset**: For special projects only, when the entry Wizcon Integration=1.
- **WizconTagATimeout**: For special projects only, when the entry Wizcon Integration=1.
- **WizconAreaRefresh**: For special projects only, when the entry Wizcon Integration=1.
- **WizconGroups**: For special projects only, when the entry Wizcon Integration=1.
- **CreateTagsAtStartup**: For special projects only, when the entry Wizcon Integration=1.
- **CreateTagsAtMidnight**: For special projects only, when the entry Wizcon Integration=1.
- **ServerRedundancy**: This entry is displayed on the GuardPointPro.ini file of the server only. If =1, the GuardPoint Pro server works as the main server. If =2, the GuardPoint Pro server works as the backup server, when the GuardPoint Pro server redundancy is used. In this case, when the backup server starts it sends a message via Spread to the main server to close itself. In addition, all workstations receive a command to switch from their main SQL database (defined in the entry SQL_Connect) to

the alternative database (defined in the entry SQL_Connect_Backup). The same way, when the main server starts it shuts down the backup server and tells the workstations to swap to the main database.

- **ServerRedundancyName**: Name of the server that it should replace. This entry is used in Multi site application, for telling to local workstations only to swap. The backup server takes the communication linked to the main server and listen to the main server messages via spread and through the QueueMSG table. Each site could have a backup server.
- **UpdatedbyDistance**: For special projects only, for updating database of distant sites (i.e. create, modify, or delete card/cardholders).
- **UpdateDistantSites**: For special projects only, for updating database of distant sites (i.e. create, modify, or delete card/cardholders).
- **UpdateDistantSitesTimeout**: For special projects only, for updating database of distant sites (i.e. create, modify, or delete card/cardholders). 5sec by default (range 0-300).
- **AllowConnectDistantSitesDB**: For special projects only, for connecting to distant databases and changes records. If =1, a new menu 'Site' appears in GuardPoint Pro menu with the name of the distant sites (up to 6 different sites).
- **Name_CurrentSite**: Name of the local site, when the entry AllowConnectDistantSitesDB=1.
- **Name_Site1**: Name of the 1st distant site, when the entry AllowConnectDistantSitesDB=1.
- **SQL_Connect_Site1**: Connection string to SQL database of the 1st distant site, when the entry AllowConnectDistantSitesDB=1.
- **Name_Site2**: Name of the 2nd distant site, when the entry AllowConnectDistantSitesDB=1.
- **SQL_Connect_Site2**: Connection string to SQL database of the 2nd distant site, when the entry AllowConnectDistantSitesDB=1.
- **Keico**: For special projects only, using Keico readers.
- Suprema: For using Suprema Biometric readers.

[Messages]

- **TRN0, TRN1, TRN2, TRN3…**: Values corresponding to each log events (e.g., Grant, Denied, Start/End alarm etc.), specifying whether or not it should be displayed on the event log, saved and what font color it should have when displayed. All these options are controlled in the Tools>Options>Menu screen.
- Color_DeniedCancel: (=2 by default) Color value of the cancelled badges transactions in the log screen. Available color values are: 0 - Light Pink; 1 - Black; 2 - Red; 3 - Blue; 4 - Bordeaux; 5 - Green; 6 - Orange; 7 - Pink; 8 - Purple; 9 - Light Gray; 10 - Light Blue.
- Color_DeniedLost: (=2 by default) Color value of the lost badges transactions in the log screen. Available color values are: 0 - Light Pink; 1 - Black; 2 - Red; 3 - Blue; 4 - Bordeaux; 5 - Green; 6 - Orange; 7 - Pink; 8 - Purple; 9 - Light Gray; 10 - Light Blue.

- Color_DeniedStolen: (=2 by default) Color value of the stolen badges transactions in the log screen. Available color values are: 0 - Light Pink; 1 - Black; 2 - Red; 3 - Blue; 4 - Bordeaux; 5 - Green; 6 - Orange; 7 - Pink; 8 - Purple; 9 - Light Gray; 10 - Light Blue.
- **SkinEnabled**: if =1 (default), GuardPoint Pro uses the Skin (or Msstyles) specified in 'SkinFile' option.
- **SkinFile**: Skin (or Msstyles) of the user interface. The skin files are located in the folder Media/Bin.
- **SkinConf**: Parameter of the Skin (or Msstyles) of the user interface.

[Personalize Cardholder Screen]

- **Cardholder_Address_Move_To_General**: Sequence order (between 1-7) in which the fields for Address and Phone located in the Cardholders>Personal screen are displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), these fields are left in the Cardholders>Personal screen.
- **Cardholder_Privileges_Move_To_General**: Sequence order (between 1-7) in which the Privileges fields (checkboxes) located in the Cardholders>Personal screen are displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), these fields are left in the Cardholders>Personal screen.
- **Cardholder_CarNumber_Move_To_General**: Sequence order (between 1-7) in which the 'Car registration No.' field located in the Cardholders>Personal screen is displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), this field is left in the Cardholders>Personal screen.
- **Cardholder_ZoneID_Move_To_General**: Sequence order (between 1-7) in which the 'Parking user group' list located in the Cardholders>Personal screen is displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), this field is left in the Cardholders>Personal screen.
- **Cardholder_LiftProgram_Move_To_General**: Sequence order (between 1-7) in which the 'Lift programme' list located in the Cardholders>Personal screen is displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), this field is left in the Cardholders>Personal screen.
- **Cardholder_CustomFields_Move_To_General**: Sequence order (between 1-7) in which the Customized fields located in the Cardholders>Customized screen are displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), these fields are left in the Cardholders>Customized screen.
- **Cardholder_Visitor_Move_To_General**: Sequence order (between 1-7) in which the Visitor fields located in the Cardholders>Visitor screen are displayed in a scrollable window, at the bottom of the Cardholders>General screen. If=0 (by default), these fields are left in the Cardholders>Visitor screen.
- **Cardholder_ID_Move_To_General**: If=1, the 'ID' field located in the Cardholders>Personal screen is moved to the Cardholders>General screen, under the 'Number' field. If=0 (by default), this field is left in the Cardholders>Personal screen.
- **Cardholder_Company_As_A_Combo**: Option for displaying the 'Company' field as a Combo box. Note that it is not supported in Light version.
- **Cardholder_Open_Maximize**: Option for opening automatically the Cardholder screen with the maximal size.

[Keesing]

- KeesingIntegration: For special projects only. Support for an integration with an Internet service allowing to check the authenticity of ID cards, driving licences and passports, by KEESING (www.keesingreferencesystems.com).
- KeesingTest: For special projects only. When the entry 'KeesingIntegration=1', if=1, connection to Test server; if=0, connection to Production server
- KeesingAccount: For special projects only. When the entry 'KeesingIntegration=1', Keesing Account name.
- KeesingUser: For special projects only. When the entry 'KeesingIntegration=1', Keesing User name.
- ScannerType: For special projects only. When the entry 'KeesingIntegration=1', type of scanner used. Available values: 0- Standard; 1- ARH PRM; 2- ARH_PRMc; 3- 3M/RTE 8000.

Hidden options

GuardPoint Pro supports the following options but they are not created by default or when clicking OK in the Tools>Options screen, unless they were previously added manually into the GuardPointPro.ini file.

- **DebugCom**: for creating communication log files of the controllers' communication.

If =1, raw HEX commands and all the polling commands including those with empty results, sent from the PC along with the controllers answers are displayed on the event log.

If =2, this information is saved on files on the AME folder, one file per hour and per controller network. Due to the empty results, this setting means quite large files, even up to few MB per hour.

If =4, the log files contain only the polling commands receiving new events (not the empty results).

If =8, the log files contain only the raw HEX commands sent to the controllers.

If =12, the log files contain the raw HEX commands and polling commands receiving new events.

If =0, no communication log files are saved and this entry is not displayed in the ini file.

- **ExecAppOtherPC: if =1,** the Action screen displays for the action "Execute external application" the computer list allowing to select which PC will execute the application (e.g. DVR program). This entry should be set on all PC where the application is about to be executed.
- **ModbusInternal**: if =1 (not recommended), ModbusTCP support is done by GuardPointPro
- **SpreadInterval**: 10ms by default (range 10-10000). Frequency (in milliseconds) in which GuardPoint Pro checks for new spread messages.

- **SpreadReConnect**: if =1, allow to reconnect to distant spread, when using the option SpreadDeamon, in case of connection failure. This function listen each 10ms by default (configurable in SpreadInterval) if new message arrives via the Spread. If the connection is failed, it returns error code that GuardPoint Pro catches and reconnects.
- **SpreadTimeout**: 16sec by default (range 1-60). Timeout (in seconds) in which GuardPoint Pro waits for an answer from another PC via the Spread.
- **woReconnect** if =1, GuardPoint Pro will never reconnect TCP connections if one or more controllers using TCP networks do not answer.