GuardPoint Pro Release Notes
Version 3.4.001 - September 2021

Contents

Introduction

Update policy for this version

From this version, the main GuardPoint Pro application requires a dongle with **earliest version 3.03.0xx** or higher.

In case there are no version details or if the version on the dongle is earlier than 3.03.0xx, GuardPoint Pro will display an error message and would close the application right after.

Default setting values

When **installing this version for the first time**, the following default settings are set in the GuardPointPro.ini file in order to optimize the system:

- MaxCardholders = 8900 instead of 44000
- NextNumBadgeRandom = 0
- UseNumBadgeTrackTable = 0
- MultipleViewPhoto = 0

IMPORTANT NOTE: When **updating an existing system**, the current settings will not be overwritten. Thus, if necessary, the default settings must be set manually.

New GuardPointPro.ini options

The following is a list of new GuardPointPro.ini entries that have been added in this version:

```
BioService = 1
BioByteOrder = 0
BioDebug = 0
BioSpeedSlow = 300
BioSpeedFast = 6
BioiClassStartBlockIndex = 0
Morpho = 0
Morpho_DB_Connection =
Morpho_MM_Connection =
Morpho_Site_Code = 0
MorphoEnrollmentClient =
MorphoVersion = 0
MorphoDebug = 0
AddCompanyNameToCHnameInLog = 0
IsTemperatureReader = 0
IsSeparateLogForEscort = 0
TA_ShowIndex = 0
ExceptionCountToDelete = 0
APBwithPConLocalNetOnly = 0
APBonPCdelayAllowedInSeconds = 3600
TRN41 = 1102
TRN42 = 1102
TRN43 = 1102
ApplyDefaultTranslation = 0
```

Release Features

OSDP readers

A new specific firmware (TPLE32-OSDP) for newer controllers allows you to use **OSDP serial readers** connected to the second RS485 port of the controller. The Open Supervised Device Protocol (OSDP) is an IEC standard that is much more secure than other common protocols (like Wiegand) and supports AES-128 encryption (generally required in federal government applications). The firmware supports OSDP readers in the following 3 modes:

1. Plain mode
2. Secure mode with default key
3. Secure mode with private key

Using OSDP enables communication among different manufacturers' readers, and it is cheaper to install because it requires less cable. Also, this interface enables a reader to function even if it's located 1200m away from the controller (vs 100m for with Wiegand readers).

Programming the OSDP reader is very simple, it is done via a single command recorded in the "Script" screen (reached, from GuardPoint Pro, by pressing SHIFT+F12 from the selected controller).

Face recognition reader

Since COVID-19, GuardPoint Pro supports the **Face Temperature Reader** (FTR), the new SENSOR facial recognition reader. With its temperature detection module, it can be used at facilities where body temperature measurement must be controlled before granting access.

The FTR can work in 'Face only' or 'Face + Card' mode. When a face is detected, it is compared to cardholder pictures stored on the device. If a match is found, the body temperature measured by the FTR and the corresponding badge code are transmitted to the SENSOR controller. The controller equipped with the 'FTR' firmware interprets the cardholder temperature as a Transaction code.

In GuardPoint Pro, in the Reader/Miscellaneous screen, a 'Maximum temperature allowed' parameter rules on the granting or denying access, depending on the cardholder's facial temperature. Access events with measured temperature are displayed in the GuardPoint Pro Log window and the temperature info may be retrieved from the GuardPoint Pro reports.

Biometric readers

Two new brands of biometric readers have been integrated:

- **Idemia** biometric readers are supported. The supported models are **Sigma Multi WR**, **Lite series**, **MorphoWave Compact**, **VisionPass**. Different device models can be combined on the same controller. The integration allows enrolling up to two fingers, hand(s) or face (according to a related device) for each cardholder from any one of the readers and automatically downloading the finger templates to all the readers within the cardholder's access group. Note that for this integration, the SQL module is a must. Morpho Manager is the Idemia utility software. It is needed for the following uses:
    1. Initial identification of the unit via RS485 link. This step is a must even if later the reader is supposed to communicate via TCP/IP.
    2. Setting the reader's details, IP address, and Port.
    3. Fingerprint enrolment.

  Both MorphoManager versions, 13 and 14 are supported.

- **Suprema2** biometric readers are supported. The supported models are **BioEntry W2**, **BioEntry P2** and **Biolite N2** (without keypad use). Different device models can be combined on the same controller. As with the older models, different modes are supported: 'Finger Only', 'Card + Finger', 'Card or Finger', or Storing fingerprints on HID iCLASS Smart Cards. Furthermore, **BioMini**, the USB enrolment reader from Suprema, is still supported with these devices. Note that you cannot mix Suprema2 readers and the older models (running with BioStar 1 platform) within the same installation. In addition to the regular features we support with Suprema readers, the following new features have been added: 1. In the "Network" screen, a button allows to display all the detectable "Suprema2" Bio-readers available on the same network segment.
    1. Once the IP address of the Bio-reader is chosen in the Reader/Fingerprint tab, the Unit ID number is filled automatically. There is no "Get Unit Address" button.
    2. Besides the standard card formats, 'Corporate 1000' format is also supported.
    3. Site code feature is supported for cards that are used with the Bio-readers.
    4. Suprema2 download mechanism is very different from the former Suprema integration. Communication is done by a service. The service is automatically installed by GuardPoint Pro once the ini entry 'Suprema2' is set.

  This integration requires the SQL module in the dongle.

New 'External Alarm' controller type

A new controller type, called '**External Alarm**' has been added to support a 3rd party alarm system. This type acts as a virtual controller that can send events (eg. alarms) through files or via UDP ports.

Commands like Arm/Disarm, Acknowledge/Confirm, etc. are stored in a new table of the database, which can be read by the alarm panel system. This new table is updated by triggers, therefore the SQL server database type is required for this feature. For more details, please contact us.

Video recorders

Three new Video recorders have been added to the supported NVR list of the V+ module: **SeeTec**, **TVT,** and **DaHua**.

Active directory support

From this version, when starting the GuardPoint Pro application, the GuardPoint Pro Login window proposes 2 possibilities: using the GuardPoint Pro credential (by entering the username and password) or using the **Windows credentials** (by checking the new Windows credentials checkbox). To use the last option, the Windows user account must be part of a User group in AD. The name of this group must contain the word 'SENSOR' (eg. "SENSOR_Security", "SENSOR_Admin", "SENSOR_Operator").

If the user chooses Windows Credentials, the application checks if this user belongs to such AD User group. If yes, it automatically logs in based on the relevant GuardPoint Pro authorization rights. If not, the application stays closed. In GuardPoint Pro, an Authorization level with the name of the relevant AD User group must be previously created.

When logging in for the first time by using the Windows credentials, a new user is automatically created in GuardPoint Pro with the username as Windows user account name and with the associated Authorization level. If later this user account is changed/assigned to another User group in AD, GuardPoint Pro is updated accordingly. Note that this integration requires an SQL server database type.

If you want to start GuardPoint Pro without the Login window and using the Windows account, add in the shortcut of the application the following command at the end of the target: "..\GuardPointPro.exe" **/ad /rs**

Cardholders' import

Two new ways to import cardholders have been developed:

- GuardPoint Pro has now the option to import cardholders via **WEB API**. Requests for cardholder import can be done from any platform that supports HTTP. The HTTP request should be in JSON format with the known GuardPoint Pro import fields. More than one cardholder can be sent in each request. GuardPoint Pro WEB API is hosted by an IIS WEB server and all the requests via WEB API are inserted into the "QueueMSGAPI" table in GuardPoint Pro database, so GuardPoint Pro processes these requests asynchronously. API module must be in the dongle. For more details, please contact us.
- It is possible to import cardholders from an **Oracle** database. The cardholders are inserted into the "QueueMSGAPI" table in GuardPoint Pro database. For more details, please contact us.

IMPORTANT: From this version, the same information contained in both import.log and importAPI.log files are integrated into the GuardPoint Pro Journal. That means that it is now possible to see in "Journal Simple" reports what changes have been made on cardholders' details following an import or via API.

Time & Attendance

For an important customer in India, SENSOR has developed a service that automatically pushes to their **T&A system server**, in JSON format, all employee Granted access events coming from T&A readers of their Sales offices across India.

Enhancements

Virtual machines support

More and more companies are migrating their systems to virtual environments (Virtual machines, cloud, etc.). When GuardPoint Pro is installed on a **Virtual Machine** (VM) and then migrating this VM from Host to Host, the PC ID of the Virtual dongle may change due to some Hardware changes and then, the GuardPoint Pro license is no longer valid.

To avoid this issue, it is now possible to use a specific PC ID when GuardPoint Pro is installed on a VM: when selecting the “Software dongle” option on the new UpdatePlug.exe tool, 2 new options are displayed: “**secondary ID**” and “**third ID**”. If pressing “Get Unique PC ID” without these new options checked, it generates the PC ID as before. If you press “Get Unique PC ID” with one of these new options checked, another PC ID based on the VM's parameters is generated.

So, from now, if installing GuardPoint Pro on a VM, generate the PC ID after checking the **secondary ID** option (the **third ID** option is reserved for specific cases). If not, generate the PC ID without these options.

Note that the dongle order process is not different as before: you may send to us one PC ID (the one you want). When receiving this PC ID, we re-send you the Virtual dongle files, as before (i.e., the “Data.plg” and “Signature.plg” files).

Protection against successive alarms

In site, faulty detectors may trigger several alarm events per second, and if no one is paying attention, it can last for several days! This may cause other issues like slowing down the access event uploading and then causing problems with the APB global or with Global Reflexes, etc.

To avoid such issues, a new field called “**Ignore successive alarm time**” has been added in the Input screen to skip a repeating alarm. This field is used to select a delay of 0 to 15 seconds (default = 0) during which successive alarm events from the same input will be ignored.

That means that when setting this delay = 5 seconds, if 3 alarms have occurred from the same input within 5 sec, the controller will send one “Start of alarm” event only. If setting this delay = 0, all the “Start of alarm” events will be recorded (as previously). The controller must have the firmware from Dec. 18, 2019, or newer).

New action for inserting a Reader exception

If you want, for example, that anyone who has entered in a room A must wait 24 hours to be authorized to access a room B, you may use this new feature that temporarily (for 1 to 1000 hours) authorizes or forbids access at one door or all doors to a cardholder via a Global Reflex. This rule may be applied to a specific cardholder or any cardholder who has swiped at a predefined reader.

When this action is triggered, the application just **creates/updates the Reader exceptions** to the relevant cardholders. Each new (or modified) exception is logged in the GuardPoint Pro audit log. Moreover, a new INI option allows you to automatically delete the expired exceptions from the Cardholders details.

Cardholder list in the Access group screen

In the 'Access group' (AG) screen, a new tab has been added to **list all cardholders** belonging to the selected AG. This tab includes a Search field to find specific persons. In addition, the title of this tab gives the total number of cardholders currently with this AG.

USB enrolment reader enhancement

Two more USB Reader formats have been added to support more USB reader models:

- INI entry **USBReaderFormat = 113**: When this option is set, the 'Code' field is disabled in the Badge screen. The card codes must be inserted into the 'Description' field of the Badge screen in Decimal format. Then, after pressing 'Save', the 'Code' field is automatically filled with the Hexadecimal value of the enrolled code. In the Cardholders' screen, the Badges are displayed with their Decimal value. If importing cardholders, the codes inserted in the 'Badge' field in the HR.XLS spreadsheet are automatically imported into the 'Description' field of the Badge screen and the relevant Hexadecimal codes are set in the 'Code' field of the Badge screen.
- INI entry **USBReaderFormat = 114**: With this entry, the maximum length of the 'Code' field in the Badge screen is increased to 13 (instead of 12). A new '**Convert to hex**' button is displayed in the Badge screen allowing the user to convert the card code entered in Decimal format into a Hexadecimal value.

Both formats require the INI entry 'UseUSBReader = 1'.

Man Trap 5

A new Man Trap type, '**Man Trap 5**', has been added in the Door type list of the Reader screen. The Man Trap feature has been designed for the Man Trap portal which allows to manage a space that only one person can occupy. Mantraps are most often used to separate non-secure areas from secure areas and prevent unauthorized access. They can also be found in high tech manufacturing to provide entry and exit chambers for clean rooms.

The Man Trap portal is a set of two interlocking doors where the first set of doors opens before the second set, causing the user to be "trapped" inside temporarily.

In GuardPoint Pro, you may define different types of Man Traps. For example, with **Man Trap Type 1**, when the entrance door is opened after a granted access, a second access cannot be granted through this door until the exit door is opened and then closed. If using the Mantrap in both directions, both readers are installed outside the portal, and both exit push buttons (RTX) are inside the Mantrap. Once one door is opened, both readers stay locked until the opposite door is opened and closed, using its RTX inside the Mantrap.

Man Trap Type 5 mode allows to manage a room having up to 4 interlocking doors, whereas the other modes allow 2.

Like the other modes, it prevents one of the doors from opening if another remains open. It is possible that the Door relay activates after authorized access, but the door is not yet open. In this case, the Door contact is not yet activated, and another door can still open. With the **Man Trap Type 5** mode, the controller checks the state of the door relays and as soon as one of the door relays is activated (by a reader or by an RTX), all readers of the same controller defined in Man Trap Type 5 mode and all the associated push buttons are inhibited until no relay AND no door contact is activated.

While the other Man Trap modes allow only one person to enter, **Man Trap Type 5** mode allows many people to stay inside the Mantrap.

Man Trap Type 5 is defined like the other modes, in the 'Door type' field of the 'Reader/Door control' screen. This feature requires a recent firmware version.

Quickly open the AME file from the application

From this version, it is now possible to **open the current AME file** by double-clicking on the bottom blue bar.

Update the APB levels on controllers in the same network ONLY

On installations having many controllers and many cardholders' movements, when using the Global anti-passback (APB) feature, events may be processing very slowly because commands for updating the cardholders' APB levels may overload the communication with unnecessary commands.

A new INI entry, APBwithPConLocalNetOnly, sends the APB level update commands in broadcast mode to the concerned network only (the one where the controller has reported the access event), and not to all the networks in the site. This feature works with ServiceCom module only.

Improvements

Alarm event colour definition

New fields have been added in the Input screen where a user can select, for each alarm, the **desired colour** for a Start of Alarm (ON) event and for an End of alarm (OFF) event in the Event log screen.

Multiple access group screen improvement

When opening the '**Multiple access group**' window from the 'Cardholder' screen, you will discover new **collapsible checkboxes** next to each AG name. These checkboxes easily allocate/remove several Access groups in one go just by selecting them and then clicking the middle arrows. Furthermore, you may show/hide the reader list of each AG by clicking the **'plus'/'minus' symbol** at the left to expand/collapse the list.

At the bottom right side of the screen, a new option named '**Show permissions for Time**' allows to display the current cardholder's **validation status** (Validated/Invalidated) according to the Validation checkbox and the cardholder's allowed reader list with their **authorization status** (V or X) in real time. The authorization status takes into account the cardholder's Exceptions, Schedule AG, Personal WP, his Card Type, the Reader Technology, Holidays and the 'No access during holidays' option.

Clicking the **'plus'/'minus' symbol** at the left of each reader name expands/collapses the details of this authorization: the corresponding Access group name with the associated Weekly Program and if relevant, the cardholder's Personal WP.

Restriction on Cardholder From date/To date fields

A new element, '**Cardholder From/To Date**', has been added in the 'Authorization level' screen under the 'All cardholders/Cardholder access rights' section. This option prevents certain users from using the 'From date' & 'To date' fields in the Cardholder screen.

Separated log transaction for escort

With the INI entry IsSeparateLogForEscort= 1, in the Log event screen, any access granted by 2 persons (the escorted guy and his escort) are displayed in **2 rows** (one 'Access Granted' per person) instead of 1 row.

Also, in the Door pass reports, 2 different records are written. Thus, by setting a filter on Transaction code = '255', it is possible to generate a report of all escort people's access events.

Likewise, it is now possible to trigger a Global Reflex when a specific person is escorting someone else.

Galaxy zones 0011 to 0018 are created by default

On a Galaxy Alarm panel (type 96, 264 or 520) the RIO switch (SW3, dipswitch 8) controls the ordering of the on-board RIO's. When setting this switch ON, the on-board RIO1 operates on line 0 and allows a RIO addressed as 1 to be connected to line 1. In this mode, the onboard RIO's configure to the following addresses: Onboard RIO0 Zone address range: 1001-1008 Outputs: 1011-1014 Onboard RIO1 Zone address range: **0011-0018** Outputs: 0011-0014

To support this setting also, when creating a Galaxy Alarm panel (type 96, 264 or 520) in GuardPoint Pro, the **0011 to 0018 inputs** are now also created by default. Note that if the Alarm panel was already created in previous GuardPoint Pro version, these inputs will not be added automatically.

Reader/Input/Relay names are updated after renaming the Controller

When creating a new controller with the name "CONTROLLER4", all its readers, inputs and relays have the suffix "/ CONTROLLER4" in their name (i.e. "Rdr01 / CONTROLLER4", "i01 / CONTROLLER4", "r01 / CONTROLLER4"). After renaming the controller, all the relevant reader, input and relay **names automatically update accordingly**.

The 'Description' field added in the "Choose a card" screen

After clicking 'Allocate' button in the 'Cardholder' screen to give a card to a cardholder, the 'Choose a card' screen displays a table if all the available card codes and their type. Now, we have also added the **'Description' field** in this table to facilitate the selection of the badge.

Fixes

GuardPoint Pro installation made the PC crash

When installing GuardPoint Pro v3.3.075 on Windows 10, if not checking the “Skip Hasp Install” checkbox, the HASP driver (used by USB dongles) setup made the PC crash at the end of the installation. After using the latest HASP driver in the GuardPoint Pro setup file, the problem has been solved.

Customized fields of some cardholders were randomly emptied

This issue happened after selecting a person that has some values in any Customized fields in the Cardholder screen, pressing ‘Search’ button once and then, closing the screen. All the customized fields of the selected cardholder were emptied. This issue has been resolved.

Deleting a Scheduled AG deleted the Access Group also

On SQL database type installation, after deleting a Scheduled AG, the AG was also deleted from the database. This issue has been fixed.

Lift and Parking groups were deleted after a DBAPI update command

In a Multisite installation, the update via DBAPI of the badge code of an existing cardholder deleted his Lift AG and Parking AG. This issue has been fixed.