GuardPoint 10 v1.80
About This Release

New

- **Biometric authentication has been expanded to include Facial Recognition technology**

  Two images per cardholder can be enrolled. Each image will have its own virtual badge code.

  GuardPoint 10 GUI impact:

  - A cardholder's details > Biometric tab will now have two enroll face image options below the ten fingerprint enrollment options already available.

  The Biometric Facial Recognition readers supported by GuardPoint 10 are as follows:

  - Suprema Facestation F2 (FSF2ODB) with firmware 1.1.2 2021/09/03 or higher
  - Suprema Facestation F2 (FSF2-DB) with firmware 1.1.2 2021/09/03 or higher
  - Suprema Facestation F2 (FSF2-AB) with firmware 1.1.2 2021/09/03 or higher

  When using one of these readers, ensure that you have the most recent firmware version installed.

- **Global Anti-Passback**

  Global Anti-PassBack (GAPB) requires that readers be used in a sequence to enter or leave an GuardPoint 10 defined area. This means that GAPB rules are centered on predefined Areas. GAPB forces a cardholder to take a predetermined path to a destination via one or more Area readers.

  GAPB is enabled from the Options > System & SQL screen. When enabled:

  The Area Setup screen displays new fields and columns to support GAPB.

  The Cardholder details > General tab displays a Global Anti-PassBack (GAPB) field, a Send GAPB button, and a Clear GAPB button.

- **Auto Archive Journal**

  The Auto Archive Journal feature is an automatic archive process for the GuardPoint 10 active journal. The archiving process secures older journal entries. A byproduct of the Auto Archive Journal feature is faster system performance.

  A successfully archived journal is stored in the current Microsoft SQL Server. An archived journal is a database that contains copies of Journal entries that were in the active journal.

  An archived journal can be viewed via a new **Journal** drop-down list at the top of the Event History screen.

- **Active Directory Integration**

  You can now provide users with the option to log in to GuardPoint 10 with their Windows Active Directory credentials.

  To enable Active Directory integration, go to the Options > General screen and set **Enable Active Directory** to **Yes**. Then enter the **Domain name** provided by the organization's IT department.

  To provide a user with the Active Directory login option, go to the user's details. A new field called **Active Directory Username** appears. Attach the user's Windows username to the GuardPoint 10 user.

  From the Login screen, the user will be able to log in to GuardPoint 10 with their GuardPoint 10 credentials or just click the **Login with Windows Credentials** button without entering a user name and password.

- **Dahua technology Integration**

  GuardPoint 10 now supports Dahua cameras and video recorders. To add this technology to the system, select 'Dahua' from the NVR/DVR screen's **Type** drop-down list when entering Dahua details.

- **Mitsubishi smart elevator DOAS system (via the ELSGW protocols) Integration**

  MITSUBISHI ELECTRIC'S DOAS SYSTEM manages smart multi-car elevator systems by allocating car efficiently according to the floors that passengers select from the elevator panel while waiting for a car's arrival.

  By integrating ELSGW protocols into GuardPoint 10, you can use cardholder information to manage the lift's elevator panel. This restricts floor selection via the elevator panel to those floors where the cardholder is authorized.

  To add this elevator integration, set the Options > General screen's **Display ELSGW Lift** option to **Yes** and enter the **IP address** and the **port** of the lift panel. This will permit you to add a lift controller to the infrastructure and an ELSGW Lift Access Groups through the Access screen.

- **An 'Unlock All Doors' Global Reflex action has been added to the list of Relay actions**

  This action changes the state of all door relays in a site. The state options are:

  - Activate all door relays
  - Return all door relays to normal
  - Activate all door relays for: (sets an activate time limit)

- **MultiSplit is now available to increase GuardPoint 10 performance**

  MultiSplit makes the GuardPoint 10 system "elastic" by using distributed computing to split the workload between multiple machines.

  MultiSplit is best for large or growing GuardPoint 10 systems. Imagine you have hundreds of controllers that generate a lot of events. These events must go through some processing, which unfortunately takes longer

than to generate. For the processing to catch up with real-time, a slave machine can be designated to handle some of the processing.

To support MultiSplit the following additions have been made to the GuardPoint 10 GUI:

- In the Options > General screen, there is a new setting called **Display MultiSplit**. When set to **Yes**, the next two elements are visible.
- In the Infrastructure screen's Action bar there is a new **Split Servers** button that opens a Split Servers popup where communication services can be added to the system.
- In an Infrastructure's Network details, there is a new **Split Server** parameter where a communication service can be selected to handle all of the data processing that takes place in the network.

For more information about setting up MultiSplit, see the online Help.

- **GuardPoint 10 is now supported on versions of Windows 11.**

  Before you upgrade, make sure you're familiar with Windows 11 specifications and system requirements and that your computer supports Windows 11.

Enhancements:

- **A GUI lag time solution has been deployed**

  From the end-user perspective, tasks will end faster (sometimes much faster). Tasks are marked as done as soon as they are sent to the communication service (even before the communication service manages to complete sending them). Waiting commands can still be seen on the Diagnostic screen.

  Improvements have been made to many SQL queries. These improvements increase performance and are most noticeable when dealing with complex or large databases with thousands of cardholders. For example, after adding new readers to a MAG, instead of removing all the cardholders and downloading them again to the controllers, GuardPoint 10 now only downloads the relevant commands.

  All GuardPoint 10 internal triggers were transformed to SignalR instead of the WCF-based service. SignalR is a new technology from Microsoft that handles push notifications very quickly.

- In the Diagnostic screen, the infrastructure tree can now be filtered by controller state (Activated/Deactivated/Disconnected). In addition, Collapse all and Expand all buttons have been added next to the Filter field.
- A new **Import Cardholder Excel Template** has been added to GuardPoint 10. It includes **License Plate** and **Badge Template** entry fields.

  With this new template, Badge codes and a License Plate number can be added or updated for a cardholder in the same import process.

  Note: A cardholder import excel template from a previous GuardPoint 10 version is invalid in this GuardPoint 10 version. **Please move to the new spreadsheet included in this GuardPoint 10 version.**

- Imported cardholders will no longer have a default Personal Weekly Program assignment. In the cardholder's details, the field will be initially empty.
- In the cardholder details' Personal Door Access Groups list, Door Access Group names can now be displayed in different colors. To do this, add the following code in the Access Group's **Description** field:

  {"Type":"SAP2AC","Color":"blue"}

  Substitute any HTML color code (i.e. #2424ff) for the word **blue** (or any other acceptable color name) in the code.

- A **Change also Supervisor area** field has been added to the Reader details' Access Mode tab.

  When **Change also Supervisor area** is set to **Yes**: A Supervisor acting as an escort for another cardholder approaches an Area door that is an entrance or exit to that Area. After both badges are swiped at the door's reader, an access event entry is recorded for both the Supervisor and the cardholder and the Supervisor's Area value is updated.

  When **Change also Supervisor area** is set to **No**: After both badges are swiped at the door's reader, an access event entry is recorded only for the cardholder. The Supervisor's Area remains unchanged.

- The **Area Setup** screen now has additional information to support the new GAPB feature.

  In an Area's details, there is a:

  - Switch to enable GAPB for the selected Area
  - A dynamic list of current Areas that have enabled GAPBs
  - A number representing the number of Areas that can still be enabled as GAPB Areas

  In an Area's the Entrance and Exit tables, there are two new columns:

  - APB Green: Displays the setting of an Area reader's Access Mode tab's **Green Zone's Anti PassBack** setting.
  - APB White: Displays the setting of an Area reader's Access Mode tab's **White Zone's Anti PassBack** setting.

  An Area reader's **Anti PassBack** setting must be set to **Yes** to participate in a GAPB environment.

- Popup windows that include a minimize button in the title bar (i.e. Cardholder details, Task List, etc.) will no longer be always on top of the GUI. Now, when the user clicks a screen behind the popup window, the popup window will automatically minimize.
- The Departments screen's list of saved departments now includes a **Search** field.
- In the Options > Event Log screen, all Access Denied event types are grouped at the top of the list.
- In the Options > Event Log screen, a new **Access Denied - Anti Passback** row has been added to the list.
- The GuardPoint 10 WebApp's Door page now includes a **Return all Doors to Normal** button to complement the existing **Open All Doors** button.
- Badge templates will now be stored in the system database. Sharing a single badge template source ensures consistency across workstations.

- In the Event Log, an alarm's text color has a default color set in the Options > Event Log screen. Now, an individual input's text color can be set in the input's details. This will allow the alarm text to stand out.
- A **Skip a repeating alarm** field has been added to the Options > General tab. It reduces unnecessary alarms caused by a malfunctioning detector (Relevant for firmware newer than 18/12/2019). If the setting is edited, the user must initialize the controller with the problematic alarm before the setting change is carried out.

  By default, alarms that repeat every 5 seconds or less will be ignored (skipped).

- Screens with a Report Template option now include a **Clear Column Filters** button. The relevant screens are Badges, Cardholders, Event History, and Infrastructure (in Table view).

Fixes:

- **Fixed**: The GuardPoint 10 WebApp's, Cardholder details now displays **Custom Fields** added via the GuardPoint 10 desktop. The displayed Custom Fields values can also be edited via the Web App.
- **Fixed**: A more robust enforcement of cardholder field value validation has been added to the GuardPoint 10 WebApp.
- **Fixed**: The Departments screen's tree of saved departments will now remain expanded or collapsed after saving a new department. The new department will automatically appear in the tree.
- **Fixed**: The Time & Attendance screen now consistently opens smoothly.
- **Fixed**: In case a query in an GuardPoint 10 API returns a response with many values, only the first 50 values are returned along with a link to get the next 50 values. This link now consistently appears in all relevant responses.
- **Fixed**: Cameras with low resolution are now supported in the GuardPoint 10 Visitor Module.
- **Fixed**: After a table error occurs on a controller, the command 03 (READER TECHNOLOGY AND CARD FORMAT) is now automatically sent consistently to rebuild the table.
- **Fixed**: The Display Events screen now formats cards that include landscape images with clearly legible text.
- **Fixed**: Dates throughout the GuardPoint 10 interface now display in the standard format DD/MM/YYYY.
- **Fixed**: An input's name can now be edited while the input is in use.
- **Fixed**: In the Infrastructure screen, switching from a controller's Readers table to the Inputs table will no longer display a save message - unless required.
- **Fixed**: The Global Reflex action **Create Template-based report**, where the selected template is an **Event History template**, will now work correctly when the template is sent by email.
- **Fixed**: LAGs with complex input selections can now be saved in the LAG consistently.

More information about the Enhancements and Improvements in this release may be found in the Online Help.