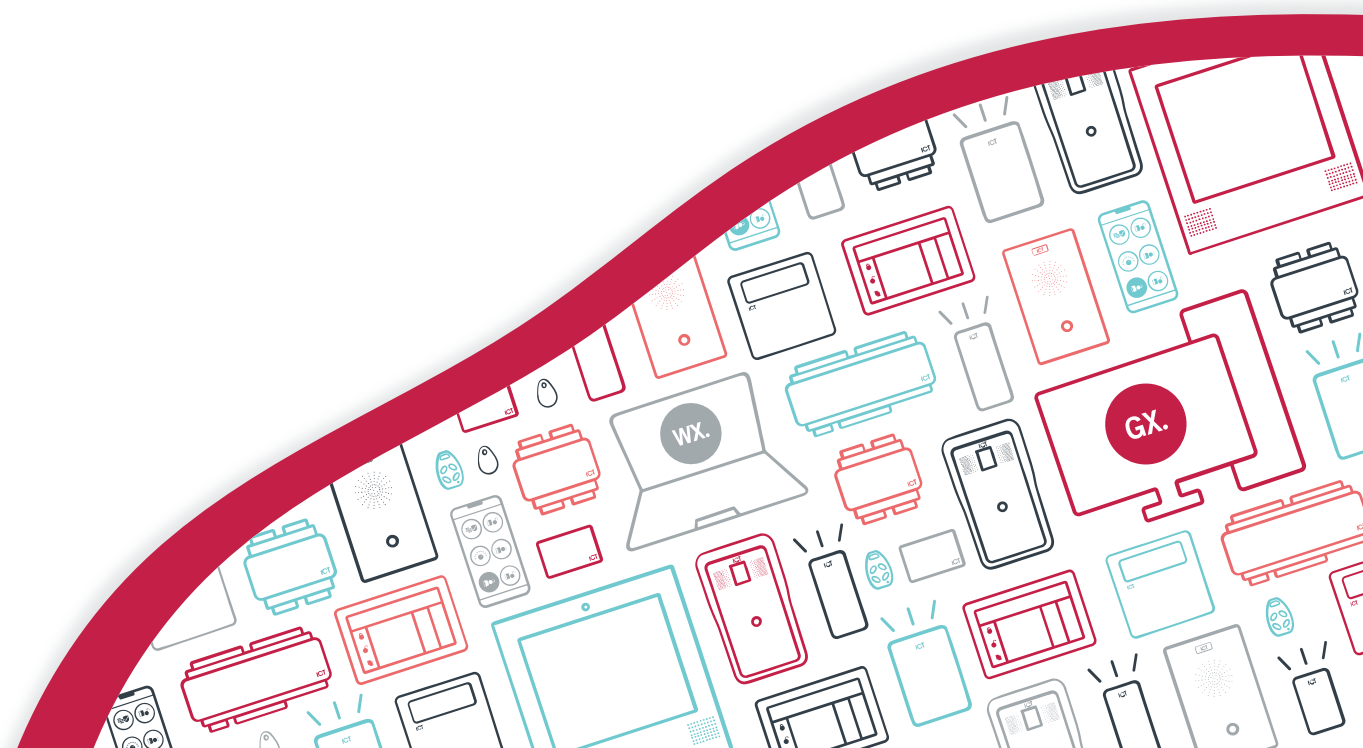
AN-332

Setting up Event Notifications in Protege GX

Application Note



Last Published: 03-Apr-23 08:32 AM

Contents

Introduction

A Protege GX system of any size generates a large number of events in its everyday operation. While this is useful for retrospective reporting and data collection, there is a risk that incidents requiring an immediate response will be lost in the noise. In addition to standard central station reporting, Protege GX offers a number of features to ensure that important events are sent to the right people, at the right time.

This application note provides an overview and programming example for two methods of sending event notifications:

- Operator alarms
- Email-on-event actions

If you are using the Protege Mobile App, an alternative option is to send push notifications directly to operators' phones. For more information about this feature and programming instructions, see Application Note 201: Protege GX Push Notification Setup.

Overview of Event Notifications

Both operator alarms and email-on-event actions allow you to send notifications based on any event in the Protege GX system. However, each has different features and is useful in different contexts, allowing you to use one or both as the situation demands.

Operator Alarms

Operator alarms send a popup window to Protege GX operators when selected events occur in the system. These are most useful for raising important events to security guards and other operators who are likely to have the Protege GX client running at all times, ensuring there will be a quick response.

Operator alarms are programmed in **Events | Alarms**.

Note: Operator alarms are different from the area alarms that are generated on site. Area alarms may be configured to send operator alarms, but this does not happen by default.

Key features:

- Operator alarms can be configured for any event type in the system, filtered by specific records such as individual doors, areas or users. Event filters are programmed in **Events | Event filters**.
- Operators must acknowledge alarms, and can be required to leave a comment. These acknowledged alarms are saved to the pre-programmed Alarms status page, creating a record of incidents and responses.
- Instructions can be associated with each alarm, to provide contact details or other relevant information.
- The display settings for alarm popups can be configured for different operators (**Global | Roles | Display**), allowing you to define which operators receive alarms and whether they can 'snooze' the notifications.
- Associate a floor plan with an alarm, so that operators can quickly view the current status of the incident.
- Alarm routing allows you to set up a custom path for the alarm: for example, a building alarm may be sent to the local guard post first, then passed on to the central office only if it is not acknowledged. Program alarm routing in **Events | Alarm routing**.
- Set a priority for each alarm so that the most urgent incidents take precedence over minor issues. Program priorities in **Events | Alarm priorities**.
- Each alarm can play a custom sound file, helping personnel to quickly differentiate between different types of alerts and respond appropriately. Add custom alarm sounds (.wav files) in **Global | Global settings | Sound**.
- If the system has integrated cameras, alarm notifications can include a camera window showing live and archived footage from the event. You can associate cameras with doors, areas, outputs or inputs. The camera popup will follow the alarm routing rules, allowing it to be passed to different workstations until it is acknowledged.

Email-on-Event Actions

Email-on-event actions allow you to automatically send a notification to key stakeholders as soon as the incident occurs. This is useful for making people aware of a situation when an urgent response is not required.

Email-on-event actions are programmed in **Events | Actions**. You must also have a valid SMTP mail server configured in **Global | Global settings | Email settings**.

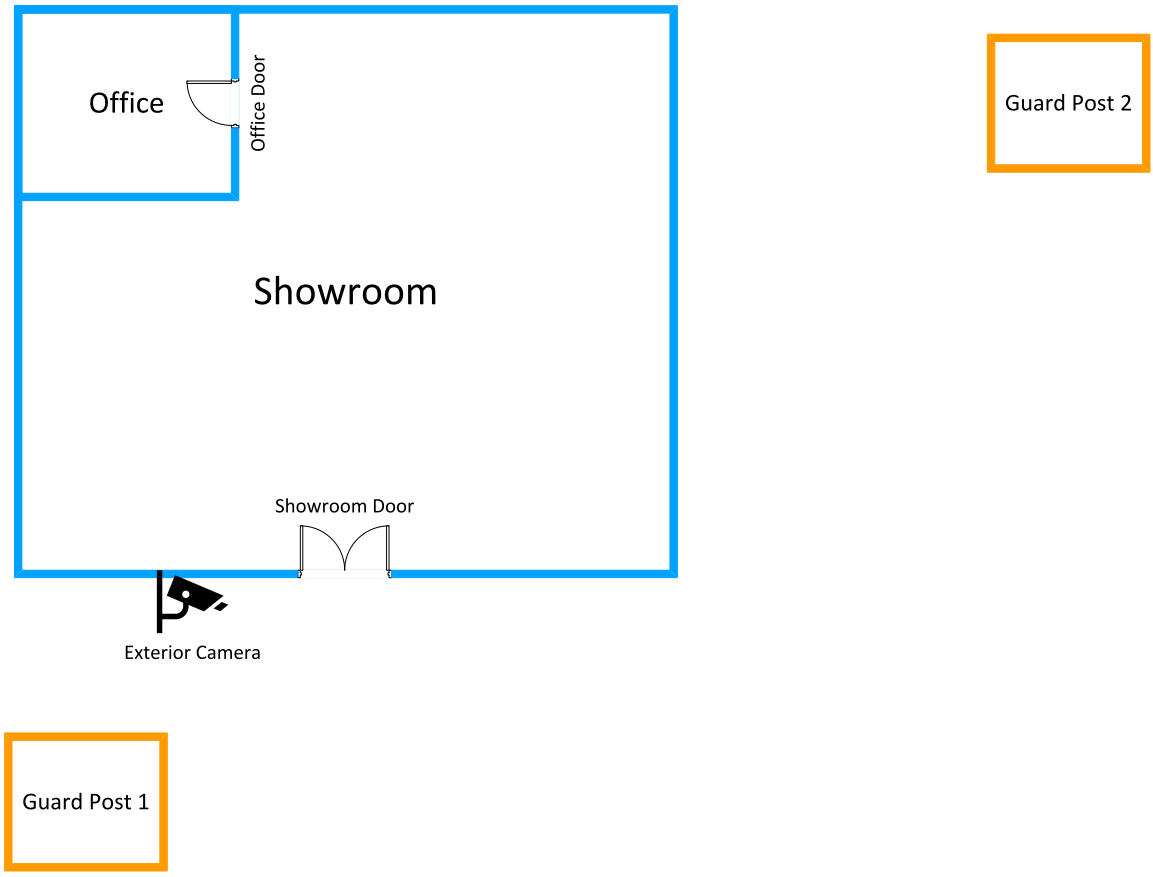
Email-on-event is not available with a Protege GX starter license. Upgrade to a standard license to access this feature.

Key features:

- Email-on-event actions can be configured for any event type in the system, filtered by specific records such as individual doors, areas or users. Event filters are programmed in **Events | Event filters**.
- Send emails to one or more recipients. Recipients do not need to be Protege GX operators.
- The Protege GX client does not need to be running.
- Include key information about the event in the email subject line and message, such as the event time, description and user name. For more information, see Appendix: Email Field Variables (page 13).

Programming Scenario

In this programming scenario we will set up event notifications for the Aperture Appliance showroom.



Before you Begin

To test this programming scenario you will need an operational Protege GX system with at least one controller online. The following records must be programmed before you begin:

- **Areas**: Showroom, Office
- **Doors**: Showroom Door, Office Door
- **Inputs**:
  - Showroom Door Sense (set as the **Door position input** for the Showroom Door)
  - Office Door Sense (set as the **Door position input** for the Office Door)
  - Showroom PIR (programmed in the Showroom area with the Instant input type)
  - Office PIR (programmed in the Office area with the Instant input type)
- **Cameras**: Exterior Camera (set as the **Camera (entry)** for the Showroom Door).

Ideally this scenario should be validated on two separate workstations with the Protege GX client installed. It is not necessary to have a physical camera connected.

Event Notification Requirements

The client is concerned about break-ins and wants the system to send notifications to nearby guard posts and company stakeholders when there is an area alarm or forced door on the premises. To achieve this, we will set up two different types of event notifications:

- **Operator alarm**:
  - The security guards in the two guard posts must receive a popup notification from the Protege GX client when one of the selected events occurs.
  - The notification must have a unique sound effect to distinguish it from standard Windows alerts.
  - When the Showroom Door is forced, the security guards must also see a camera popup with live footage of the intrusion.
  - The notification will be sent to the Protege GX workstation in Guard Post 1 (computer name: GUARD01) first. If it is not acknowledged within 2 minutes it will be sent to Guard Post 2 (computer name: GUARD02).
  - To ensure a full record is kept, the security guards must leave a comment with their name when they respond to the incident.
- **Email-on-event action**:
  - The showroom manager and company CEO must receive an email when one of the selected events occurs.
  - The email will contain key information about the event.

For detailed information about these features which is not covered in this scenario, see the Protege GX Operator Manual (click **About | Help** in the Protege GX software).

Creating the Event Filter

Both operator alarms and email-on-event actions require an event filter record. Event filters instruct alarm and action records which types of events will be sent as notifications.

For our scenario we can use the same event filter for both the alarm and email-on-event programming. It needs to include alarms in the Showroom and Office areas, as well as door forced events for the Showroom Door and Office Door.

To program the event filter:

1. Navigate to **Events | Event filters**.
2. **Add** a new event filter with the name Aperture Event Notifications.
3. In the **Event types** tab, uncheck **Include all event types**.
4. Click **Add** to open the **Select event types** window. This window allows you to select the specific event types that will be included in this filter.

   The event types are grouped by category and can also be searched by keyword. If you are unsure which event types should be included, use a status page to check which events are recorded when certain incidents occur.

5. From the **All area events** group, select the event type:
   `Area <AREA_NAME> Alarm Activated`
6. From the **All door events** group, select the event type:
   `Door <DOOR_NAME> Forced Open`
7. Open the **Records** tab. This tab allows you to select the specific records which will be included in the event filter. Only events that match both the event types and the record filters will be included.
8. Click **Add** to open the **Select devices** window.
9. Select the Showroom Door and Office Door and click **OK**.

10. Click **Add** again and set the **Device type** to Area.
11. Select the Showroom and Office and click **OK**.
12. Click **Save**.

Programming the Operator Alarm

In this section we will program the operator alarm which will be sent to the two guard posts. First we must add a custom sound for the alarm, then create the workstation and workstation group records required for alarm routing. Then we can create the alarm record.

Adding a Custom Alarm Sound

By default, alarms use the default Windows alert sound. To distinguish Protege GX alarms from other notifications you can customize sounds in the global settings.

The **Alarm sound** setting provides a default sound configuration for all alarms that do not have a custom sound assigned, while custom sounds can be assigned to specific Protege GX alarms.

In this scenario we will add a custom sound to be used for door forced and area alarms:

1. Navigate to **Global | Global settings | Sound**.
2. Under **Sounds**, click **Add** to create a new custom sound record.
3. Browse your system and select a **.wav** file to be the sound for this alarm. This can be any wave file on the computer, with a maximum file size of **3 MB**. Common wave file locations include:
   - C:\Program Files (x86)\Integrated Control Technology\Protege GX\Alarm Sounds
   - C:\Windows\Media

   Custom sounds assigned to an alarm record will be automatically synchronized to each client machine when an operator logs in.
4. Enter the name Intruder Alarm Sound.
5. Click **Save**.

Adding Workstations and Workstation Groups

Workstation records represent computers on the network that are running the Protege GX client. Programming workstations and workstation groups allows us to send incoming alarms to one group of operators first, and then route them to a different group of operators if the first group does not acknowledge and respond.

Adding the Workstations

Two workstations are required to represent the Protege GX clients in our two guard posts.

1. Navigate to **Events | Workstations**.
2. Click **Add** to create a workstation with the name Guard Post 1.
3. Enter the **Computer name**: GUARD01

   For testing purposes you may enter the name of your computer.
4. Click **Save**.
5. **Add** a second workstation with the name Guard Post 2.
6. Enter the **Computer name**: GUARD02

   For testing purposes you may enter the name of another computer on the network.
7. Click **Save**.

There is no need to program the **SIP client** or **Cencon key box** settings.

Adding the Workstation Groups

Each workstation must be placed in a workstation group.

1. Navigate to **Events | Workstation groups**.
2. Click **Add** to create a workstation group with the name Aperture Alarms First Group.
3. In the **Workstations** tab, check the box beside Aperture Guard Post 1.
4. Click **Save**.
5. **Add** a second workstation group called Aperture Alarms Second Group.
6. In the **Workstations** tab, check the box beside Aperture Guard Post 2.
7. Click **Save**.

Configuring Alarm Routing

Alarm routing records instruct the system where incoming alarms should be sent and what to do if the alarms are not acknowledged. We need to program an alarm routing record which will send alarms to Guard Post 1 first, and if the alarm is not acknowledged within 2 minutes transfer it to Guard Post 2.

1. Navigate to **Events | Alarm routing**.
2. **Add** a new alarm routing record called Aperture Alarm Routing.
3. Open the **Workstation groups** tab. It will display the workstation groups we programmed above.
4. Enter the settings for the Aperture Alarms First Group:
   - **Transfer after**: 120 (seconds)
   - **Transfer priority**: <not set>
   - **Routing order**: 1
   - **Active**: Enabled
5. Enter the settings for the Aperture Alarms Second Group:
   - **Transfer after**: 120 (seconds)
   - **Transfer priority**: <not set>
   - **Routing order**: 2
   - **Active**: Enabled
6. Click **Save**.

Creating the Alarm

Finally, we can create the alarm record which allows the system to start sending operator alarms to the guard posts.

1. Navigate to **Events | Alarms**.
2. **Add** a new alarm record called Aperture Alarms.
3. The **Instructions** field allows you to enter brief instructions for the security guards who will be responding to the incident. Enter the following **Instructions**: Investigate Aperture premises. Call Caroline on 021345678.

   If your site uses a second language, you can enter the translated instructions in the **Instructions 2** field.
4. Set the **Event filter** to Aperture Event Notifications.
5. Set the **Alarm routing list** to Aperture Alarm Routing.
6. Set **Alarm acknowledgement comments** to Must. This ensures that security guards cannot close the alarm window without leaving a comment.
7. Set the **Alarm sound** to Intruder Alarm Sound.
8. Enable **Allow camera popup**. When the Showroom Door is forced, a window showing footage from the Exterior Camera will pop up.
9. Click **Save**.

Programming the Email-on-Event Action

In this section we will set up the email which must be sent to the showroom manager and CEO of Aperture Appliance when there is an alarm on the premises.

Configuring the SMTP Settings

Protege GX must have access to an SMTP server so that it can send emails out. This can be configured in the global settings.

1. Navigate to **Global | Global settings** and open the **Email settings** tab.
2. Enter the details of the SMTP server. For testing purposes you will need to connect to a real SMTP server. The following settings are an example:
   - **SMTP mail server**: mail.sentrysecurity.com
   - **SMTP port**: 587
   - **Use SSL**: Enabled
   - **SMTP logon**: ProtegeGX
   - **SMTP password**: XXXXXX
   - **SMTP timeout**: 100
   - **Sender email address**: alarms@sentrysecurity.com
   - **Sender display name**: Sentry Security
3. Test the email settings by entering a **Test email address** and clicking the **Test email settings** button.

   To validate that the email settings will work for sending automated event emails, ensure that you test from the Protege GX server machine.
4. Click **Save**.

Creating the Email-on-Event Action

Finally we can create the action record which instructs Protege GX to send emails when selected events occur.

1. Navigate to **Events | Actions**.
2. **Add** a new action called Aperture email-on-event.
3. Set the **Type** to Send email.
4. Set the **Event filter** to Aperture Event Notifications.
5. Enter the **Email address** which will receive the email. For this scenario, we want to send emails to both the showroom manager and CEO, so we will enter two email addresses separated by a comma: caroline@apertureappliance.com, cave@apertureappliance.com

   For testing purposes you may enter your own email address.
6. The automated emails should include relevant information so that the recipients immediately know what has happened on site. We can achieve this by using field variables. These can be used to include key information such as the event time, description and other details.

   For this scenario, we will enter the following settings:
   - **Subject**: Alarm in Aperture Showroom
   - **Message**: <DESCRIPTION> at <FIELDTIME>. Sentry Security is investigating the incident and will contact you shortly.

   For a full list of field variables, see the appendix (see page 13).
7. Click **Save**.

Validating the Event Notifications

Once the alarm and action records are completed we can test the operation by generating our selected alarm events. Ensure that you have Protege GX running on both workstations.

1. Make sure the Showroom area is armed using a keypad or the Protege GX interface.
2. Open the Showroom PIR input. The area should go into alarm.
3. You will see a popup window appear on the first workstation, showing the event:
   ```
   Area Showroom Alarm Activated
   ```
   The workstation should play your custom alarm sound.
4. To acknowledge the alarm, right click on the event and select **Acknowledge alarm**.
5. Enter a comment in the field, and click **OK**. You cannot acknowledge the alarm until you have entered the comment.
6. In addition, after a short delay you should receive an email with the following information:
   - **Subject**: Alarm in Aperture Showroom
   - **Message**: Area Showroom Alarm Activated at 7/29/2021 5:32:53 AM. Sentry Security is investigating the incident and will contact you shortly.
7. Navigate to **Monitoring | Status page view** and select the **Alarms** status page.
8. In the **All acknowledged alarms** section, you should see the showroom alarm event listed, along with the comment you made when you acknowledged the alarm.
9. Make sure the Showroom Door is locked, then open the Showroom Door Sense input to force the Showroom Door.
10. On the first workstation, you should receive both an alarm popup and a camera popup showing live and recorded footage from the event (if there is no physical camera connected, this will say Failed to retrieve camera image).
    You should receive an email with the event details:
    ```
    Door Showroom Door Forced Open
    ```
11. Do not acknowledge the alarm immediately.
12. After 2 minutes the alarm and camera popups should appear on the second workstation.
13. Acknowledge the alarm on the second workstation.
14. Repeat the testing with the Office area and Office Door.

Appendix: Email Field Variables

Email-on-event actions support a number of field variables which can be entered in the **Subject** or **Message** fields. When the email is sent each placeholder will be substituted with information from the triggering event. This allows you to send relevant and useful information to recipients instead of a generic message.

Field variables are case sensitive.

Field Variable	Information
<EVENTID> or <EVENT_ID>	The Database ID of the logged event.
<FIELDTIME> or <FIELD_TIME>	The field time, or time the event was generated at the controller.
<LOGGEDTIME> or <LOGGED_TIME>	The logged time, or time the event was logged by the server.
<DESCRIPTION>	The description or full text of the event as it appears in the event log.
<DESCRIPTION2>	The description of the event in the second language.
<DOORNAME> or <DOOR_NAME>	The name of the door involved with the event.
<USERNAME> or <USER_NAME>	The name of the user involved with the event.
<USERID> or <USER_ID>	The Database ID of the user involved with the event.
<FACILITYNUMBER> or <FACILITY_NUMBER>	The facility number of the user credential involved with the event.
<CARDNUMBER> or <CARD_NUMBER>	The card number of the user credential involved with the event.
<ALARM>	A binary value that indicates whether the event is classed as an alarm. • **0** = The event is not an alarm. • **1** = The event is an alarm.
<INSTRUCTIONS>	The text of the **Instructions** field for alarms.
<INSTRUCTIONS2>	The text of the **Instructions 2** field for alarms (instructions in the second language).
<ACKNOWLEDGED>	A binary value that indicates whether the event has been acknowledged. This only applies to alarms. • **0** = The alarm has not been acknowledged. • **1** = The alarm has been acknowledged.
<COMMENTS>	The text of any comments made by the operator who acknowledged the alarm.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.