Bosch Control Panel Integration Guide

5.3

Genetec

Copyright notice

Document information

Document title: Bosch Control Panel Integration Guide 5.3

Document number: EN.500.010-V5.3.C1(1)

Document update date: June 18, 2015

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide describes how to integrate Bosch intrusion panels in Security Center, and how to monitor them in Security Desk. This guide supplements Security Center and Bosch documentation.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip**. Suggests how to apply the information in a topic or step.
- **Note**. Explains a special case, or expands on an important point.
- **Important**. Points out critical information concerning a topic or step.
- **Caution**. Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning**. Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Topics appearing in this guide that reference information found on third-party websites were accurate at the time of publication, however, this information is subject to change without prior notice to Genetec.

Contents

1

Introduction to Bosch intrusion panel integration

This section includes the following topics:

Bosch control panel integration

The Security Center Intrusion Manager role integrates Bosch control panels into Security Center for centralized monitoring, control, and reporting.

The integration allows you to do the following:

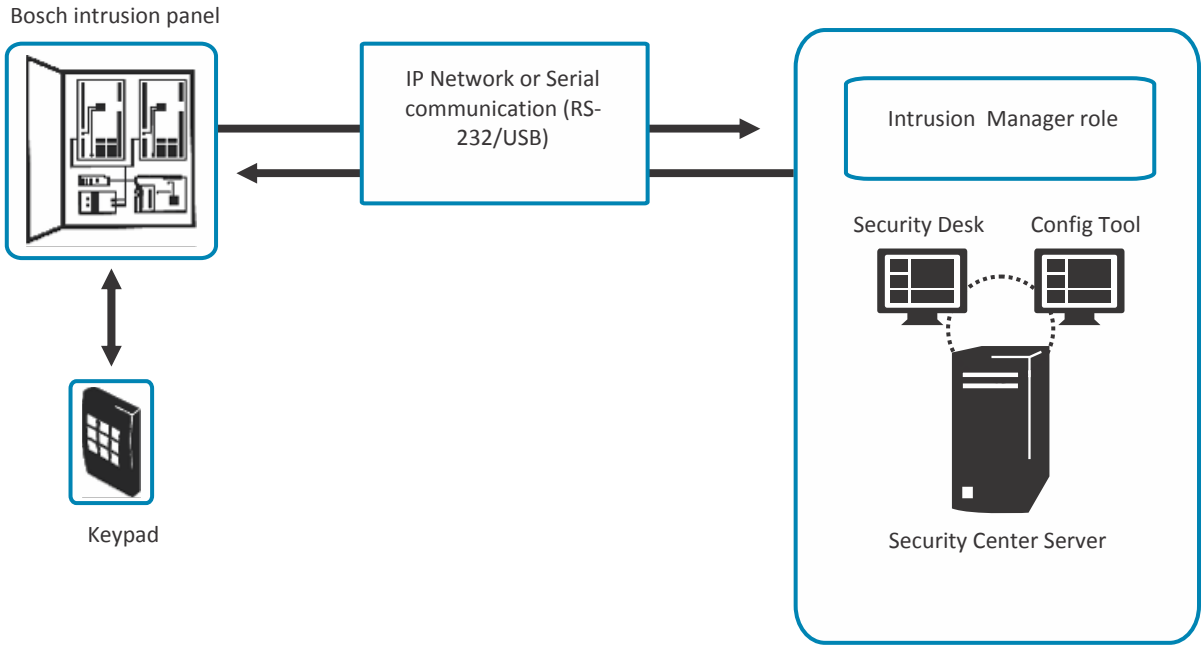
- Map Bosch control panels to Security Center intrusion detection units.
- Monitor intrusion detection area state changes in real-time in Security Desk.
- Monitor the status of intrusion detection units and intrusion detection areas in real-time, using the System status task.
- Monitor intrusion detection units and intrusion detection areas using Plan Manager.
- Receive events and alarms from the control panel, and monitor them in Security Desk.
- Create event-to-actions for events that are sent from the panel.
- Generate reports on activities related to intrusion detection areas and intrusion detection units.
- Generate reports on events related to intrusion detection units.
- Attach cameras to intrusion detection areas to view recorded video associated with events and alarms from the panel.
- Manually arm and disarm the intrusion detection areas defined on your panel in Security Desk using the intrusion detection area widget.

For more information about monitoring events, alarms or intrusion detection units, the intrusion detection area widget, triggering hot actions, monitoring the status of entities in your system using the *System status* task, or using the *Intrusion detection area activities* or *Intrusion detection unit events* task, see the *Security Desk User Guide*. You can access this guide by clicking **F1** in Security Desk.

How Bosch control panel integration works

Bosch control panels are integrated to Security Center using the Intrusion Manager role.

The Intrusion Manager role receives events from the panel over an IP network or serial connection, reports them live in Security Desk, and logs them in a database for future reporting. The role also relays user commands to the panel (such as arming and disarming the intrusion detection areas), and triggers the outputs connected to the panel through event-to-actions (for example, an *Intrusion detection area master armed* event in Security Center can trigger an output on the panel).



Disarming intrusion detection areas when alarms are active

When an intrusion detection area currently in alarm is disarmed from the Monitoring task in Security Desk, Security Center automatically sends an arming command followed by a disarming command to the panel to acknowledge the alarm. This way you do not have to physically go to the panel keypad to acknowledge the alarm. However, this feature includes the following limitations:

- You can only acknowledge *Burglary* alarms from Security Desk. *Fire* alarms must be acknowledged using the panel keypad.
- Because of the arming and disarming commands that Security Center sends to panel, corresponding *armed* and *disarmed* events might be triggered in the system and might be visible in the Monitoring task and in reports.

How Bosch control panel terminology is used in Security Center

Bosch intrusion detection components are mapped as entity types in Security Center.

The following table lists some Bosch control panel components and terms, and how they are represented in Security Center.

Item	Bosch term	Security Center term
Input states	Normal	Normal
	Shorted, Open, Missing, Trouble, FireTrouble	Trouble
	FireAlarm, Alarm	Active
Intrusion area states	AreaNotInUse	Offline
	MasterArmed. MasterInstantArmed	MasterArmed
	PerimeterInstantArmed, PerimeterDelay	PerimeterArmed
	PerimeterExitDelay, AreaExitDelay	Arming
	Disarmed	Disarmed
	AreaPointsNotReadyToArm(0)	ReadyToArm
	Area has an input in a trouble state	Trouble
	Fire, FireTrouble, FireSupervisory, Burglar, BurglarTrouble, BurglarSupervisory	AlarmActive
Logged events	Duress	IntrusionAreaDuressEvent
	PointBypass	InputBypassed(On)
	BypassRestore	InputBypassed(Off)
	StatusAlarm, FireAlarm, Alarm	IntrusionAreaStateLog(AlarmActive)
	PointTrouble	InputStateLog(Trouble)
	PointRestoral	InputStateLog(Normal)
	OpeningReport	IntrusionAreaAlarmCanceledEvent

Item	Bosch term	Security Center term
	ClosingReport	IntrusionAreaStateLog(MasterArmed)
	ACFail	ACFailureLog(true)
	ACRestoral	ACFailureLog(false)
	BatteryMissing, BatteryLow	BatteryFailureLog(true)
	BatteryRestoral	BatteryFailureLog(false)
	StatusPerimeterInstantByArea, PerimeterInstantByAreaArmed	IntrusionAreaStateLog(PerimeterArmed)
	StatusPerimeterDelayByArea, PerimeterDelayByAreaArmed	IntrusionAreaStateLog(MasterArmed)

Supported number of Bosch devices and entities

The following table lists the number of intrusion detection units, intrusion detection areas, inputs, and outputs that are supported with Bosch control panel integration in Security Center.

D9412GV4	Per Intrusion Manager role	10	320	2460	1310
	Per Directory	200	1600	49200	26200
D9412GV2 D9412GV3[a]	Per Intrusion Manager role	10	80	2460	1310
	Per Directory	200	1600	49200	26200
D7412GV2 D7412GV3 D7412GV4	Per Intrusion Manager role	10	80	750	640
	Per Directory	200	1600	15000	12800
D7212GV2 D7212GV3 D7212GV4	Per Intrusion Manager role	10	40	400	270
	Per Directory	200	800	8000	5400

[a]A firmware limitation prevents the panel to support more than 8 areas.

Supported features with Bosch control panel integration

The following table lists the Security Center intrusion detection features that are supported with the Bosch control panel integration.

Feature		Supported
RS-232 serial connection		Yes
TCP/IP connection		Yes
Data encryption over TCP/IP		No
Authentication between control panel and server		No
Get input bypass status		Yes
Set input bypass status		Yes
Arm/disarm from Security Center	Instant arming/ disarming	Yes
	Delayed arming	Yes
Use control panel inputs in virtual zones		Yes
Trigger outputs on control panels		Yes
Discover intrusion detection areas and devices automatically		Yes
Create intrusion detection areas automatically in Security Center		Yes
Create input entities automatically in Security Center		Yes
Create output entities automatically in Security Center		Yes
Link input entities to intrusion detection areas automatically in Security Center		Yes
Download Offline logs automatically on connection		Yes
Clear offline logs manually		No
Trigger alarms on the control panel from Security Center		Yes (GV4 v2 panels only)
Create custom Security Center events tied to panel pin events		No

Feature		Supported
Monitor Security Center Server connection from the intrusion panel		No
Intrusion detection unit events	Unit connected	Yes
	Unit Lost	Yes
	AC fail	Yes
	Battery fail	Yes
	Input supervision trouble	Yes
	Input bypass activated	Yes
	Input bypass deactivated	Yes
	Tamper	No
Intrusion detection area events	Master armed	Yes
	Perimeter armed	Yes
	Disarmed	Yes
	Auto-arming postponed	Yes
	Forced arming	Yes
	Input bypass activated	Yes
	Input bypass deactivated	Yes
	Duress	Yes
	Entry delay started	Yes
	Intrusion alarm activated	Yes
Intrusion detection area states	Master armed	Yes
	Perimeter armed	Yes
	Disarmed	Yes
	Ready-to-arm	Yes
	Intrusion alarm active	Yes
	Input trouble	Yes

Feature		Supported
	Arming countdown	Yes
	Entry delay	Yes
Arming commands	Instant master arm	Yes
	Delayed master arm	Yes
	Instant perimeter arm	Yes
	Delayed perimeter arm	Yes
	Forced arm	Yes
	Bypass arm	No
Live input entity state changes	Normal	Yes
	Active	Yes
	Trouble	Yes
	Bypassed	Yes
Report live online/offline control panel status changes		Yes
Report live online/offline control panel status changes on expansion modules		No
Synchronize time zone automatically from the control panel value		Yes

Limitations: Intrusion control panel inputs monitored in Security Center

We recommend that you use intrusion control panels for intrusion monitoring only. If you decide to monitor changes of input states of an intrusion control panel in Security Center, using for example virtual zones or Plan Manager, you must be aware of the following limitations.

- Some changes of input states may not be reported in Security Center.

  The main purpose of an input on an intrusion panel is to raise an alarm when its state changes. When the input becomes active while its intrusion area is armed, the panel will raise an alarm. Security Center then uses this alarm to trigger an *Intrusion detection area alarm activated* event. You can always decide to monitor changes of input states of an intrusion control panel, using virtual zones or Plan Manager for example, but some changes may not be detected if they occur too quickly. Because of this, events configured in a virtual zone may not be triggered, or inputs displayed in Plan Manager may not reflect their actual state.

  NOTE: The panel will always raise intrusion alarms even though changes of input states may not be reported in Security Center.

- It can take some time to receive changes of input states in Security Center.

  Intrusion control panels have limitations in the number of events they can report and how fast they can transmit them.

BEST PRACTICE: Intrusion control panels are not designed to capture rapid consecutive state changes on their inputs, such as doors being opened and closed rapidly, or motion sensors being saturated with detected movements. Make sure the inputs you want to monitor will not have their state changed too quickly for the panel your are using.

2

Configuring Bosch intrusion panels in Security Center

This section includes the following topics:

Installation and configuration overview

The following table summarizes the configuration process for the Bosch control panel integration:

Phase	Description	See
1	Before you start installing and configuring Bosch intrusion panels, you should understand the relationship between Bosch terms and Security Center entities.	How Bosch control panel terminology is used in Security Center on page 4
2	Read all the required information, and perform all the required tasks before integrating the Bosch control panel in Security Center.	• Preparing to integrate Bosch control panels on page 13
3	Set up communication between Security Center server and the Bosch control panel using an IP network, or a Serial connection, and configure the panel settings.	• Configuring the panel for IP communication on page 15 • Configuring the panel for serial communication on page 24
4	(Optional) Add an expansion board to your intrusion panel. For a list of supported expansion boards, see the *Security Center Release Notes*.	For information about installing an expansion board, see your Bosch manufacturer documentation.
5	Create the Intrusion Manager role in Security Center to manage the intrusion detection unit.	Creating the Intrusion Manager role on page 27
6	Create the Bosch control panel as an intrusion detection unit in Security Center.	Creating the intrusion detection unit on page 29
7	Configure the intrusion detection unit properties, such as interface type, status update interval, clock synchronization, and so on.	Configuring intrusion detection unit properties on page 31
8	Configure the inputs and outputs controlled by the control panel.	Configuring inputs and outputs on page 33
9	Map Security Center cameras to intrusion detection areas.	Mapping intrusion detection areas to cameras on page 37
10	Configure Security Center to be able to trigger an intrusion detection alarm on a selected intrusion detection area in Security Desk.	Configuring intrusion alarms on areas (Bosch GV4 v2 panels) on page 36
11	(Optional) Create events-to-actions, for Bosch control panel events received in Security Center to trigger actions.	Mapping control panel events to Security Center actions on page 38
12	(Optional) Monitor your intrusion detection areas using a Plan Manager map.	For information about creating and using maps in Plan Manager, see the *Plan Manager User Guide*.

Preparing to integrate Bosch control panels

Before integrating Bosch control panels in Security Center, you need to perform a series of pre-configuration steps.

Before integrating Bosch control panels:

1 Read the release notes for any known issues, limitations, supported firmware, and other information about this release.

For more information, see the *Security Center Release Notes*.

2 Make sure your system meets Security Center and Bosch requirements.

For more information, see the *Security Center Release Notes* and your Bosch documentation.

3 Make sure you have the proper license.

To use the panels in Security Center, your license must include the correct "Number of Intrusion detection units" you want to control. For more information about licensing, see Genetec Technical Support.

4 Make sure you have the right user privileges.

5 Do one of the following:

- Configure the control panel for IP communication.
- Configure the control panel for serial communication.

Related Topics

Configuring the panel for IP communication on page 15
Configuring the panel for serial communication on page 24

Best practices for connecting intrusion control panels to the network

Intrusion detection panels are not typically designed to withstand heavy traffic from the network, especially when broadcast messages occur frequently. Because the panel needs to process incoming packets to check whether it is the recipient, this might lead to increased demand on processing resources. Under heavy network load conditions, you might notice that the panel drops offline and reconnects repeatedly.

To avoid this behavior, we recommend to connect the panel to Security Center through an isolated network to isolate the panel from traffic for which it is not the recipient. Many panels can be connected to the same isolated network, as long as the network is not also the hub for other traffic which does not involve the panels.

You can build an isolated network by adding a dedicated hardware network node (switch or router), or by creating a dedicated Virtual Local Area Network (VLAN) on a network node that provides such configuration capabilities.

Required Security Center user privileges for control panel integration

To use control panels in Security Center, you require the right user privileges.

The following table lists the minimum user privileges you require to monitor and control control panels in Security Center.

NOTE: You may require more, depending on the tasks you want to perform in Config Tool and Security Desk.

Privilege	Task
Config Tool	To use Config Tool.
Security Desk	To use Security Desk.
Monitoring	To use the Monitoring task in Security Desk.
Intrusion detection	To use the Intrusion detection task in Security Desk.
Intrusion detection area activities	To use the Intrusion detection area activities task in Security Desk.
Intrusion detection unit events	To use the Intrusion detection unit events task in Security Desk.
Alarm monitoring	To use the Alarm monitoring task in Security Desk.
Alarm report	To use the Alarm report task in Security Desk.
Acknowledge alarms	To acknowledge active alarms in Security Desk.
Forward alarms	To forward alarms in Security Desk.
Snooze alarms	To snooze active alarms in Security Desk.
Trigger alarms	To trigger alarms in Security Desk.
Arm/disarm intrusion detection areas	To arm or disarm the intrusion panel from Security Desk.
View intrusion detection areas	To view the intrusion detection area configuration pages in Config Tool.
View intrusion detection units	To view the intrusion detection area configuration pages in Config Tool.
Modify alarms	To modify alarm configuration settings in Config Tool.
Add/delete alarms	To add or delete alarms in Config Tool.

Configuring the panel for IP communication

For Security Center to communicate with the Bosch control panel through an IP network, you must connect the panel to an Ethernet module, and then configure the panel settings using the Bosch Management Remote Programming Software (RPS) before you add the unit in Security Center.

To configure the panel for IP communication:

1 Select one of the supported Ethernet modules.

2 Enable communication between the Bosch Management Remote Programming Software (RPS) and the panel.

The steps required to enable communication with the Bosch RPS differ whether you are using the DX4020 or the B426 Ethernet module.

3 Configure the panel settings using the Bosch RPS.

4 Enable communication between Security Center and the panel.

The steps required to enable communication with Security Center differ whether you are using the DX4020 or the B426 Ethernet module.

The panel can now communicate with Security Center.

Ethernet modules you can use

Bosch control panels can communicate with Security Center through an IP network using the Conettix DX4020 or B426 Ethernet Network Interface Module. The Ethernet module you should use depends on the panel model and firmware you are using.

The following table lists your options.

Ethernet module	GV2	GV3	GV4
DX4020	Yes	Yes	No
B426	Yes	Yes	Yes

Enabling communication with Bosch RPS using the DX4020

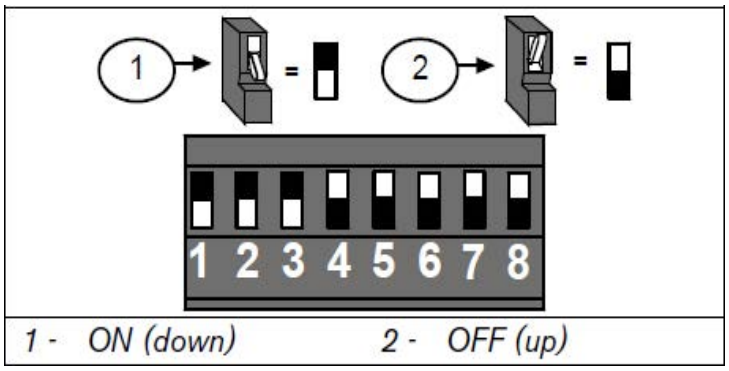
If you have a Bosch GV2 or GV3 control panel, you can enable communication with Bosch RPS using the DX4020.

To enable communication with Bosch RPS using the DX4020:

1 Connect the DX4020 Ethernet module to the panel using the SDI connector.

For information about connecting the Ethernet module to the panel, see “3.0 Installation” in the *Bosch Conettix DX4020 Installation Guide*.

2 Configure the DIP switches on the Ethernet module as follows:

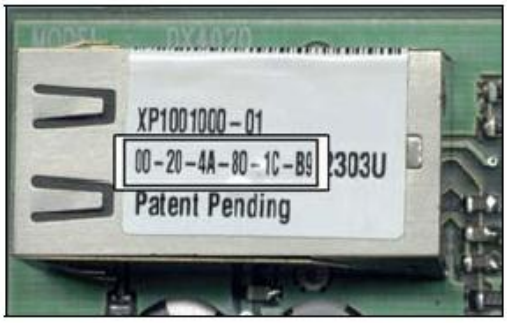


3 Set the IP address for the DX4020 Ethernet module.

The default IP configuration is as follows:

- IP configuration number: DHCP
- Port: 7700
- DHCP device name: Cxxxxxx

Where xxxxxx is the last 6 digits of the MAC address located on the XPort connector.



To assign an IP address on the DX4020 Ethernet module, see sections “6.3 Obtaining an IP address”, and “6.4 Assigning the Initial IP address” in the *Bosch Conettix DX4020 Installation Guide*.

4 On your computer, open the Windows Command Prompt.

5 Type `Telnet <DX4020 IP address> 9999`.

6 To go into setup mode, press **ENTER**.

7 Press **1** to configure Channel 1, and enter the following values:

NOTE: For the settings not listed here, use the default value.

- Baudrate: 9600
- I/F Mode: 4C
- Flow: 00
- Port: 7700
- Connect Mode: CC
- Datagram: 02
- Remote IP Adr: 127.0.0.1:0000
- Disconn Mode: 00
- Flush Mode: 00

8 In the main setup screen, press **9** to save your changes and exit.

You can now connect to the panel using the Bosch Management RPS.

After you finish

Configure the panel settings.

Enabling communication with Bosch RPS using the B426

If you have a Bosch GV2, GV3, or a GV4 panel, you can enable communication with Bosch RPS using a B426 Ethernet module.

Before you begin

- Make sure that Web access is enabled on the B426.
- Make sure that encryption and security options are disabled on the B426.

To enable communication with Bosch RPS using the B426:

1 Using the dial on the Ethernet module, set the address switch to **0**.

2 Connect the Ethernet module to the panel using one of the following:

- If you have a GV4: Connect to the B426 using an SDI or SDI2 connector.
- If you have a GV2 or GV3: Connect to the B426 using an SDI connector.

For more information about connecting the B426 Ethernet module to the panel, see your Bosch documentation.

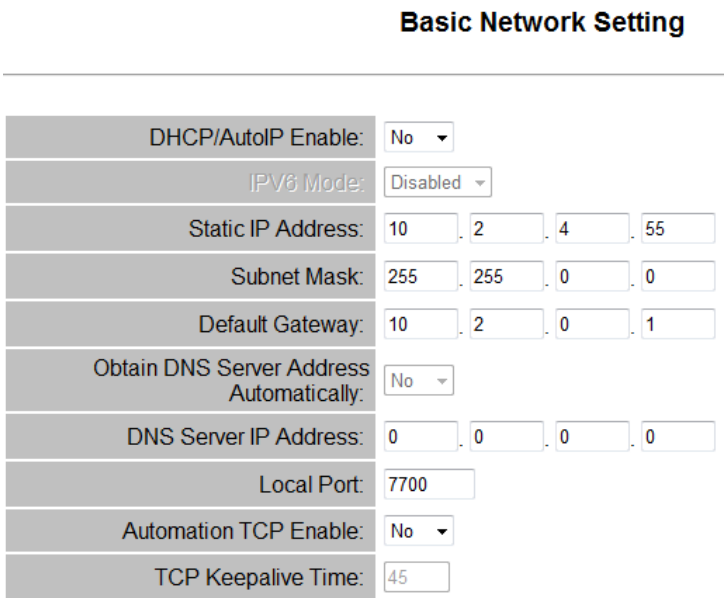
3 Open the B426 Web page, using the following URL: *http://<B426 IP address>*.

NOTE: If you do not know the IP address of the Ethernet module, you can type the host address (B + the last 6 digits of the unit MAC address). For more information about setting the IP address or locating the MAC address, see your Bosch documentation.

4 Log on using the default password: **B42V2**.

5 From the Home page, click the **Basic Network Settings** page.

6 From the **Automation TCP Enable** option drop-down list, select **No**.



7 Click **OK**, and then click **Save and Execute**.

8 Disconnect the cable from the SDI or SDI2 connector.

9 Using the dial on the Ethernet module, set the address switch to **4**.

10 Reconnect the cable using the SDI or SDI2 connector.

You can now connect to the panel using the Bosch Management RPS.

After you finish

Configure the panel settings.

Configuring the panel settings using Bosch RPS

Before integrating Bosch control panels to Security Center, you must configure the panel settings, such as the intrusion areas, inputs and outputs, and other behavior, using the Bosch Management Remote Programming Software (RPS).

Before you begin

- Make sure you have the Bosch RPS installed. If you are using the Bosch GV4 panel, you require Bosch RPS version 5.14.4 or later.
- Make sure you can connect to the panel using the Bosch Management RPS.

To configure the panel settings using Bosch RPS:

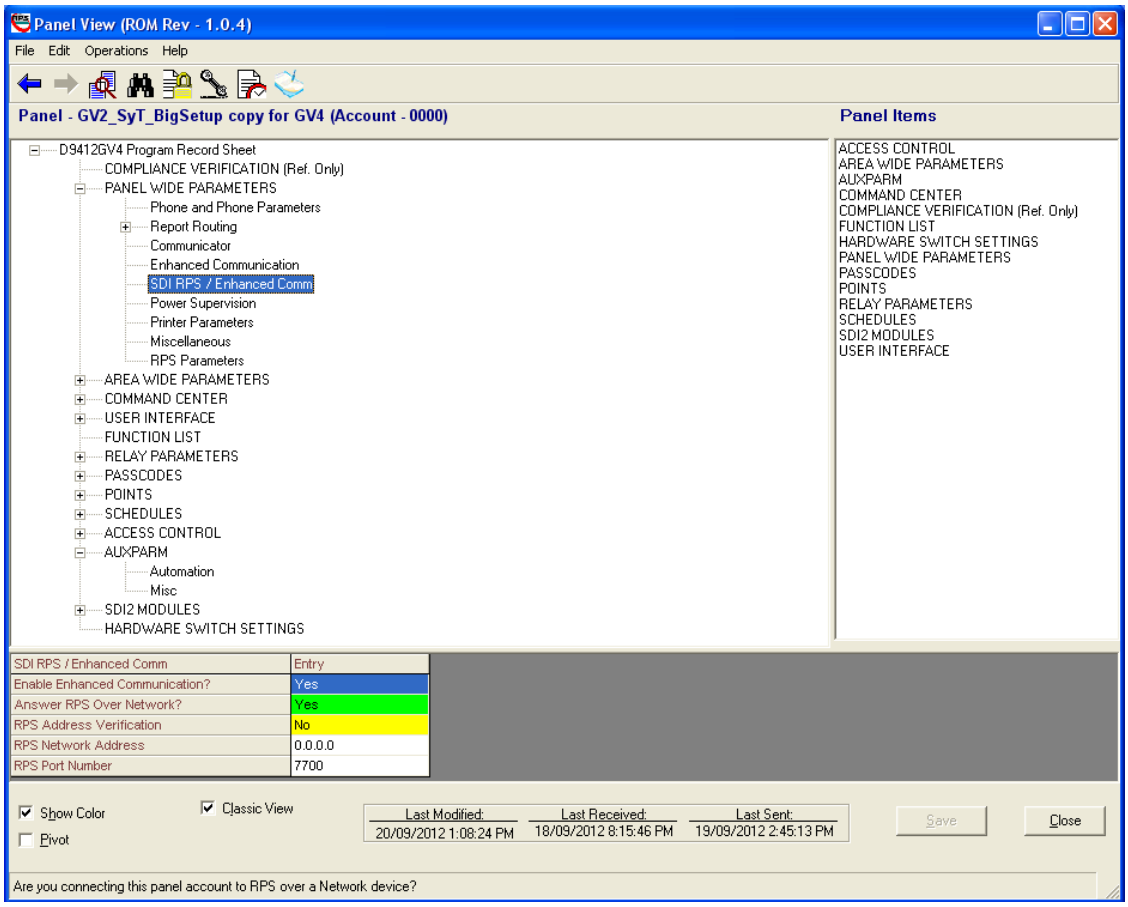
1 On your computer, open the Bosch Management RPS.

2 Click **New**, and select the panel model (for example, **D9412GV4**).

3 In the **Panel Info** tab, type a name for the panel.

4 Double-click on the panel row, and then click **Connect**.

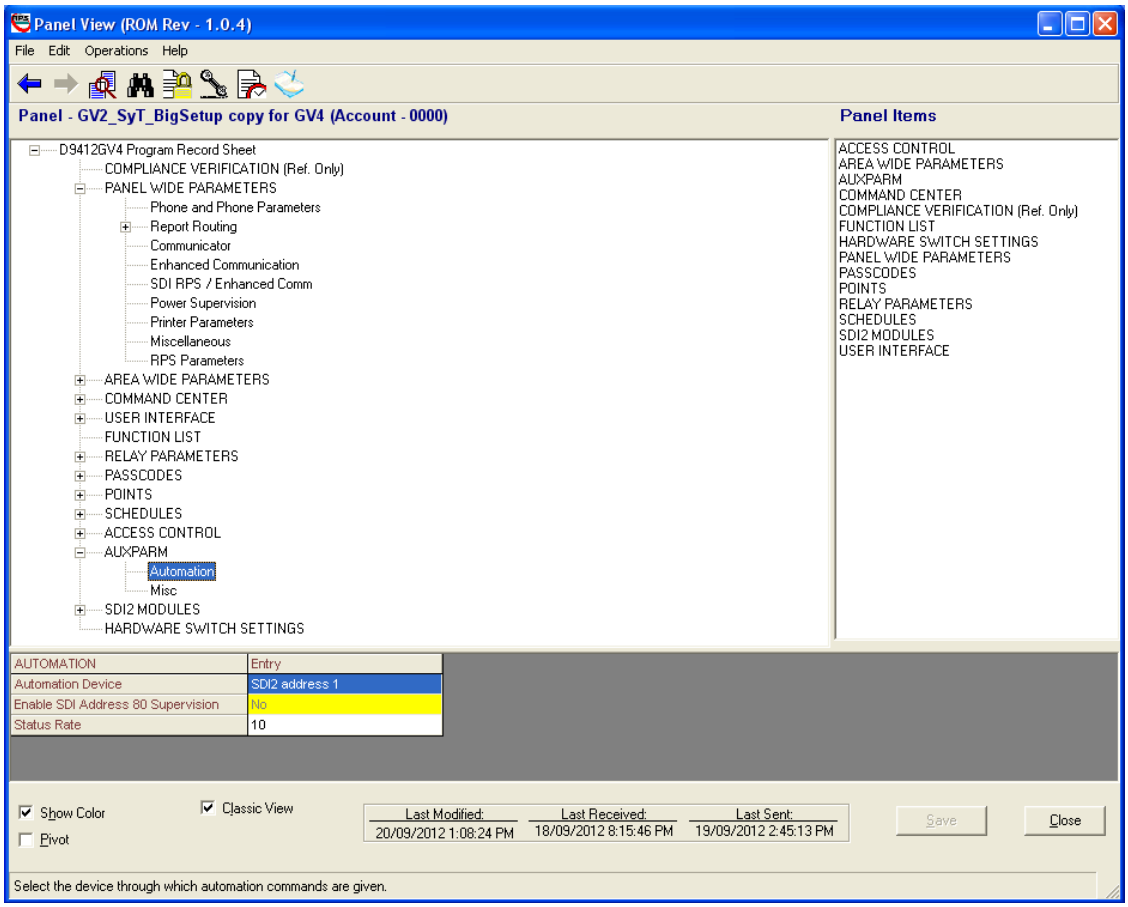
5 In the **Panel View** page, click **PANEL WIDE PARAMETERS** > **SDI RPS/ENHANCED Comm**, and then set the **Enable Enhanced Communication** option to **Yes**.



6 Click **Save**.

7 In the **Panel View** page, click **AUXPARM** > **Automation**, and then set the **Automation Device** option as follows:

- **B426:** If you are using a GV4 with an SDI2 connector: **SDI2 address 1**.
- **B426:** If you are using a GV4 with an SDI connector: **SDI address 80**.
- **B426:** If you are using a GV2/GV3 with an SDI connector: **SDI address 80**.
- **DX4020:** If you are using a GV2/GV3 with an SDI connector: **SDI address 80**.



8 Click **Save**.

9 Define the panel's inputs, outputs, areas, and other behavior.

For more information about configuring the panel using the Bosch RPS, see your Bosch documentation.

10 Click **Connect**, and then send the updated settings to the panel.

11 Reset the panel.

Related Topics

Enabling communication with Bosch RPS using the DX4020 on page 15

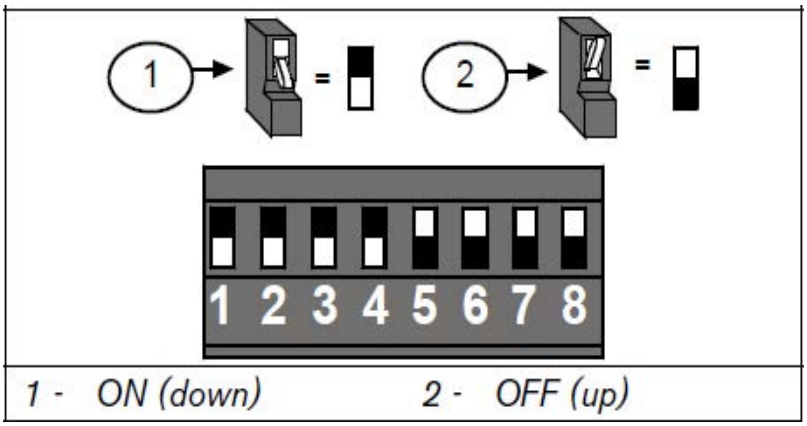
Enabling communication with Bosch RPS using the B426 on page 17

Enabling communication with Security Center using the DX4020

Before enrolling a GV2 or GV3 panel into Security Center, you must re-configure the DIP switches on the Ethernet module, and the panel's telnet console settings.

To enable communication with Security Center using the DX4020:

1 Configure the DIP switches on the Ethernet module as follows:



2 Configure the panel's Telnet console settings as follows.
   a) Open the Windows Command Prompt.
   b) Type `Telnet <DX4020 IP address> 9999`.
   c) To go into setup mode, press **ENTER**.
   d) Press **1** to configure Channel 1, and enter the following values:

      NOTE: For the settings not listed here, use the default value.

      - Baudrate: 9600
      - I/F Mode: 4C
      - Flow: 00
      - Port: 3001 (This is the default port used by Security Center)
      - Connect Mode: C0
      - Enable the '+++' in **Modern Mode**.
      - Disable the **Auto increment source port.**
      - Datagram: 02
      - Remote IP Adr: 127.0.0.1:0000
      - Disconn Mode: 00
      - Flush Mode: 00

   e) In the main setup screen, press **9** to save your changes, and to exit.

The panel can now communicate with Security Center.

After you finish

Create an Intrusion Manager role in Security Center.

Enabling communication with Security Center using the B426

If you have a Bosch GV2 panel with firmware version 7.06, a GV3 panel with firmware version 8.02, or a GV4 panel, you can enable communication with Security Center using a B426 Ethernet module.

Before you begin

Make sure that encryption and security options are disabled on the B426.

To enable communication with Security Center using the B426:

1 Disconnect the cable from the SDI or SDI2 connector.

2 Using the dial on the Ethernet module, set the address switch to **0**.

3 Connect the Ethernet module to the panel using one of the following:

- If you have a GV4: Connect to the B426 using an SDI or SDI2 connector.
- If you have a GV2 or GV3: Connect to the B426 using an SDI connector.

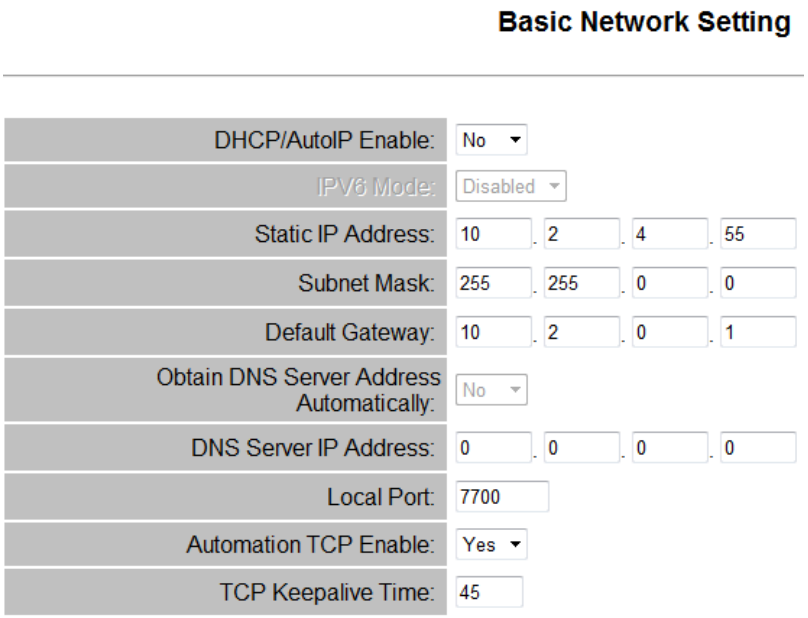
For more information about connecting the B426 Ethernet module to the panel, see your Bosch documentation.

4 Open the B426 web page, using the following URL: *http://<B426 IP address>*.

5 Log on using the default password: **B42V2**.

6 From the Home page, click the **Basic Network Settings** page.

7 From the **Automation TCP Enable** option drop-down list, select **Yes**.



8 Click **OK**.

9 Click the **Maintenance** page.

10 From the **Panel Programming Enable** option drop-down list, select **No**.

Disabling the *Panel Programming Enable* option ensures that your custom settings on the B426 are maintained when you connect to Security Center.

11 Click **OK**, and then click **Save and Execute**.

12 Disconnect the cable from the SDI or SDI2 connector.

13 Using the dial on the Ethernet module, set the address switch to the following:

- If you are using a GV4 with an SDI2 connecter: **1**.
- If you are using a GV2/GV3/GV4 with an SDI connector: **3**.

14 Reconnect the cable using the SDI or SDI2 connector.

The panel can now communicate with Security Center.

After you finish

Create an Intrusion Manager role in Security Center.

Disabling encrypted communication using the B426

For Security Center to be able to communicate with the B426 Ethernet module, you must disable the **Encryption Enable** and **Web and Automation Security** options on the module via its web interface.

To disable encrypted communication using the B426:

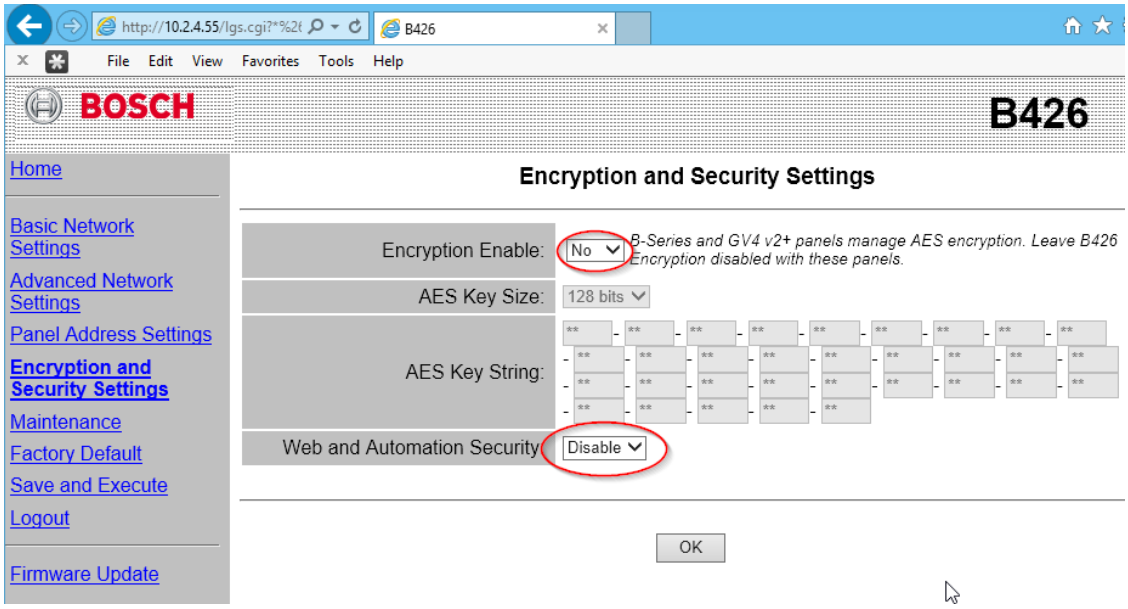
1 Open the B426 web page, using the following URL: *http://<B426 IP address>*.
If you cannot connect to the module using *http://*, try to connect with *https://* instead.

2 Log on using the default password: **B42V2**.

3 From the Home page, click the **Encryption and Security Settings** page.

4 From the **Encryption Enable** option drop-down list, select **No**.

5 From the **Web and Automation Security** option drop-down list, select **Disable**.



6 Click **OK**, and then click **Save and Execute**.

Security Center should now be able to communicate with the module.

Configuring the panel for serial communication

For Security Center to communicate with the Bosch control panel using a serial connection, you must connect the panel to the DX4010V2 serial module using an RS-232 or USB cable, and then configure the panel settings using the Bosch Management Remote Programming Software (RPS).

To configure the panel for serial communication:

1 Make sure the serial module is compatible with your panel.
2 Configure the settings on the panel using the Bosch RPS.
3 Enable communication between Security Center and the panel.

The panel can now communicate with Security Center.

Serial module compatibility

Bosch control panels can communicate with Security Center using the DX4010V2 serial module.

The following table lists your options.

Serial module	GV2	GV3	GV4
DX4010V2	Yes, with SDI only (SDI2 is not supported)	Yes, with SDI only (SDI2 is not supported)	Not supported

Configuring the panel settings using Bosch RPS

Before integrating Bosch control panels to Security Center, you must configure the panel settings, such as the intrusion areas, inputs and outputs, and other behavior, using the Bosch Management Remote Programming Software (RPS).

Before you begin

- Make sure you have the Bosch RPS installed. If you are using the Bosch GV4 panel, you require Bosch RPS version 5.14.4 or later.
- Make sure you can connect to the panel using the Bosch Management RPS.

To configure the panel settings using Bosch RPS:

1 Configure the DIP switches on the Ethernet module as follows:
   - Set switches 1, 2, and 3 on.
   - Set switches 4, 5, 6, 7, and 8 off.
2 Connect the panel to the SDI connector on the DX4010V2 serial module.
3 Do one of the following:
   - If you are using an RS-232 cable, connect the cable to your computer using the COM1 port, and apply power to the panel.
   - If you are using a USB cable, connect the cable to your computer using the COM3 or COM4 port, and apply power to the panel.

NOTE: If your computer does not recognize the USB port, you need to install the *Silicon Labs CP210x USB UART Bridge* driver provided in your kit.

A red LED flashes on the DX4010V2 indicating that the connection is working.

4 On your computer, open the Bosch Management RPS.

5 Click **New**, and select the intrusion panel model (for example, **D9412GV4**).

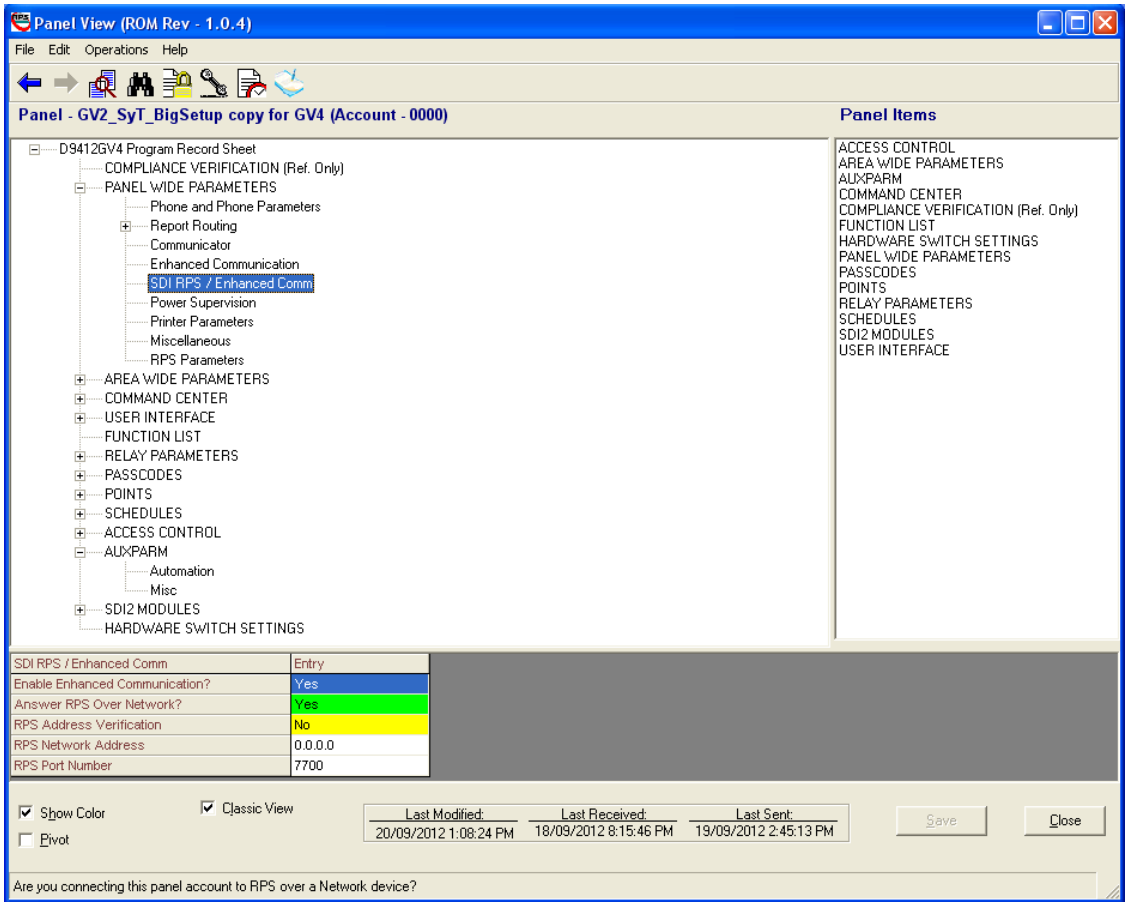
6 In the **Panel Info** tab, type a name for the panel.

7 Double-click on the panel row, and then click **Connect**.

8 In the dialog box that opens, select **Enhanced Direct** connection, and in the **COM Port** field, type the COM port number you used to connect the cable to the computer.

9 Click **OK**.

10 In the **Panel View** page, click **PANEL WIDE PARAMETERS** > **SDI RPS/ENHANCED Comm**, and then set the **Enable Enhanced Communication** option to **Yes**.



11 Click **Save**.

12 In the **Panel View** page, click **AUXPARM** > **Automation**, and then set the **Automation Device** to **SD1 address 80**.

13 Click **Save**.

14 Define the panel's inputs, outputs, areas, and other behavior.

For more information about configuring the panel using the Bosch RPS, see your Bosch documentation.

15 Click **Connect**, and then send the updated settings to the panel.

16 Reset the panel.

Enabling communication with Security Center

Before enrolling the panel into Security Center, you need to re-configure the DIP switches on the DX4010V2 serial module, and then connect your cable.

To enable communication with Security Center:

1 Disconnect the DX4010V2 serial module from the panel.
2 Configure the DIP switches on the serial module as follows:
   - Set switches 1, 2, 3, and 4 on.
   - Set switches 5, 6, 7, and 8 off.
3 Connect the panel to the SDI connector on the DX4010V2 serial module.
4 Do one of the following:
   - If you are using an RS-232 cable, connect the cable to your computer using the COM1 port, and apply power to the panel.
   - If you are using a USB cable, connect the cable to your computer using the COM3 or COM4 port, and apply power to the panel.

     NOTE: If your computer does not recognize the USB port, you need to install the *Silicon Labs CP210x USB UART Bridge* driver provided in your kit.

     A red LED flashes on the DX4010V2 indicating that the connection is working.

The panel can now communicate with Security Center.

After you finish

Create an Intrusion Manager role in Security Center.

Creating the Intrusion Manager role

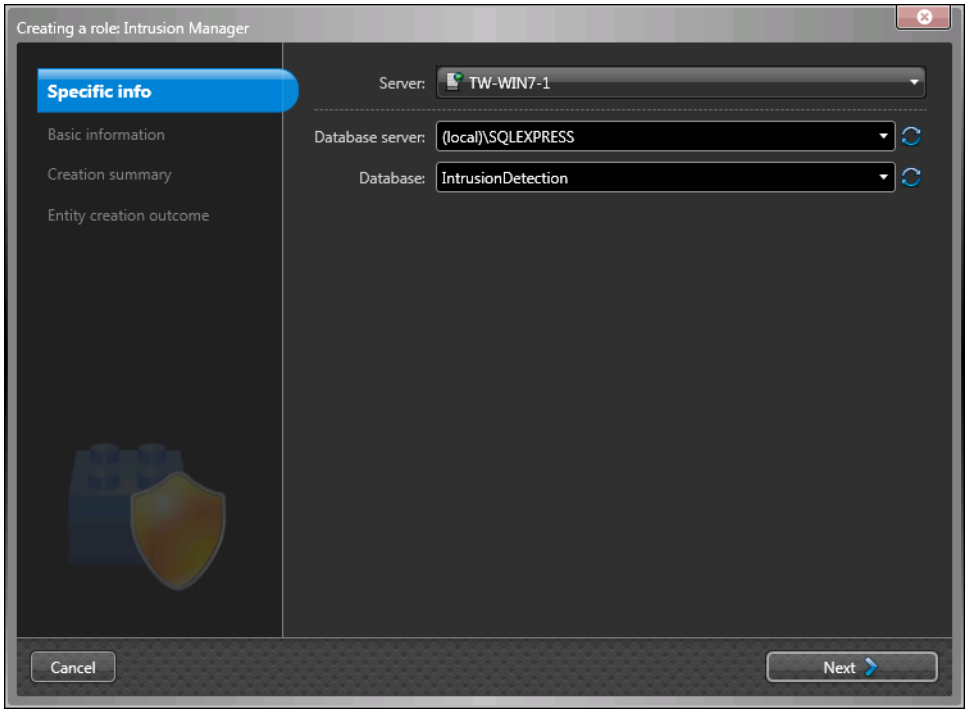
You must create an Intrusion Manager role in Config Tool to manage the panel.

To create an Intrusion Manager role:

1 From the Config Tool home page, open the **System** task.

2 Click **Add an entity** (), and then **Intrusion Manager**.

The *Creating a role: Intrusion Manager* window opens.



3 On the **Specific info** page, do the following:

a) From the **Server** drop-down list, select the server assigned to this role.

NOTE: If no expansion server is present, this option is not available.

b) In the **Database server** field, select or type the name of the database server.

c) In the **Database** field, select or type the name of the database (for example, **IntrusionDetection**).

d) Click **Next**.

4 On the **Basic information** page, do the following:

a) Type the **Entity name** (**Intrusion Manager**)

b) (Optional) Type an **Entity description** for the role.

c) From the **Partition** drop-down list, select an existing partition, or click to create a new partition.

Partitions are logical groupings used to control the visibility of entities. Only users with permission to that partition can view or modify the role.

d) Click **Next**.

5 On the **Creation summary** page, do the following:

a) Verify the information you entered.

b) If everything is correct, click **Create**, or click **Back** to modify your settings.

When the role is created, the following message appears: **The operation was successful**.

6 Click **Close**.

The Intrusion Manager role appears in your entity browser.

After you finish

Add the intrusion panel in Security Center.

Related Topics

Creating the intrusion detection unit on page 29

Creating the intrusion detection unit

To be able use the control panel in Security Center, you must create it as an *intrusion detection unit* in Config Tool.

Before you begin

Create an *Intrusion Manager* role to manage the unit..

To create an intrusion detection unit:

1 From the Config Tool home page, open the **Intrusion detection** task.

2 Click **Intrusion detection unit** ( ).

3 In the **Basic Information** page, do the following:

a) Type the **Entity name** (Intrusion unit).

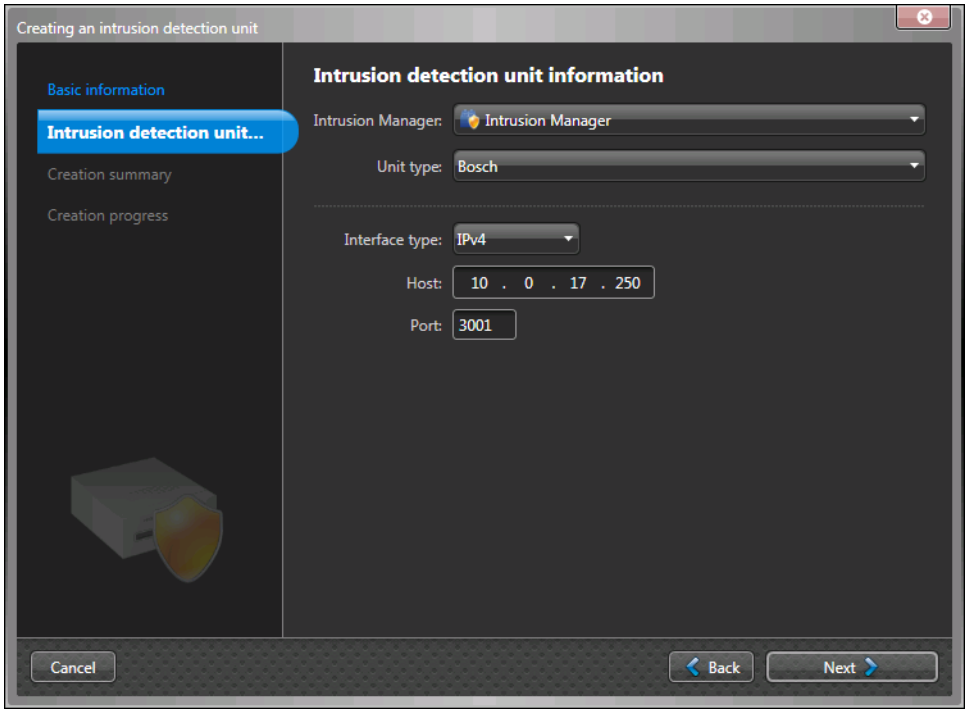
b) (Optional) Type a **description** for the entity.

c) From the **Partition** drop-down list, select an existing partition, or click to create a new partition.

Partitions determine which Security Center users have access to this entity. Only users that are part of the partition can view or modify the intrusion detection unit.

d) Click **Next**.

4 From the **Intrusion Manager** drop-down list, select the *Intrusion Manager* role that will manage the control panel.



5 From the **Unit type** drop-down list, select the manufacturer.

6 In the **Interface type** option, select **IPv4** or **Serial**.

- If you selected **IPv4**, type the **Host** (IP address) and **Port** number you configured on the panel.
- If you selected **Serial**, type the **COM** port used to connect the panel to Security Center.

7 Click **Next**.

8 On the **Creation summary** page, do the following:

a) Verify the information you entered.

b) If everything is correct, click **Create**, or click **Back** to modify your settings.

When the intrusion detection unit is created, the following message appears: **The operation was successful**.

9 Click **Close**.

The intrusion detection unit appears under the Intrusion Manager role in the entity browser. The Intrusion Manager automatically creates the intrusion detection areas (zones and partitions), inputs, and outputs that are configured on the panel.

Related Topics

Creating the Intrusion Manager role on page 27

Configuring intrusion detection unit properties

To receive intrusion events and alarms from the Bosch control panel in Security Desk, you need to configure the intrusion detection unit (panel) in Config Tool.

What you should know

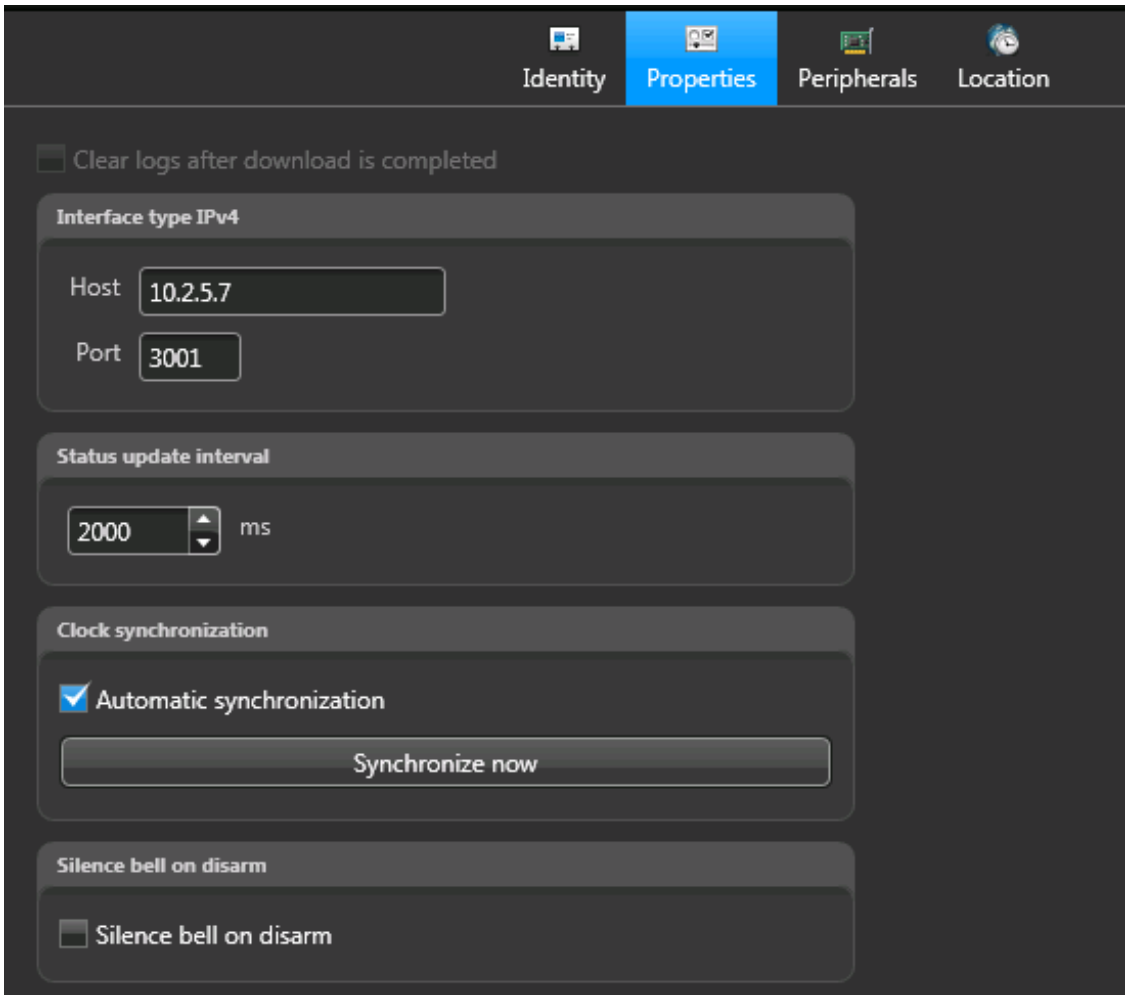
The intrusion detection unit **Properties** tab allows you to modify settings for the panel such as the host address and port, status update interval, clock synchronization and so on.

To configure the intrusion detection unit properties:

1 From the Home page in Config Tool, open the **Intrusion detection** task.

2 Under the Intrusion Manager role in the entity tree, select the intrusion detection unit to configure, and click the **Properties** tab.

NOTE: The **Interface type**, **Host name**, and **Port** fields were configured when you created the intrusion detection unit.



3 Under **Status update interval**, enter how often Security Center polls the panel for a status update. The possible values are 2000 ms up to a maximum of 25500 ms.

IMPORTANT: When you modify this setting, the unit will be restarted.

4 Under **Clock synchronization**, the **Automatic synchronization** option is enabled by default. This option synchronizes the panel with the Security Center server every 60 minutes.

Alternatively, you can clear this option and manually synchronize the panel at any time by clicking **Synchronize now**.

5 Select the **Silence bell on disarm** option if you don't want the siren on the panel to continue beeping once an intrusion detection area is disarmed from Security Desk.

6 If you are using a GV4 v2 panel, you can configure the panel to trigger an intrusion alarm on a selected intrusion detection area.

7 Click **Apply**.

Related Topics

Configuring intrusion alarms on areas (Bosch GV4 v2 panels) on page 36

Configuring inputs and outputs

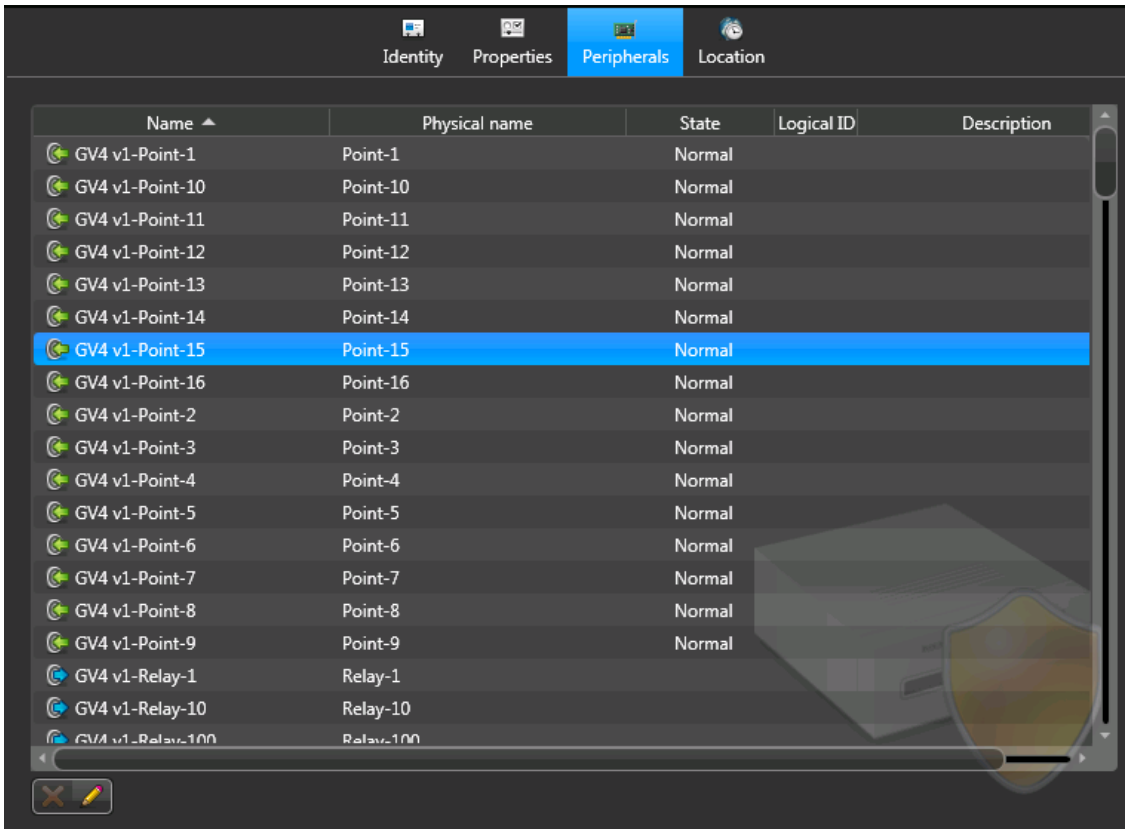
In the intrusion detection unit **Peripherals** tab, you can assign logical IDs and descriptions to the inputs and outputs controlled by the unit. You can also define whether an output monitors the exterior or interior of an area, and its normal contact state.

What you should know

IMPORTANT: Configuration of input and contact types in Security Center is optional. They are displayed for reference only and the changes are not reflected on the panel. Input and contact types must be configured on the panel itself.

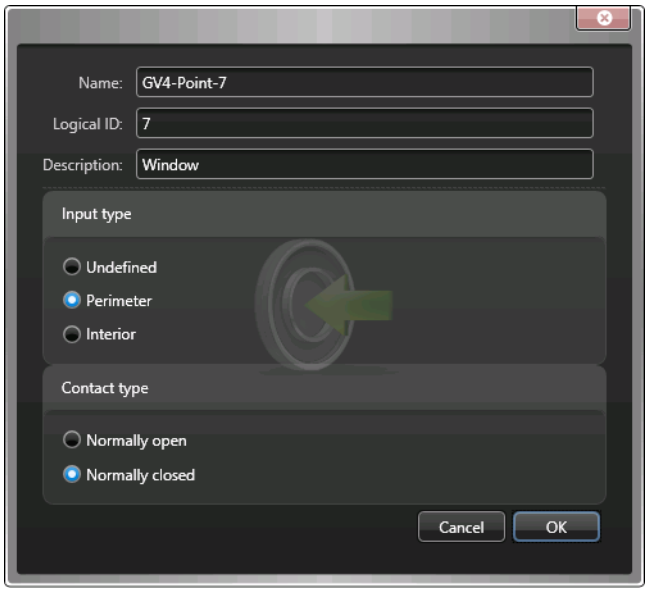
To configure inputs and outputs:

1 From the *Intrusion detection* task in Config Tool, select the intrusion detection unit to configure, and click the **Peripherals** tab.



2 Select an input, and at the bottom of the **Peripherals** tab, click .

A dialog box appears.



3 In the **Name** field, the name of the input is displayed. This is the name of the input connected to the panel.

4 (Optional) Type a **Logical ID** for the input. Setting a Logical ID helps you to easily identify the input in Security Center.

5 (Optional) Type a **Description** for the input.

6 In the **Input type** field, select one of the following options according to the input's configuration on the panel:

- **Undefined:** The input does not have a set type. If you select this option, the input is considered as a *Perimeter* input type.
- **Perimeter:** The input is configured to monitor the perimeter of an intrusion detection area.
- **Interior:** The input is configured to monitor inside the intrusion detection area.

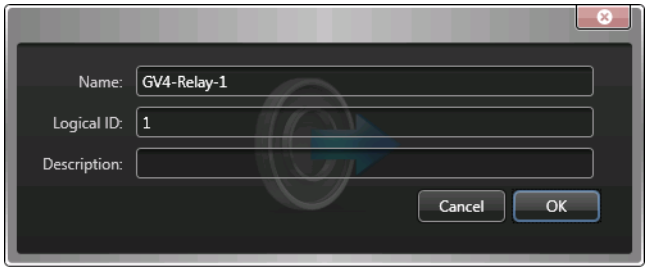
7 In the **Contact type** field, select one of the following options:

- **Normally open:** The normal contact state of the input is open.
- **Normally closed:** The normal contact state of the input is closed.

8 Click **OK**, and then click **Apply**.

9 Select an output, and at the bottom of the **Peripherals** tab, click .

A dialog box appears.



10 In the **Name** field, the name of the output is displayed. This is the name of the output connected to the panel.

11 (Optional) Type a **Logical ID** for the output. Setting a Logical ID helps you to easily identify the output in Security Center.

12 (Optional) Type a **Description** for the output.

13 Click **OK**, and then click **Apply**.

Related Topics

Creating the intrusion detection unit on page 29

Configuring intrusion alarms on areas (Bosch GV4 v2 panels)

If you are using a Bosch GV4 v2 panel, you can configure an output for an intrusion detection area that will trigger an alarm on the panel. This enables a security guard to manually trigger an intrusion alarm for a selected intrusion detection area in Security Desk.

Before you begin

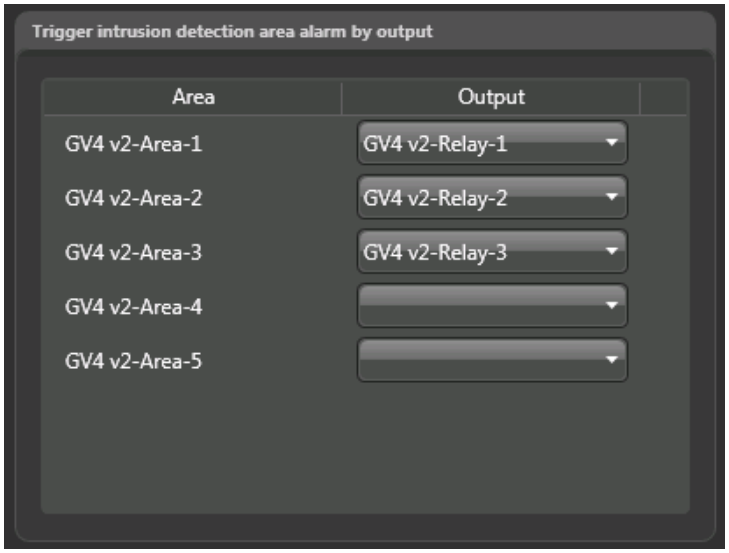
Using the Bosch Remote Programming Software (RPS), set the *Point Source* to *Output* for each point on the panel that you want to use to trigger an alarm. The outputs can then be used in Security Center to trigger alarms for the areas that the points are associated with. For more information on how to configure a *Point Source* as an *Output* using the Bosch RPS, see your Bosch documentation.

To configure an intrusion alarm on an area:

1 From the Config Tool home page, open the **Intrusion detection** task.

2 Select the intrusion detection unit to configure, and click the **Properties** tab.

3 Under **Trigger intrusion detection area alarm by output**, select the **Output** that is associated to each intrusion detection area on the panel.



4 Click **Apply**.

You can now use the **Trigger intrusion alarm** command in the *Intrusion detection area* widget to trigger an alarm in Security Desk for the configured areas.

Mapping intrusion detection areas to cameras

You can associate cameras to intrusion detection areas so that when they are viewed in Security Desk, video is displayed instead of the intrusion detection area icon.

To map an intrusion detection area to a camera:

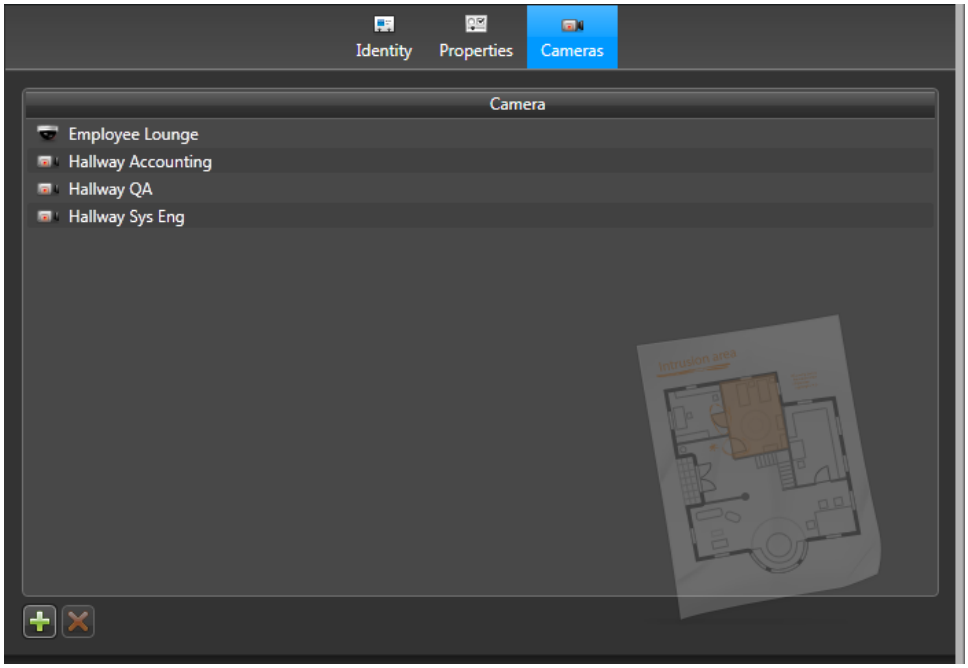
1 From the Config Tool home page, open the **Intrusion detection** task.

2 Select the intrusion detection area to configure, and then click the **Cameras** tab.

3 Click **Add a camera** ( ).

4 In the dialog box that opens, select a camera, and click **OK**.

The camera is added to the **Camera** list.



5 Click **Apply**.

Mapping control panel events to Security Center actions

You can set up events from the panel to trigger actions in Security Center, using event-to-actions.

What you should know

For example, a *Unit tamper* event on the control panel can trigger a Security Center alarm.

To map a panel event to a Security Center action:

1 From the Config Tool home page, open the **System** task.

2 Click the **General settings** view, and click the **Actions** page.

3 In the **Actions** page, click .

The *Event-to-action* window opens.

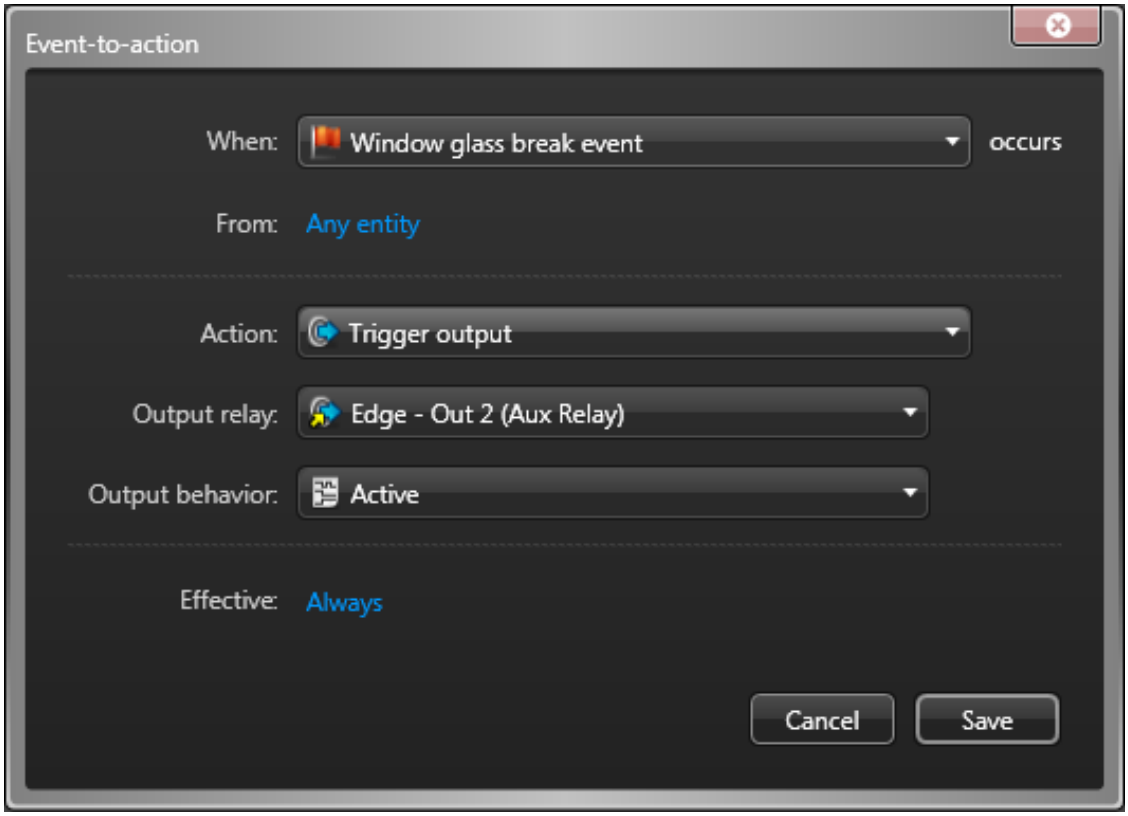
4 In the **When** drop-down list, select an event.

5 In the **From** field, select a specific **Intrusion detection unit** or **Intrusion detection area** that is the source of the event.

You can also decide to select **Any entity**.

6 In the **Action** drop-down list, select an action, and enter any additional information required about the action.

Example: If you select the **Trigger output** action, you must select the output relay to trigger, and its output behavior.



7 Select the **Effective** schedule under which the event-to-action will be active.

The default schedule is **Always**, however you can select any other schedule defined in your system.

8 Click **Save**.

Where to find product information

You can find our product documentation in the following locations:

- **Genetec Technical Information Site:** The latest version of the documentation is available from the Documents page of the Technical Information Site. To access the Technical Information Site, simply log on to GTAP and click the tab for the Technical Information Site.
- **Installation package:** The documentation is available in the Documentation folder of the installation package. Some of the documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. To access the help, click Help, press F1, or tap the ? (question mark) in the different client applications.

Technical support

Genetec Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a Genetec customer, you have access to the Genetec Technical Information Site, where you can find information and search for answers to your product questions.

- **Genetec Technical Information Site:** Browse over 5000 articles or download one of our many technical publications to find information on how to deploy and use Genetec products. Prior to contacting GTAC or opening a support case, it is recommended to search the Technical Information Site for potential fixes, workarounds, or known issues. To access the Technical Information Site, simply log on to GTAP and click the tab for the Technical Information Site.
- **Genetec Technical Assistance Center (GTAC):** Live support is available during business hours over the phone or using GTAP chat at https://gtap.genetec.com/Cases. For GTAC's contact information in your region see the Contact page at https://gtap.genetec.com.

  NOTE: To open a case with GTAC, you must provide your System ID (Omnicast, Synergis and Security Center) and/or SMA contract number. To obtain phone support, you must provide a certification number and the last six digits of your system ID. Refer to the Genetec Training FAQ for more information.
- **Licensing:**
  - For license activations or resets, please contact GTAC at https://gtap.genetec.com.
  - For issues with license content or part numbers, or concerns about an order, please contact Genetec Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
  - If you require a demo license or have questions regarding pricing, please contact Genetec Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Additional resources

If you require additional resources other than the Genetec Technical Assistance Center, the following is available to you:

- **GTAP Forum:** The Forum is an easy to use message board that allows clients and Genetec staff to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in or sign up at https://gtapforum.genetec.com.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/Services.