DMP Control Panel Integration Guide

5.3

Genetec

Copyright notice

Document information

Document title: DMP Control Panel Integration Guide 5.3

Document number: EN.550.023-V5.3.C(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 DMP control panels in Security Center, and how to monitor them in Security Desk. This guide supplements Security Center and DMP 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

Preface: Preface
Copyright notice ii
About this guide iii

Chapter 1: Introduction to DMP control panel integration
DMP control panel integration 2
How DMP control panel integration works 3
How DMP control panel terminology is used in Security Center 4
Supported number of DMP control panel devices and entities 5
Supported features with DMP control panel integration 6
Limitations: Intrusion control panel inputs monitored in Security Center 9

Chapter 2: Configuring DMP control panels in Security Center
Installation and configuration overview 11
Preparing to integrate DMP control panels 12
Best practices for connecting intrusion control panels to the network 12
Required Security Center user privileges for control panel integration 12
Creating the Intrusion Manager role 14
Configuring DMP extension properties 16
Creating the intrusion detection unit 18
Configuring intrusion detection unit properties 20
Configuring panel information 20
Configuring user management rights 21
Configuring entity mappings 22
Configuring area bad inputs arming behaviors 24
Configuring output trigger overrides 25
Configuring inputs and outputs 26
How contact types work with DMP 28
Mapping intrusion detection areas to cameras 29
Mapping control panel events to Security Center actions 30
Where to find product information 32
Technical support 33

1

Introduction to DMP control panel integration

This section includes the following topics:

- "DMP control panel integration" on page 2
- "How DMP control panel integration works" on page 3
- "How DMP control panel terminology is used in Security Center " on page 4
- "Supported number of DMP control panel devices and entities" on page 5
- "Supported features with DMP control panel integration" on page 6
- "Limitations: Intrusion control panel inputs monitored in Security Center" on page 9

DMP control panel integration

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

The integration allows you to do the following:

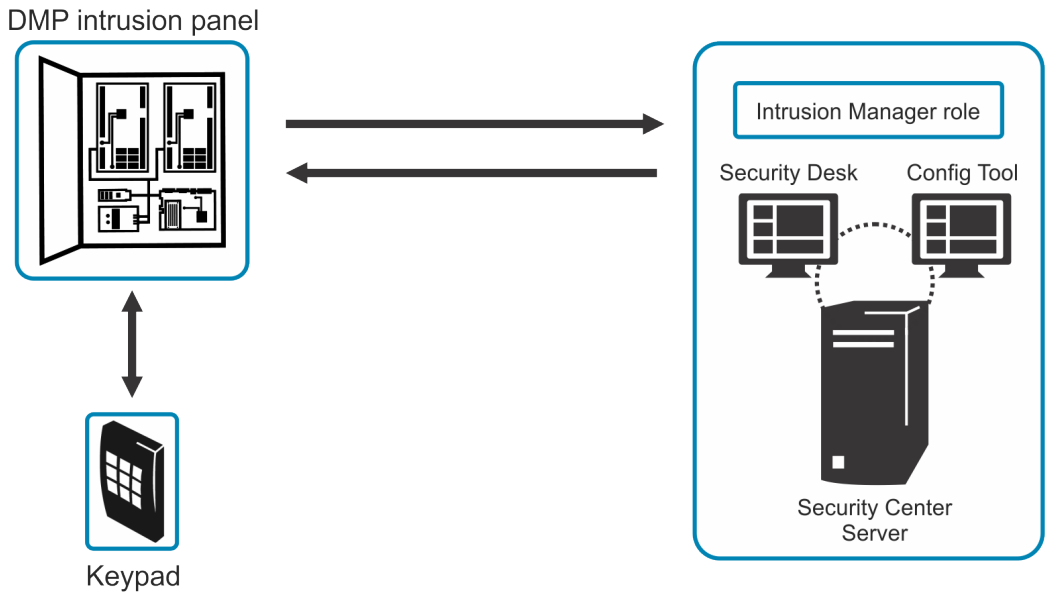
- Map DMP control panels to Security Center intrusion detection units.
- Map groups of inputs and devices on the control panel to Security Center intrusion detection areas.
- Monitor intrusion detection area state changes in real-time in Security Desk.
- Monitor the status of intrusion detection units 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.
- Receive live notifications on input state changes in Security Desk.
- Configure the way outputs are triggered.
- Trigger outputs from event-to-actions.
- Grant users the right to configure the panel.

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 DMP control panel integration works

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

The Intrusion Manager role receives events from the intrusion panel, reports them live in Security Desk, and logs them in a database for future reporting. The role also relays user commands to the intrusion 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 area master armed event in Security Center can trigger an output on the intrusion panel).



How DMP control panel terminology is used in Security Center

DMP intrusion detection components are mapped as entity types in Security Center. The following table lists some DMP control panel components and terms, and how they are represented in Security Center.

DMP term	Description	Security Center term
DMP command processor panel	The control panel that is monitored and controlled by Security Center. Each control panel can control multiple areas.	Intrusion detection unit
Area	A group of zones configured on the control panel that specify a physical area, such as a floor of a building. These groups can be monitored and armed in Security Desk.	Intrusion detection area
Zone	Inputs for devices such as glass break detectors, motion sensors, temperature sensors, and so on, that are connected to the control panel.	Input
Output	Output pin connected to the control panel.	Output

Supported number of DMP control panel devices and entities

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

	No. of intrusion detection units	No. of intrusion detection areas	No. of inputs	No. of outputs
Per Intrusion Manager role	10	80	640	160
Per Directory	200	1600	12800	3200

Supported features with DMP control panel integration

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

Feature		Supported
Data encryption over TCP/IP		Yes (XR500E). Some parts of data like user information, pin, and credential are encrypted.
Authentication between control panel and server		No
Get input bypass status		Bypassed area can be detected. However, the exact input is not available.
Set input bypass status		No
Arm/disarm from Security Center	Instant arming/ disarming	Yes
	Delayed arming	Yes A 30-second delay is applied before arming the panel.
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

Feature		Supported
Trigger alarms on the control panel from Security Center		No
Create custom Security Center events tied to panel pin events		No
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	Yes
Intrusion detection area events	Master armed	Yes
	Perimeter armed	No
	Disarmed	Yes
	Auto-arming postponed	Yes
	Forced arming	Yes
	Input bypass activated	Yes
	Input bypass deactivated	Yes
	Duress	Yes This corresponds to the *Ambush* event received from the panel.
	Entry delay started	No
	Intrusion alarm activated	Yes
Intrusion detection area states	Master armed	Yes

Feature		Supported
	Perimeter armed	No
	Disarmed	Yes
	Ready-to-arm	Yes
	Intrusion alarm active	Yes
	Input trouble	No
	Arming countdown	No
	Entry delay	No
Arming commands	Instant master arm	Yes
	Delayed master arm	Yes
	Instant perimeter arm	No
	Delayed perimeter arm	No
	Forced arm	Yes
	Bypass arm	Yes
Live input entity state changes	Normal	Yes
	Active	Yes
	Trouble	Yes
	Bypassed	No
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
Link cardholders to panel code users		Yes
Modify user codes and PINs		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. For example, DMP panels typically send 1 event every 2 seconds. If you monitor 100 inputs and all of them have their state changed at the same time, it will require more than 3 minutes to receive the last event.

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.

Example: DMP panels scan their inputs every 500 ms to detect state changes, but only send corresponding events every 2 seconds. Because of this behavior, we do not recommend to monitor inputs that change at a rate faster than once every 2 seconds using these panels.

2

Configuring DMP control panels in Security Center

This section includes the following topics:

- "Installation and configuration overview" on page 11
- "Preparing to integrate DMP control panels" on page 12
- "Creating the Intrusion Manager role" on page 14
- "Configuring DMP extension properties" on page 16
- "Creating the intrusion detection unit " on page 18
- "Configuring intrusion detection unit properties" on page 20
- "Configuring inputs and outputs" on page 26
- "How contact types work with DMP" on page 28
- "Mapping intrusion detection areas to cameras" on page 29
- "Mapping control panel events to Security Center actions" on page 30

Installation and configuration overview

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

Phase	Description	See
1	Before you start installing and configuring DMP control panels, you should understand the relationship between DMP terms and Security Center entities.	How DMP control panel terminology is used in Security Center on page 4
2	Read all the required information about this release, and perform all the required tasks before integrating the DMP control panel in Security Center.	Preparing to integrate DMP control panels on page 12
3	Configure the inputs, outputs, and partitions on your DMP control panel.	See the DMP documentation.
4	If you already have users programmed in the DMP control panel that you want to preserve, back up the user code database before connecting to Security Center as a precaution.	See the DMP documentation.
5	If you have users configured in your DMP control panel that you do not want to import to Security Center, manually delete those users from the panel before connecting to Security Center.	See the DMP documentation.
6	Set up communication between Security Center server and the DMP control panel using an IP network.	See the DMP documentation.
7	Create the Intrusion Manager role in Security Center to manage the intrusion detection unit.	Creating the Intrusion Manager role on page 14
8	Configure the DMP extension of the Intrusion Manager role.	Configuring DMP extension properties on page 16
9	Create the DMP control panel as an intrusion detection unit in Security Center.	Creating the intrusion detection unit on page 18
10	Configure the intrusion detection unit properties (for example, grant users access to panel configuration, configure cardholders to be programmed in the panel).	Configuring intrusion detection unit properties on page 20
11	(Optional) Map intrusion detection areas to cameras to view video associated to intrusion events in Security Desk.	Mapping intrusion detection areas to cameras on page 29
12	(Optional) Create events-to-actions, for DMP control panel events received in Security Center to trigger actions.	Mapping control panel events to Security Center actions on page 30

Preparing to integrate DMP control panels

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

Before integrating DMP 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 DMP requirements.

For more information, see the *Security Center Release Notes* and your DMP 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 Configure the DMP control panel for IP communication.

For more information on how to configure your DMP control panel for IP communication, see the DMP documentation.

5 Make sure you have the right user privileges.

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.

NOTE: Field notice for DMP. Please contact DMP support to get the latest firmware that includes a fix to ignore the broadcast packets, which will prevent overloading the panel unnecessarily.

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.

Creating the Intrusion Manager role

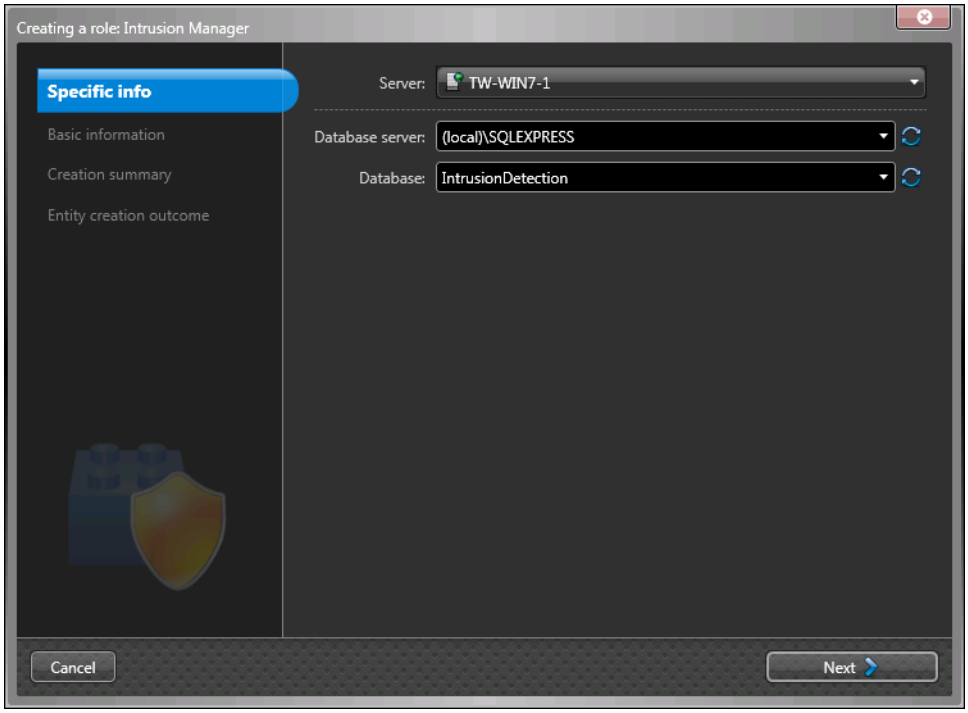
You must create an Intrusion Manager role in Config Tool to manage the panel.

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

Configure the DMP extension properties.

Related Topics

Configuring DMP extension properties on page 16

Configuring DMP extension properties

The **Extensions** tab of the Intrusion Manager role allows you to configure properties that apply to all DMP panels, such as communication timeout, time synchronization interval, and the number digits in user codes.

Before you begin

Create an Intrusion Manager role.

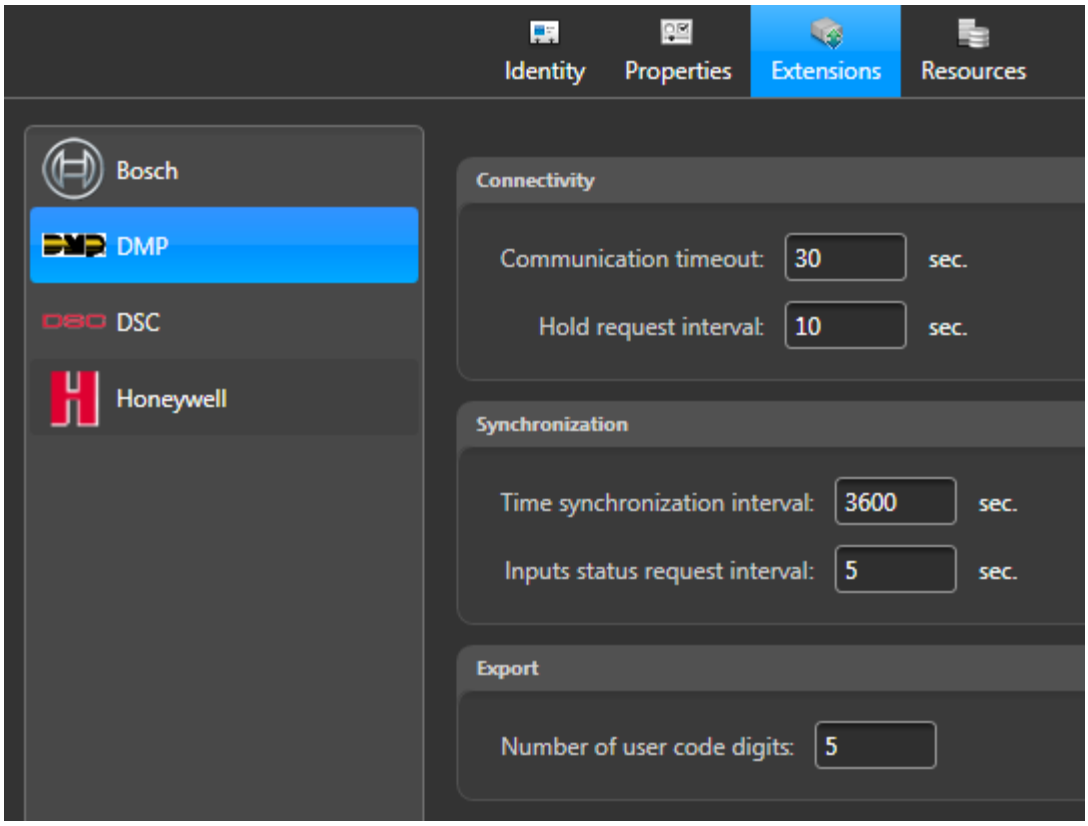
What you should know

Default values have been optimized for most setups, however you may want to adjust them to meet your specific needs.

To configure the DMP extension:

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

2 In the entity tree, select the *Intrusion Manager* role to configure, click the **Extensions** tab, and then select **DMP**.



3 Set the following properties:

- **Communication timeout:** After sending a message to the panel, this is the time delay after which, if no response is received, Security Center will raise a disconnection event.
- **Hold request interval:** To maintain an active connection with the panel, Security Center sends a message to the panel following this interval.

- **Time synchronization interval:** Time period used between two clock synchronization requests when automatic time synchronization is enabled.
- **Input status request interval:** Polling period used to get the inputs' status from the panel when **Real-time Status** is disabled.

4 Enter the number of digits of the user codes to be programmed in the panel.

IMPORTANT: This value must be identical to the one configured in the panel.

After you finish

Create the intrusion detection unit.

Related Topics

Creating the Intrusion Manager role on page 14
Creating the intrusion detection unit on page 18

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.
- Configure the DMP extension.

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).

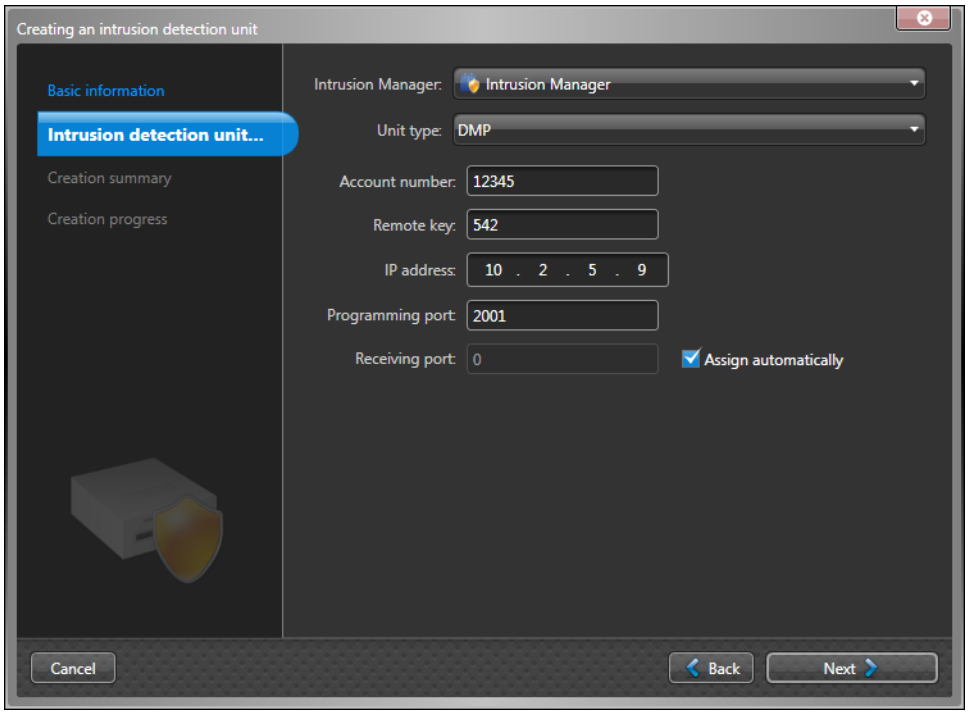
b) (Optional) Type a **description** for the entity.

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 Enter the appropriate **Account number**.

The account number is a 1 to 5 digit number used to identify the panel.

7 Enter the **Remote key** code for the panel that was assigned using DMP Remote Link.

IMPORTANT: Security Center cannot communicate with the control panel unless the correct remote key is provided.

8 Enter the **IP Address** of the unit.

9 Enter the **Programming port** used to connect the panel to Security Center.

This port is a TCP port with a default value of 2001.

10 Enter the **Receiving port** used to receive events messages from the panel.

When the check box is selected, Security Center will update the PC Log Reports configuration with the default values when connecting to the panel.

11 Click **Next**.

12 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**.

13 Click **Close**.

The intrusion detection unit appears under the Intrusion Manager role in the entity browser.

Related Topics

Configuring DMP extension properties on page 16

Configuring intrusion detection unit properties on page 20

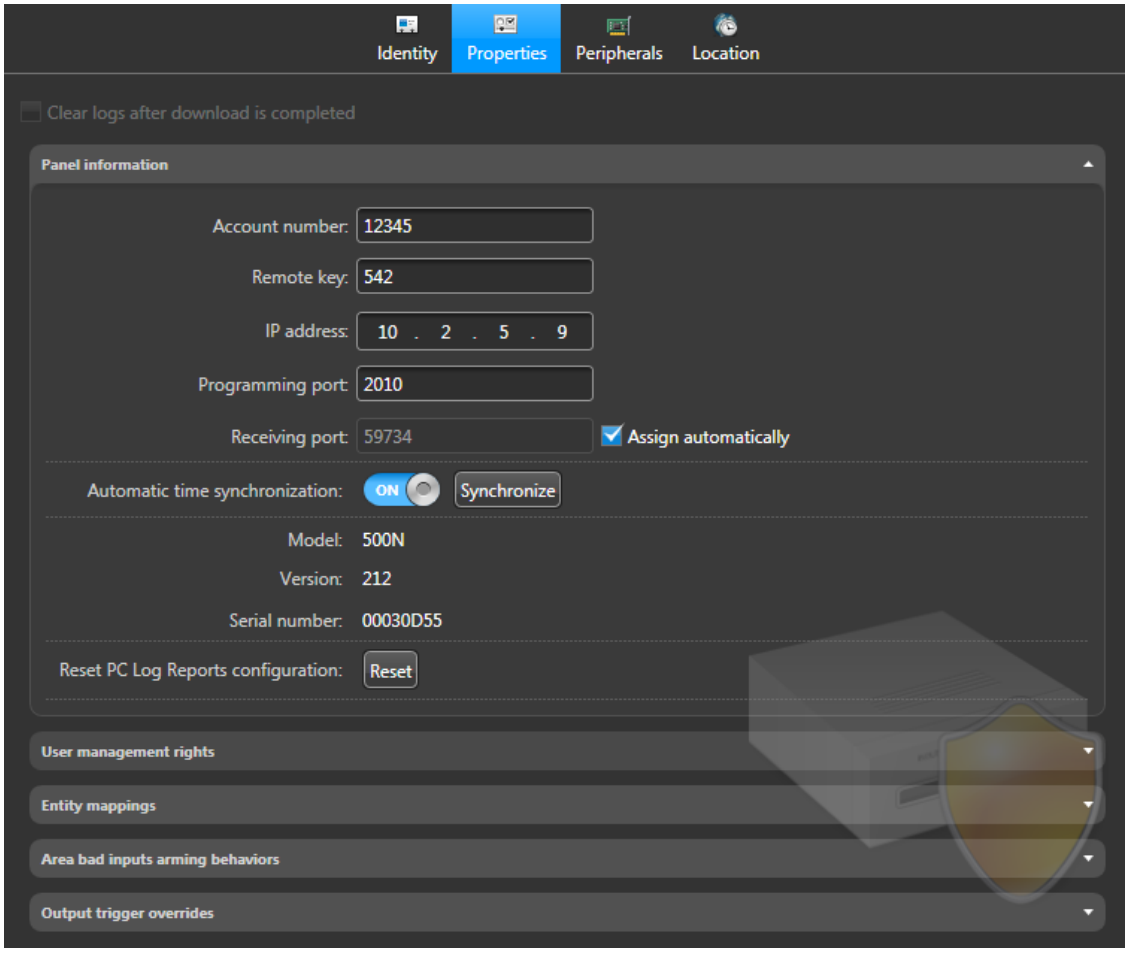
Configuring intrusion detection unit properties

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

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.



Related Topics

Creating the intrusion detection unit on page 18

Configuring panel information

Under **Panel information** you can modify information such as the remote key, IP address, and port numbers of your panel.

What you should know

Only Administrators or a user with user management rights can modify these fields.

To configure panel information:

1 Expand the **Panel information** area.

2 Enter the **Account number**, **Remote key**, **IP address**, **Programming port**, and **Receiving port** associated with the panel.

3 Turn **Automatic time synchronization** on if you want Security Center to automatically synchronize its clock with the panel.

You can also synchronize the time manually by clicking **Synchronize**.

NOTE: When you synchronize the clocks, the time is set to the control panel's local time zone.

4 (Optional) Click **Reset** to revert the panel's PC Log Reports configuration to the default values.

Users have the flexibility to modify the panel's PC Log Reports configuration using Remote Link. Security Center will not automatically alter the new configuration. If changes were made and affect the communication through PC Log Reports; that is, Security Center does not receive events anymore from the panel, you can click **Reset** to revert the configuration to its default values.

Configuring user management rights

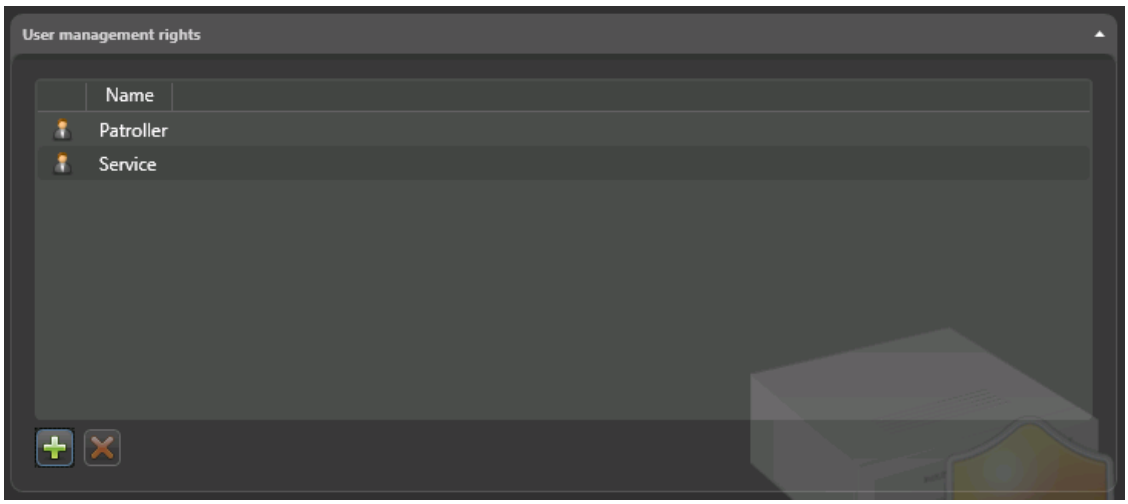
Under **User management rights** you can specify the users and user groups that have the right to configure the panel. This can be used in place of partitions or in conjunction with partitions to provide configuration rights on the panel for specific users.

What you should know

- Administrators and users that are part of the Administrators user group can always configure DMP panels.
- When a user or user group does not have the rights to configure the panel, they can view the information on the **Properties** page but they cannot make any modifications.
- A user still needs to be given user management rights in order to be able to configure the panel even when security is enforced with partitions. If you are using partitions, assign users the right to configure the panel first and then add the user to a partition. For more information about partitions, see the *Security Center Administrator Guide*.

To configure user management rights:

1 Expand the **User management rights** area.



2 Click the button, select a user or user group, and then click **Select**.

The user or user group is added to list. You can remove a user at any time by selecting the user and clicking the button.

Configuring entity mappings

Under **Entity mappings** you can select the cardholders and cardholder groups that will be programmed in the panel as users that can arm and disarm intrusion areas. Cardholders and cardholder groups are mapped to the available profiles configured on the panel.

What you should know

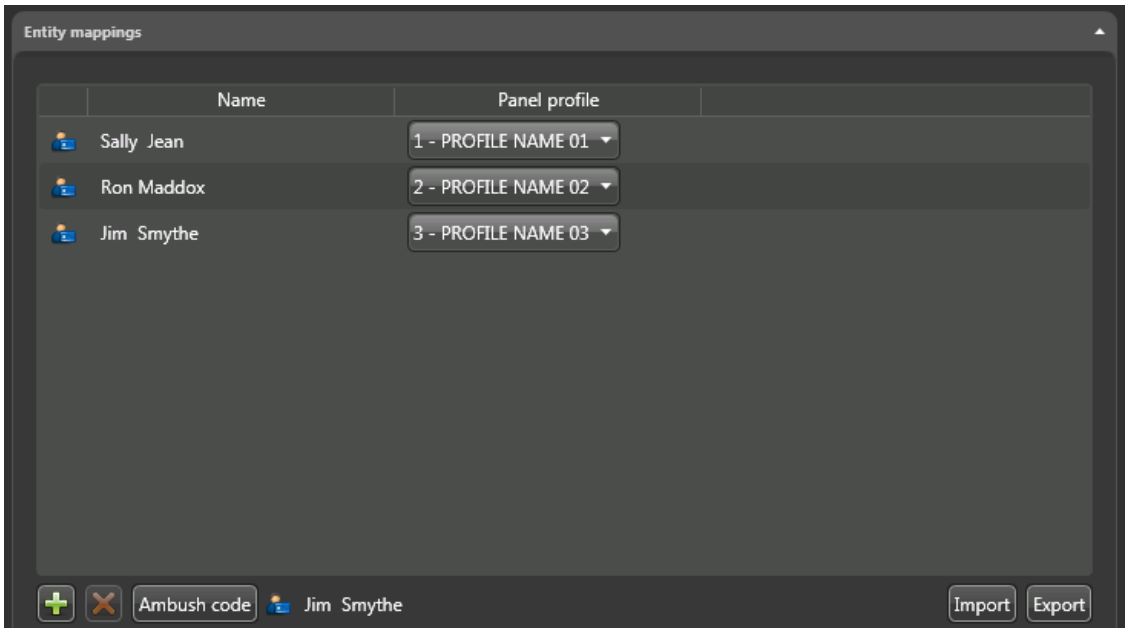
- You must always click the **Export** button to have your changes in the **Entity mappings** programmed in the panel.
- When a specific cardholder entity is added to the entity mapping its associated user profile is programmed in the panel. This user profile has priority over any user profile associated with cardholder groups that the cardholder belongs to.
- A cardholder that is part of multiple cardholder groups which are added to the entity mapping may have multiple user profiles associated with it. In these cases, the user profile with the lowest number is automatically selected by Security Center to be programmed in the panel.
- A cardholder with multiple credentials will result in multiple user entries created on the panel, one for each card credential and PIN credential combination. For example, a user may have a card and a key fob that uses the same PIN.
- Facility codes are not exported to the panel. They must be manually configured on the panel to ensure that the panel will be able to read the cards.
- The same card format must be configured for a cardholder in both Security Center and on the panel. If a 37-bit card format is configured in Security Center and a 26-bit format is used in the panel, the card credentials won't be exported properly.

An **Import** option is also available, which is useful if you already have users set up on the control panel and you want to import them as cardholders in Security Center instead of recreating everything manually.

IMPORTANT: Once you export your entity mappings, existing preconfigured mappings on the DMP panel will be overwritten. Therefore, ensure that you import any entity mappings that you want to preserve from the panel before performing an export. You may also want to backup the user code database of the panel as a precaution.

To configure entity mappings:

1 Expand the **Entity mappings** section.



2 Click the button, select a cardholder or cardholder group, and then click **Select**.

The cardholder or cardholder group is added to list.

3 Under **Panel profile** for the cardholder or cardholder group you just added, select the desired profile.

4 (Optional) If the *Ambush* function is enabled on the control panel, select the cardholder that will be programmed on the panel for the *Ambush* (Duress) user code.

NOTE: This cardholder must only have one associated card credential and one PIN credential.

a) Click **Ambush code**.

b) Select the appropriate cardholder, and then click **Select**.

The cardholder is added to the list of entity mappings and their name also appears beside the **Ambush code** button.

c) Under **Panel profile** for the cardholder you just added, select the desired profile.

5 Click **Export** to have the mappings programmed in the panel.

You can remove a mapping at any time by selecting it from the **Entity mappings** list and clicking the button.

Importing entity mappings

You can use the **Import** button to import entity mappings (panel users) directly from the panel. The import automatically creates cardholders with pin and card credentials on the Security Center system. This useful if you already have a DMP panel that is set up with the appropriate panel users and you don't want to recreate them manually in Security Center.

What you should know

- Any user modifications made directly on the panel after an import will not be synchronized with Security Center unless you perform another manual import.
- Card credentials will be created with the HID H10302 format available in Security Center.

To import entity mappings:

1 Expand the **Entity mappings** section.

2 Click Import.

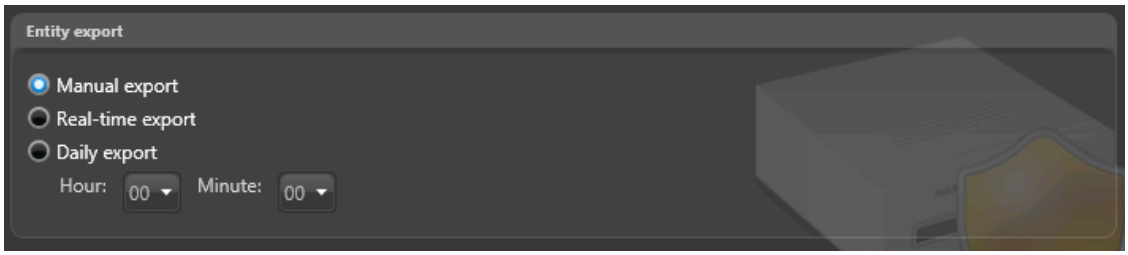
The users programmed in your panel are imported to Security Center as cardholders.

Exporting entity mappings

Under **Entity export** you can specify how the entity mappings are exported to the panel when changes are made using other Security Center tasks such as the *Cardholder management task*.

To configure how entity mappings (panel users) are exported:

1 Expand the **Entity export** section.



2 Select one of the following options:

- **Manual export:** Entity mappings are manually exported. When this option is selected you will always have to click the **Export** button for your changes to be pushed to the panel.
- **Real-time export:** Entity mappings are exported to the panel as they are created or modified.
- **Daily export:** Entity mappings are exported at a given time. You must specify the **Hour** and **Minute**.

Configuring area bad inputs arming behaviors

Under **Area bad inputs arming behaviors** you can configure an area to have a different arming behavior if a faulty input linked to an area is detected.

What you should know

When connecting to the panel, Security Center retrieves the panel configuration to display the option currently set for each area. When properties are changed in Config Tool, they are programmed in the panel.

To configure an arming behavior for an area:

1 Expand the **Area bad inputs arming behaviors** section.

2 Beside the area under **Faulty input arming behavior**, select one of the following options:

- **Refuse arm:** The panel does not arm the area if a faulty input is detected. This is the default setting.
- **Force arm:** The panel ignores the faulty input and arms the area. The input is not permanently bypassed.
- **Bypass:** The faulty input is bypassed in the panel and the area is armed. The bypass status is cancelled when the area is disarmed.

Configuring output trigger overrides

Under **Output trigger overrides** you can configure the way each output on the panel is triggered.

To configure an output trigger override:

1 Expand the **Output trigger overrides** section.

2 Beside the name of the output under **Triggering mode** choose one of the following options:

- **Steady:** The output is turned on and remains on.
- **Momentary:** The output is turned on only once for one second.
- **Pulse:** The output alternates between the on state and off state
- **Temporal:** The output follows a pattern of half a second on and half a second off for three times and then 2.5 seconds off.

Configuring inputs and outputs

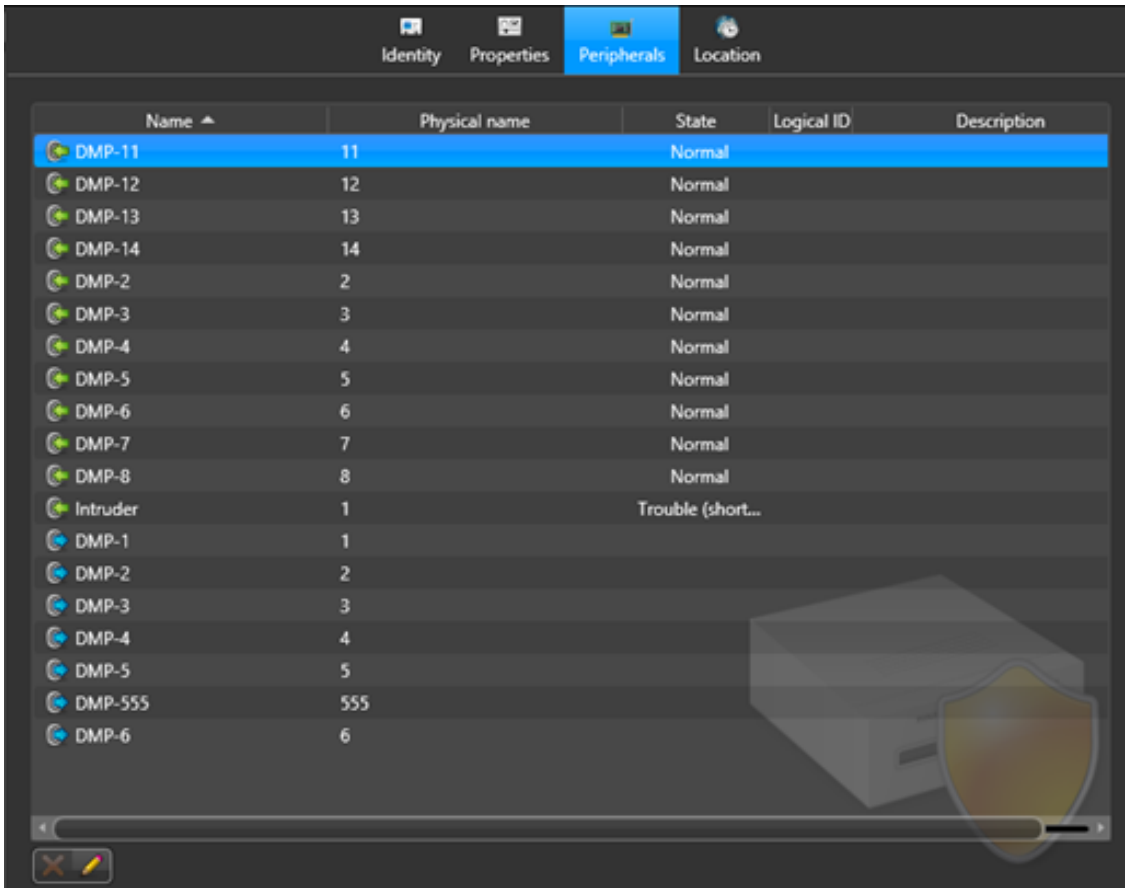
In the intrusion detection unit **Peripherals** tab, you can assign a name, logical ID, and a description to the inputs and outputs controlled by the unit. You can also see the state of inputs.

What you should know

IMPORTANT: The panel does not prioritize *ZoneAlarm* events over *ZoneTrouble* events. If a zone changes from *Normal* to *Trouble* for minutes and an alarm is triggered, the alarm will be reported after several minutes. To ensure fast alarm reporting, we recommend that you enable *Swinger bypass* on every zone where it is acceptable to do it.

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 or output from the list and click .

3 In the dialog box that appears, enter the **Name**, **Logical ID**, and **Description** for that input or output.

4 Select the required **Real-time status** option for the input.

Enabling this option displays the contact type as configured on the panel. Disabling it allows you to select the **Contact type** in Config Tool and specify how Security Center will manage the input state received from the panel.

5 Click **OK**

6 Click **Apply**.

After you finish

You can associate cameras to intrusion detection areas, and map DMP control panel events to Security Center actions.

How contact types work with DMP

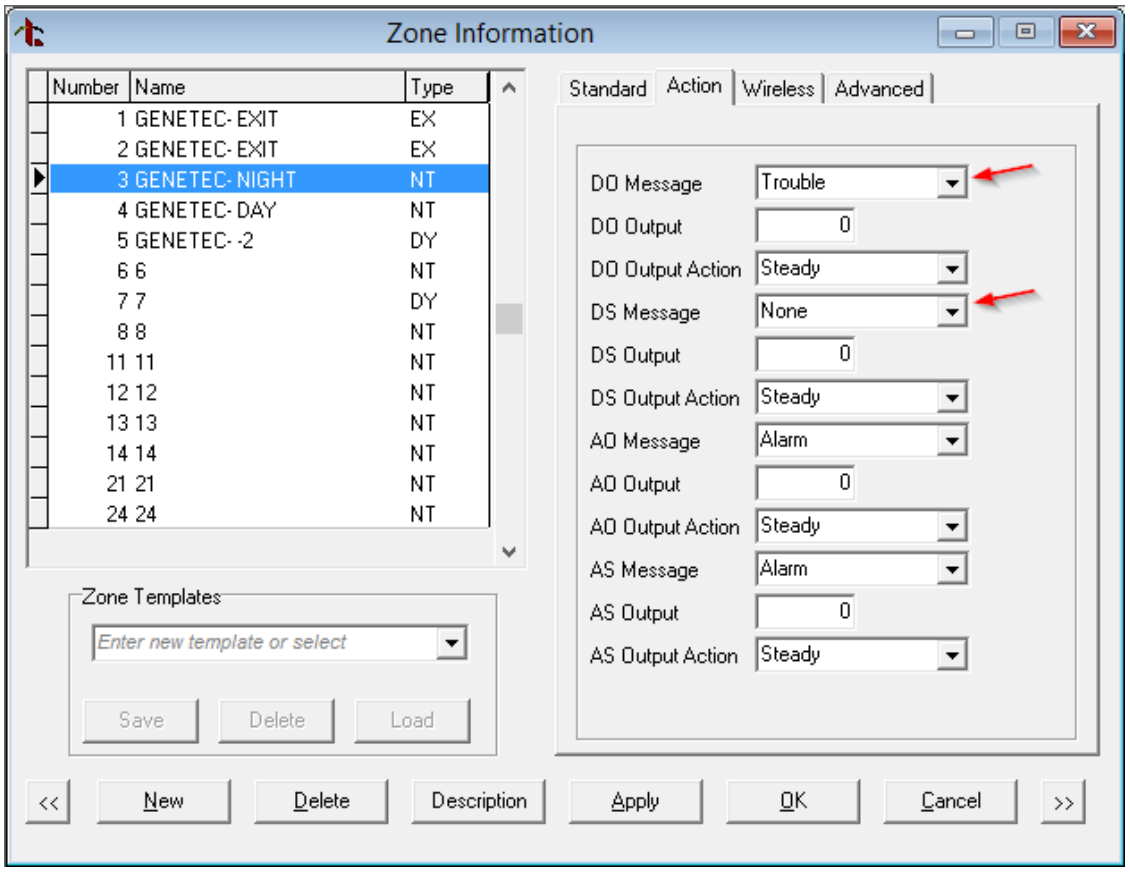
The way contact types (*Normally open*, *Normally closed*) are managed by Security Center depends on the **Real-time Status** option selected for each input.

When **Real-time Status** is disabled (unchecked) in Config Tool:

- The contact type can be configured as *Normally open* or *Normally closed*.
- A *Normally open* input that is electrically open is reported as *Trouble*.
- A *Normally closed* input that is electrically shorted is reported as *Trouble*.

When **Real-time Status** is enabled (checked) in Config Tool:

- The contact type must be configured using Remote Link.
- The contact type displayed in Config Tool reflects the panel's configuration.
- *Zone Information* must be configured on the panel according to the following:
  - For a *Normally open* zone, **DO Message** must be set to *Trouble* and **DS Message** must be set to any other value than *Trouble*.
  - For a *Normally closed* zone, **DO Message** must be set to any other value than *Trouble*, and **DS Message** must be set to *Trouble*.



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:

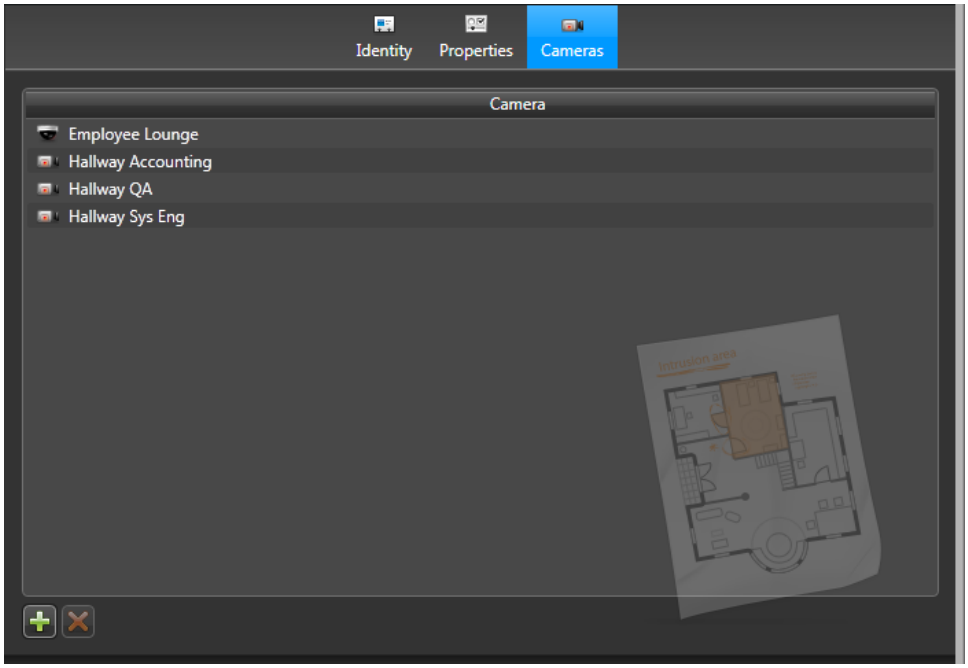
1 From the Config Tool home page, open the **Intrusion detection** task.

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.

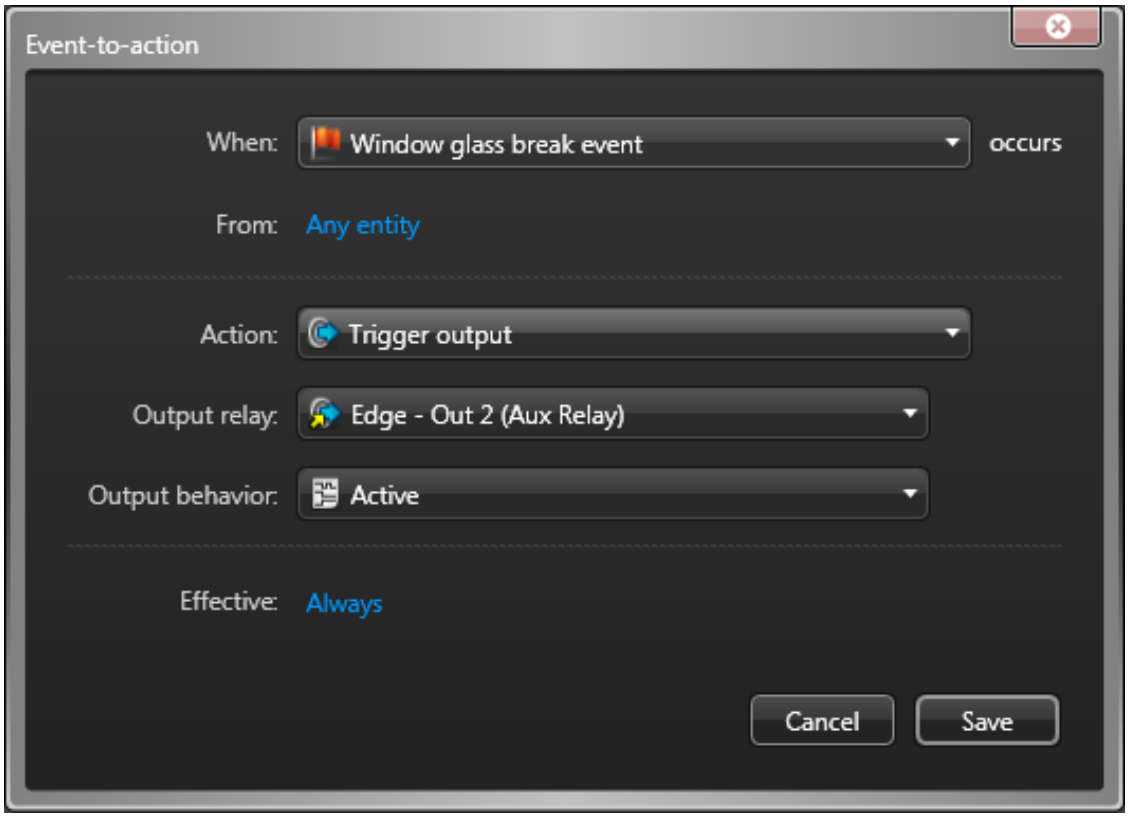
4 In the **When** drop-down list, select an event.

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. The output behavior will be ignored because the *Output trigger overrides* will be transmitted to the panel instead.



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**.

After you finish

See the following sections in your *Security Desk User Guide* online help for information about how to monitor intrusion detection areas, arm and disarm intrusion detection areas, and investigate intrusion detection area activities and intrusion detection unit events.

- Monitoring events
- Monitoring alarms
- Intrusion detection area widget
- System status
- Intrusion detection area activities
- Intrusion detection events

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.