DSC PowerSeries Control Panel Integration Guide

5.3

Genetec

Copyright notice

Document information

Document title: DSC PowerSeries Control Panel Integration Guide 5.3

Document number: EN.500.018-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 DSC PowerSeries control panels in Security Center, and how to monitor them in Security Desk. This guide supplements Security Center and DSC 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 DSC PowerSeries control panel integration

This section includes the following topics:

DSC PowerSeries control panel integration

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

The integration allows you to do the following:

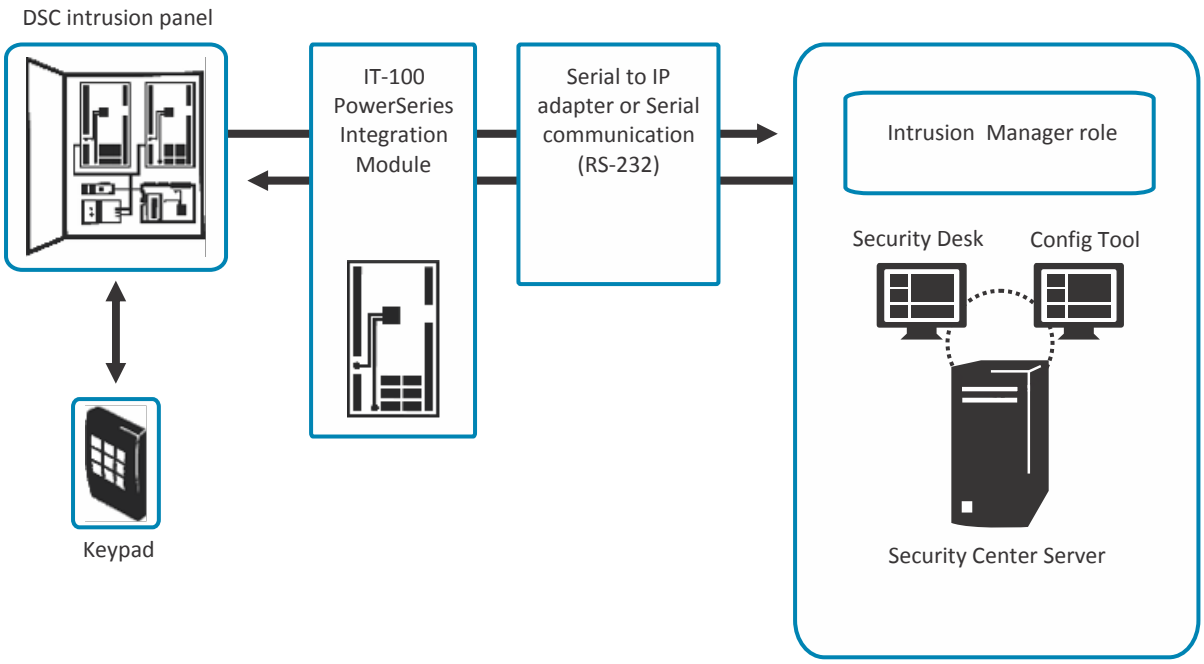
- Map DSC PowerSeries control panels to Security Center intrusion detection units.
- Map groups of inputs and devices on the control panel to Security Center intrusion detection areas.
- Monitor intrusion detection area state changes in real-time in Security Desk.
- Monitor the status of intrusion detection 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.

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 DSC PowerSeries control panel integration works

DSC PowerSeries 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).



How DSC PowerSeries control panel terminology is used in Security Center

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

DSC term	Description	Security Center term
DSC PowerSeries control panel	The control panel that is monitored and controlled by Security Center. Each control panel can control multiple groups.	Intrusion detection unit
Partition	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 DSC PowerSeries devices and entities

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

	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 DSC PowerSeries panel integration

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

Feature		Supported
RS-232 serial connection		Yes, with IT-100 PowerSeries integration Module
TCP/IP connection		Yes, with Lantronix UDS1100 Serial to Ethernet converter
Data encryption over TCP/IP		No
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	No
	Delayed arming	Yes
Use control panel inputs in virtual zones		Yes
Trigger outputs on control panels		Yes
Discover intrusion detection areas and devices automatically		No
Create intrusion detection areas automatically in Security Center		No
Create input entities automatically in Security Center		No
Create output entities automatically in Security Center		No
Link input entities to intrusion detection areas automatically in Security Center		No
Download Offline logs automatically on connection		No
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	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

Feature		Supported
	Ready-to-arm	Yes
	Intrusion alarm active	Yes
	Input trouble	Yes
	Arming countdown	Yes
	Entry delay	Yes
Arming commands	Instant master arm	No
	Delayed master arm	Yes
	Instant perimeter arm	No
	Delayed perimeter arm	Yes
	Forced arm	No
	Bypass arm	No
Live input entity state changes	Normal	Yes
	Active	Yes
	Trouble	Yes
	Bypassed	can detect that an area was bypassed. However, the exact input is not available.
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 DSC PowerSeries control panels in Security Center

This section includes the following topics:

Installation and configuration overview

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

Phase	Description	See
1	Before you start installing and configuring DSC PowerSeries control panels, you should understand the relationship between DSC terms and Security Center entities.	How DSC PowerSeries 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 DSC PowerSeries control panel in Security Center.	Preparing to integrate DSC PowerSeries control panels on page 12
3	Configure the inputs, outputs, and partitions on your DSC PowerSeries control panel.	See the DSC PowerSeries documentation.
4	Set up communication between Security Center server and the DSC PowerSeries control panel using IP network or RS-232 communication.	Preparing to integrate DSC PowerSeries control panels on page 12
5	Create the Intrusion Manager role in Security Center to manage the intrusion detection unit.	Creating the Intrusion Manager role on page 14
6	Create the DSC PowerSeries control panel as an intrusion detection unit in Security Center.	Creating the intrusion detection unit on page 16
7	Configure the intrusion detection unit basic properties (for example, activating the inputs, outputs, and intrusion detection areas to monitor).	Configuring intrusion detection unit properties on page 18
8	(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 21
9	(Optional) Create events-to-actions, for DSC PowerSeries control panel events received in Security Center to trigger actions.	Mapping control panel events to Security Center actions on page 22

Preparing to integrate DSC PowerSeries control panels

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

Before integrating DSC PowerSeries 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 DSC requirements.

For more information, see the *Security Center Release Notes* and your DSC 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:

- If you want the Security Center server to communicate with the DSC PowerSeries control panel using IP communication, you must use a Lantronix UDS1100 Serial to Ethernet converter. You will also need the following:
  - Lantronix 500-163-R DB9F to DB25M serial cable (or equivalent)
  - Lantronix 140-448-R Null Modem crossover adapter (or equivalent)

  For more information about configuring the Lantronix UDS1100 Serial to Ethernet converter, please see the Lantronix documentation.
- If you want the Security Center server to communicate with the DSC PowerSeries control panel using serial communication, ensure that the DB9 "straight-through" serial cable that connects the control panel to the Security Center system is connected to the Security Center server hosting the Intrusion Manager role.

  NOTE: The DSC PC Link serial cable is not supported.

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.

Creating the Intrusion Manager role

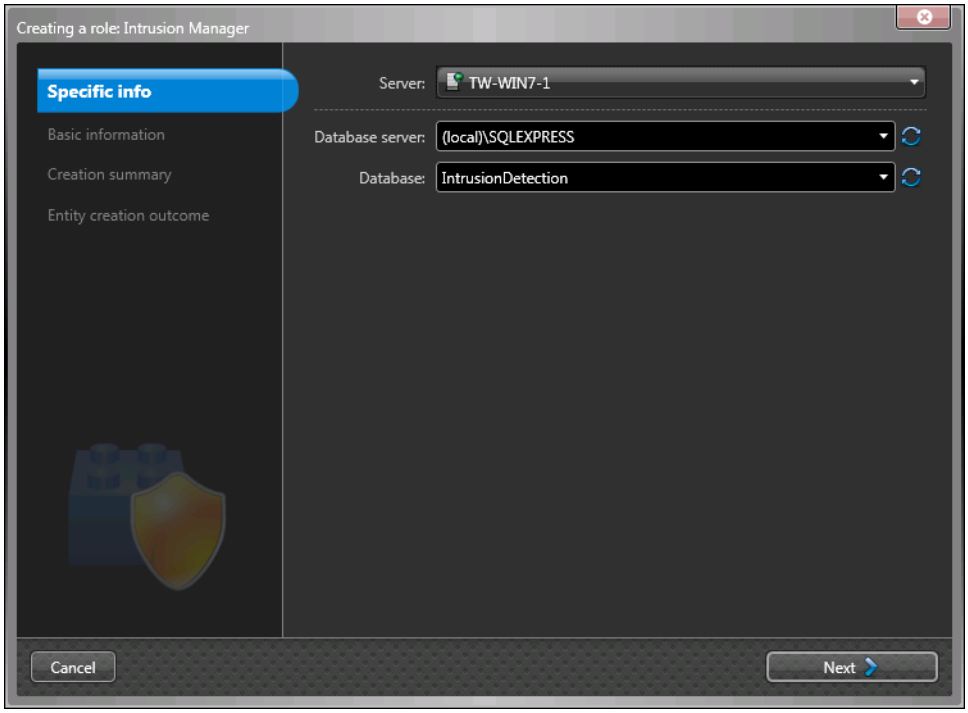
You must create an Intrusion Manager role in Config Tool to manage the panel.

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 16

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).

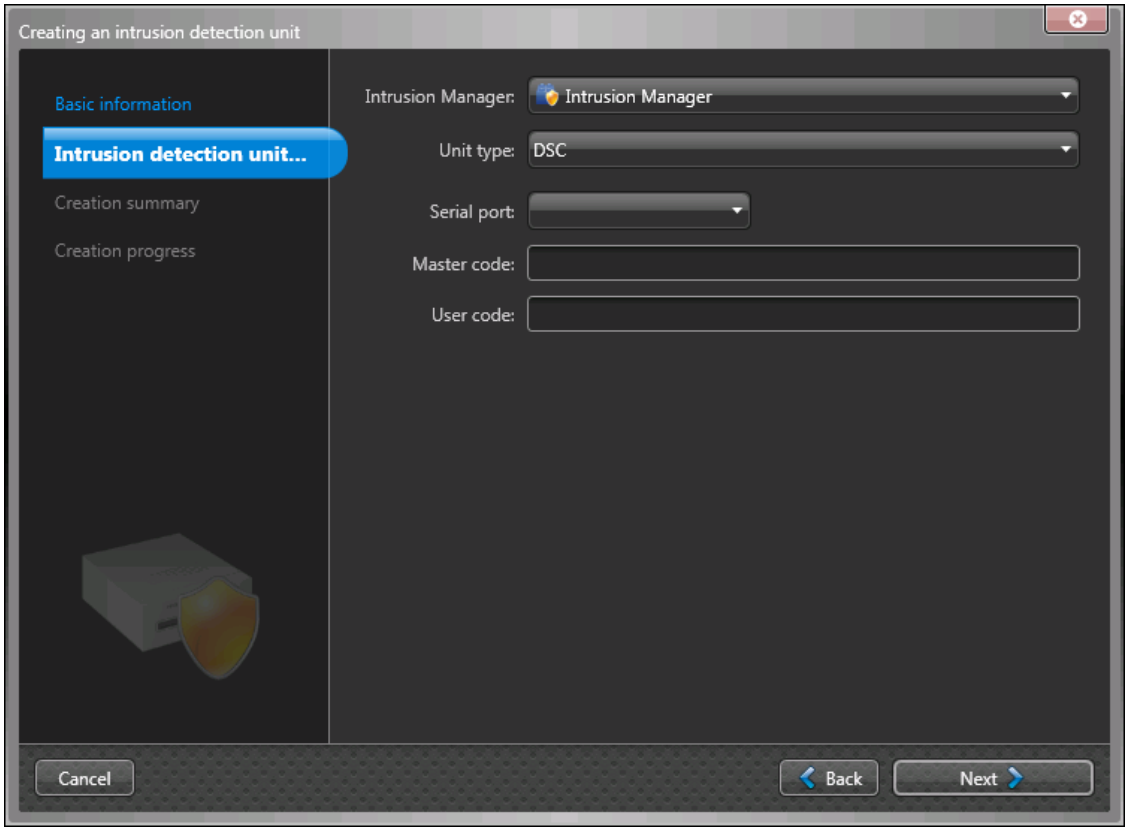
b) (Optional) Type a **description** for the entity.

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 From the **Serial port** drop-down list, select the COM port used to connect the panel to Security Center.
7 Enter the **Master code** and **User code** used to authenticate the commands sent to the panel.
8 Click **Next**.
9 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**.
10 Click **Close**.

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

Related Topics

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

Configuring intrusion detection unit properties

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

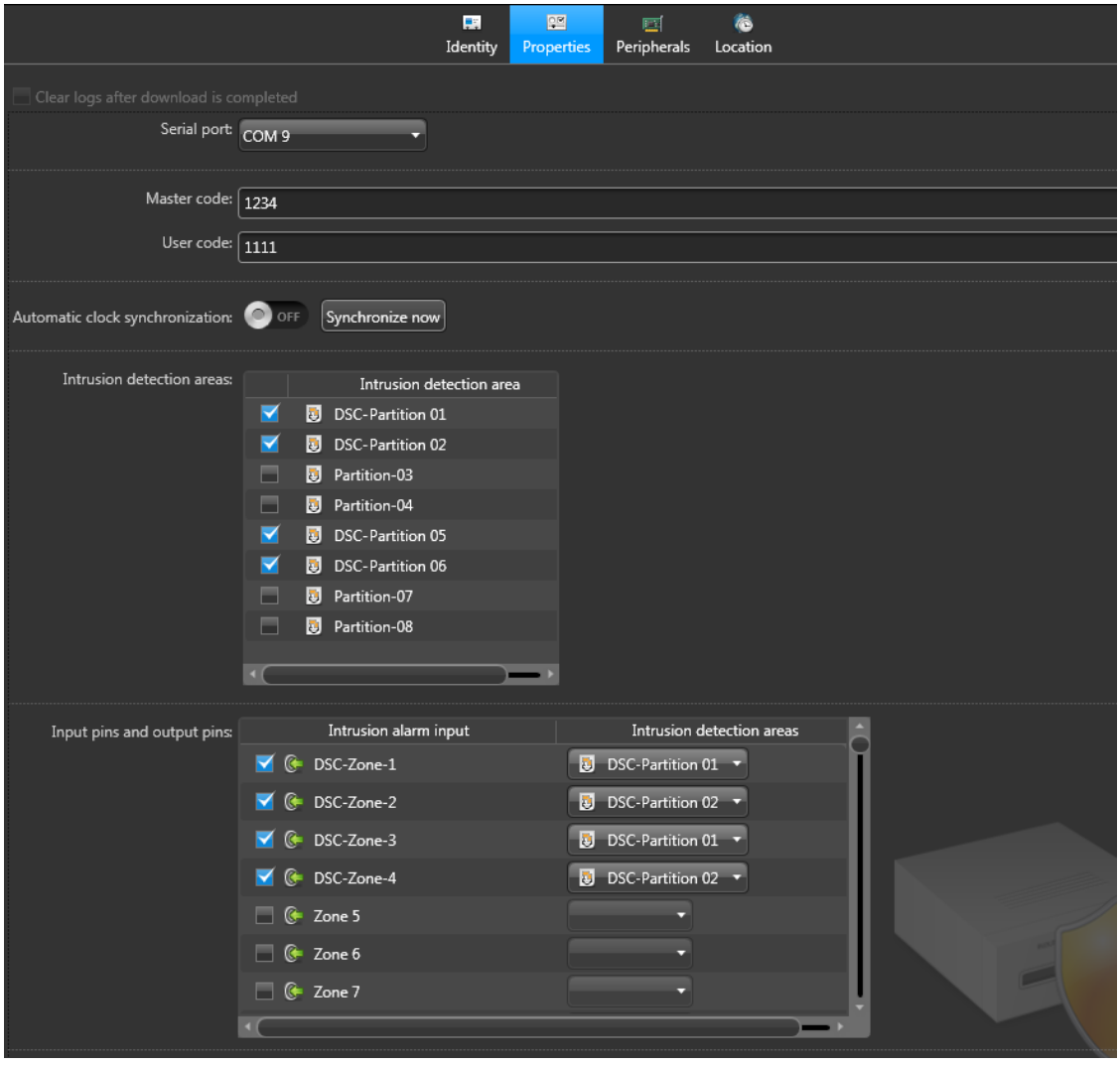
What you should know

In the intrusion detection unit **Properties** tab, you need to activate the intrusion detection areas to monitor, and map inputs and outputs to intrusion detection areas.

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 **Serial Port, Master code** and **User code** fields were configured when you created the intrusion detection unit.

3 (Optional) To synchronize the control panel's clock with Security Center server, set the **Automatic clock synchronization** option to **ON**.

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

4 In the **Intrusion detection areas** section, select the **Intrusion detection areas** to monitor in Security Desk.

5 In the **Input pins and output pins** section, select an intrusion detection area (partition) to map to each input and output. This helps identify where the input or output is located when you receive events from the control panel in Security Desk.

NOTE: Multiple intrusion detection areas can be selected for an output.

Related Topics

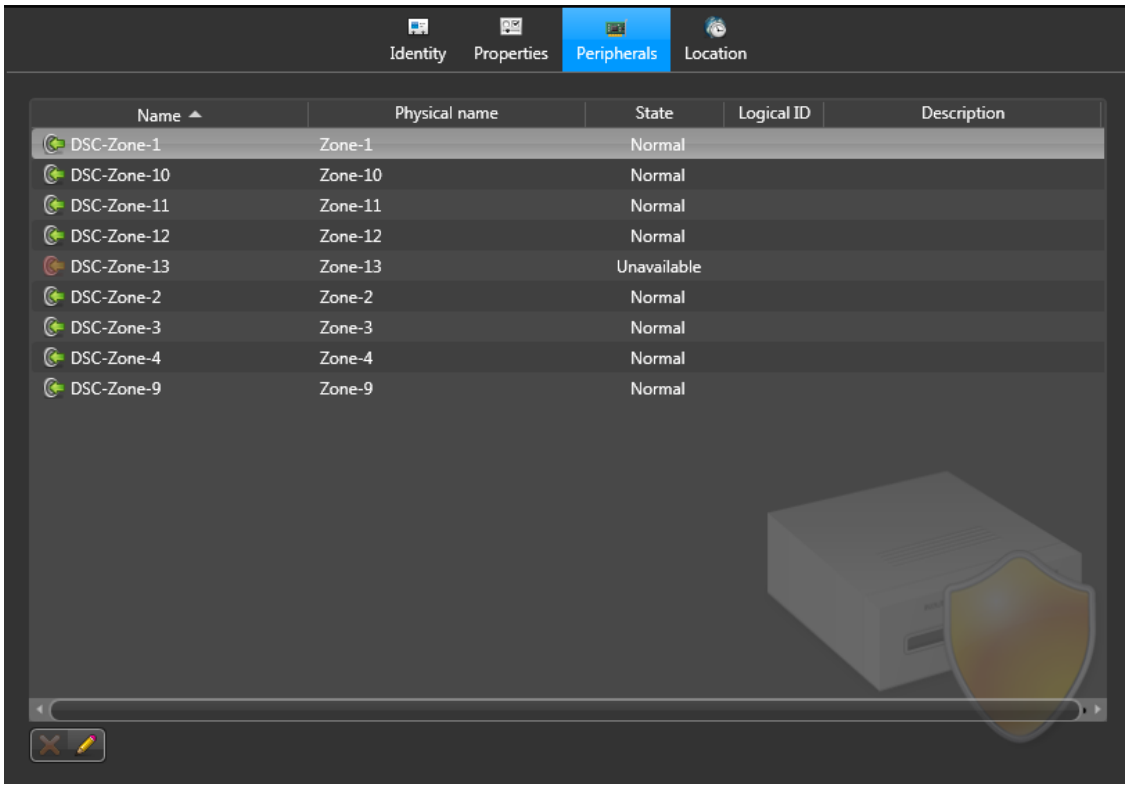
Creating the intrusion detection unit on page 16

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 and outputs.

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 Click **OK** > **Apply**.

After you finish

Associate cameras to intrusion detection areas, and then map DSC control panel events to Security Center actions.

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:

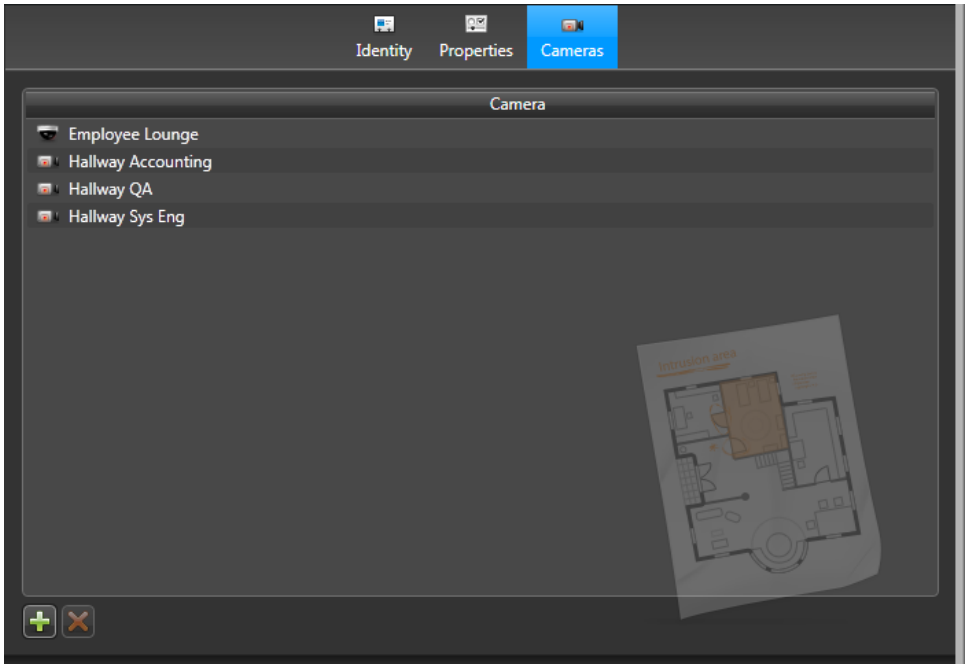
1 From the Config Tool home page, open the **Intrusion detection** task.

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.

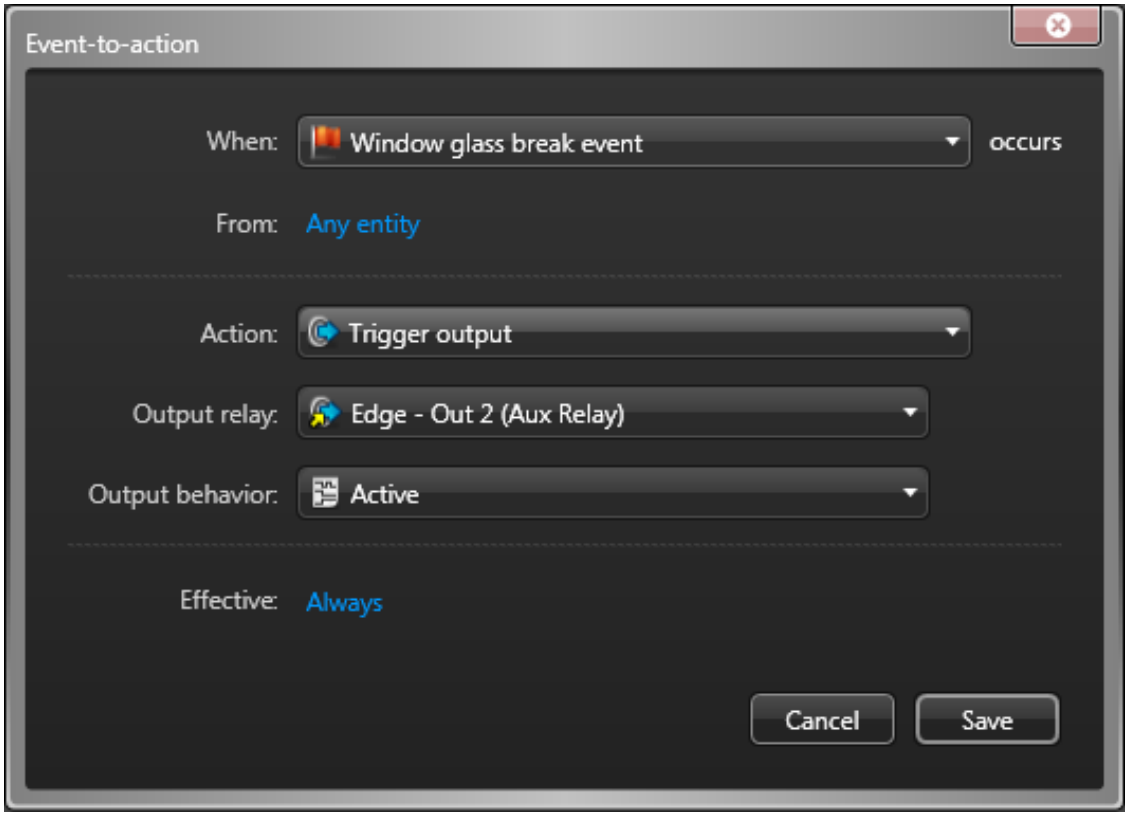
4 In the **When** drop-down list, select an event.

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**.

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.