Genetec™ Security Center.

Vanderbilt SPC Intrusion Panel Extension Guide 3.1

Click here for the most recent version of this document.

Document last updated: February 12, 2019

Genetec™

Legal notices

Document information

Document title: Vanderbilt SPC Intrusion Panel Extension Guide 3.1

Document number: EN.550.043-V3.1(4)

Document update date: February 12, 2019

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

About this guide

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

This guide supplements the documentation provided with Security Center. It assumes that you are a certified user of Security Center, Synergis™, and Omnicast™, and that you are familiar with the configuration and use of the following:

- Security Center systems
- Configuration and use of Vanderbilt SPC intrusion panels

For a list of Security Center courses, visit https://www.genetec.com/support/training/certification-courses.

For specific information regarding your hardware, software, and systems, refer to their manufacturer's documentation and website.

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 from Genetec Inc.

Contents

1

Introduction to the Vanderbilt SPC extension

This section includes the following topics:

What is the Vanderbilt SPC extension?

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

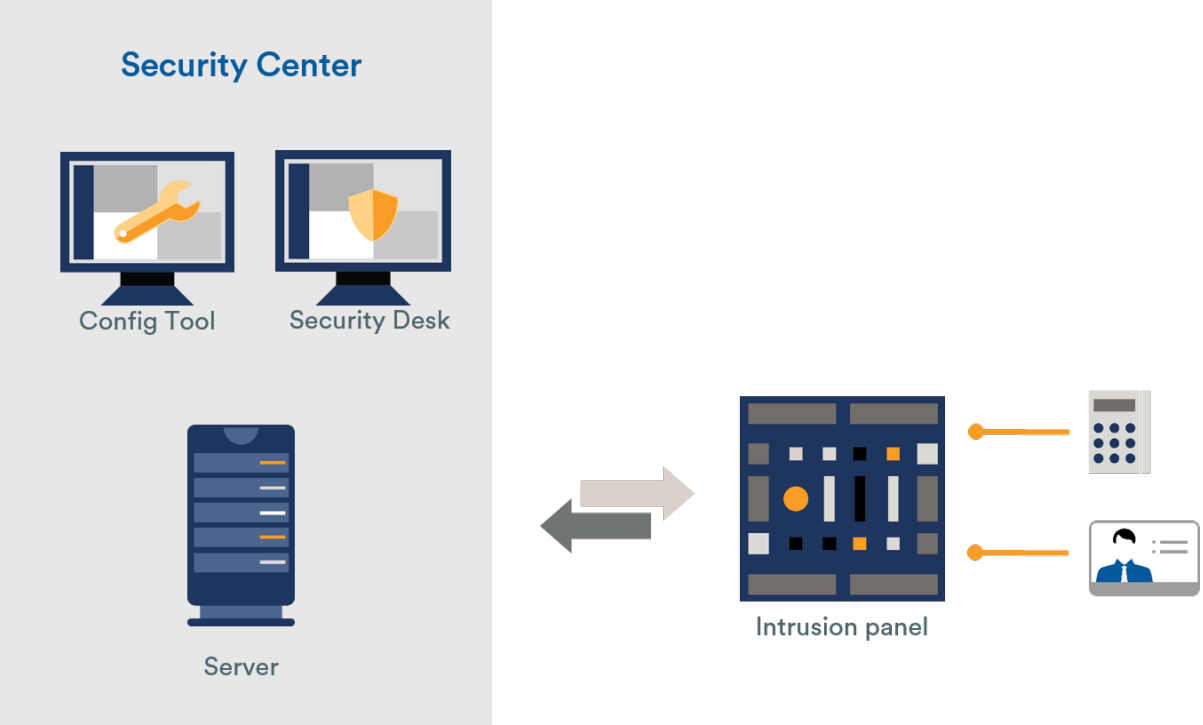
The integration allows you to do the following:

- Synchronize SPC intrusion panels and Security Center intrusion detection units,
- Synchronize SPC areas and Security Center intrusion detection areas,
- Synchronize SPC zones and Security Center inputs,
- Monitor SPC panel state changes in real-time using the *Monitoring* task and the *Maps* task in Security Desk,
- Monitor SPC area state changes in real-time using the *Monitoring* task and the *Maps* task in Security Desk,
- Monitor SPC zone state changes in real-time using the *Monitoring* task and the *Maps* task in Security Desk,
- Create event-to-actions for events that are sent from the SPC detection unit,
- Generate reports on activities related to SPC intrusion detection areas,
- Link Security Center virtual zones to SPC inputs,
- 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 using the intrusion detection area widget,
- Silence alarms on intrusion detection areas in Security Desk using the intrusion detection area widget,

How the Vanderbilt SPC extension works with Security Center

SPC intrusion panels are integrated to Security Center using the Intrusion Manager role.

The Intrusion Manager role receives events from the panel over an IP network, 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 SPC inputs are monitored

It is recommended that you only use intrusion panels for intrusion monitoring. Intrusion panels are not designed to capture rapid consecutive changes to their input states, such as doors being opened and closed rapidly, or motion sensors that detect constant movements.

The main purpose of an input on an intrusion panel is to trigger an alarm when its state changes. When the input becomes active, the panel raises an alarm. Security Center uses this alarm to trigger an *Intrusion detection area alarm activated* event.

Integration overview for Vanderbilt SPC intrusion panels

Integrating Vanderbilt SPC intrusion panels in Security Center consists of a series of steps that need to be followed in sequence.

Step	Description	Where to find more information
Learn about the release		
1	Read the release notes. Learn about any known issues, limitations, supported software, and other information about this release of the extension.	• What's new in the Vanderbilt SPC extension 3.1 on page 7 • Known issues in the Vanderbilt SPC extension 3.1 on page 8 • Limitations in the Vanderbilt SPC extension 3.1 on page 9 • Product compatibility for the Vanderbilt SPC extension 3.1 on page 10 • Supported devices with the Vanderbilt SPC extension 3.1 on page 11
Install the extension		
2	Make sure your system meets the Security Center and SPC requirements.	• *Security Center System Requirements* • Vanderbilt SPC documentation
3	Verify that your Security Center license has a valid certificate for the Vanderbilt SPC extension. From the Config Tool home page, click **About** > **Certificates** to confirm that *SPC* is on the list.	• The license number is included in the product-release email sent by Genetec Inc. This email also includes links to the extension download package and other license information. • If you need to acquire a new license, refer to License options for the Vanderbilt SPC extension on page 15.
4	Make sure you have the required Security Center user privileges for intrusion panel integration.	Granting user privileges for an intrusion panel integration on page 20
5	On the Security Center server, download the extension and install it.	Downloading and installing the Vanderbilt SPC extension on page 17
Configure your Vanderbilt SPC intrusion panels		
6	Using the SPC Pro application, configure your SPC intrusion panels to communicate over an IP network.	• Configuring Vanderbilt SPC panels for IP communication on page 22 • Best practices for connecting intrusion panels to the network on page 19 • Vanderbilt SPC documentation

Step	Description	Where to find more information
Configure the extension		
7	In Config Tool, create an Intrusion Manager role.	Creating the Intrusion Manager role on page 23
8	Configure the properties of the Vanderbilt SPC extension.	Configuring the Vanderbilt SPC extension properties on page 25
9	Create intrusion detection units in Security Center for each of your intrusion panels.	Creating the intrusion detection unit on page 26
10	Configure the properties for the intrusion detection units.	• Configuring properties of intrusion detection units on page 28 • Copying properties of intrusion detection units on page 30
11	(Optional) Assign a logical ID or a description to the inputs and outputs of your intrusion detection units.	Configuring inputs and outputs on page 31
12	Assign cameras to monitor your intrusion detection areas.	Mapping intrusion detection areas to cameras on page 32
13	Create event-to-actions using the custom events created by the Vanderbilt SPC extension in Security Center.	• Mapping intrusion panel events to Security Center actions on page 33 • How Vanderbilt SPC events are mapped in Security Center on page 37

2

Release notes

This section includes the following topics:

What's new in the Vanderbilt SPC extension 3.1

With each release, new features, enhancements, or resolved issues are added to the product.

The Vanderbilt SPC extension includes the following new features and enhancements.

- **Copying configuration:** You can now copy the properties from one intrusion detection unit to another from the *Copy configuration* page of the unit.
- **Configuring grace periods:** You can now configure a **Grace period**, **Alarm grace period**, and **Persistence grace period** from the *Extensions* page.
- **Configuring Listener settings:** Listener settings are now configured when you create an intrusion detection unit in Security Center or from the *Properties* page of the intrusion detection unit.

Released documents for Vanderbilt SPC extension 3.1

The documentation provided with a product is subject to change. With each product release, new documents might be added, current ones updated, and older ones replaced. For the latest version of the documentation, see the Genetec™ TechDoc Hub.

Document title	Status	Languages	Availability
Vanderbilt SPC Intrusion Panel Extension Guide 3.1	New	English, Spanish	TechDoc Hub, Azure, Installation package
Supported Plugins in Security Center	Updated	English, French, Spanish, German	TechDoc Hub

Known issues in the Vanderbilt SPC extension 3.1

Known issues are software issues that have been discovered in the current release or a previous release, and have not yet been resolved.

There are no known issues in the Vanderbilt SPC extension 3.1.

Limitations in the Vanderbilt SPC extension 3.1

Limitations are software or hardware issues that cannot be fixed. For certain limitations, workarounds are documented.

The Vanderbilt SPC extension 3.1 includes the following known limitation.

Issue	Description
401	On the *Properties* page of the Intrusion Manger role, the **Reconnection delay** setting does not work.
388	Failover is not supported.
378	When the alarm state of an intrusion detection area is *Active*, you can physically silence the alarm, but the alarm state will remain as *Active* instead of changing to *Silenced*.
376	In the case of a connection loss, the Intrusion Manager will download the event logs from the SPC panel after the panel is reconnected. If the clock of the panel is not synchronized with the clock of the Security Center server, events will not be logged properly. For example, if the clock of the panel is slower, current events will not appear in the *Monitoring* task, and will be logged as offline events instead.
375	If an administrator deletes an enrolled intrusion detection unit (intrusion panel) from the Intrusion Manager, a new ATS configuration needs to be created using the SPC Pro application to enroll the panel again.
374	The *Inhibit*, *Deinhibit*, and *Restore* actions in SPC, are mapped to the *Bypass*, *Clear bypass*, and *Restore* actions, respectively, in Security Center. The *Isolate* and *Deisolate* actions are not supported in Security Center.
369	You can Perimeter arm an intrusion detection area to either **Partset A** or **Partset B**, but not to both.
366	The *Force set* action in SPC Pro is not available in Security Center.
271	When using Full Engineer Mode in SPC Pro, you cannot receive input state change events in Security Center.
246	SPC panels must have an IP connection.

Product compatibility for the Vanderbilt SPC extension 3.1

Product compatibility indicates that the product can support and run with specific versions of other products.

To be eligible for technical support, you must install the Security Center and third-party software versions that are listed as certified or supported by design in the following table.

Extension	Third-party version	Certified Security Center version
Vanderbilt SPC extension 3.1	**Certified:** Firmware version 3.6.6 **Supported by design:** Firmware version 3.8.5	5.6 SR1 and 5.7

Product compatibility indicates that the product supports and can run with specific versions of other products. A product is compatible when it meets one of the following certification levels:

- **Certified:** Genetec Inc. has tested and validated the product.
- **Supported by design:** The product has similar characteristics or is a newer version of a certified version, but Genetec Inc. has not tested or validated the product.

  NOTE: Service releases of a major release are supported by design. For example, if 5.6 SR2 is listed, then SR3 and subsequent service releases for 5.6 are supported. If a major release is not listed, then it is not supported.

Related Topics

Supported devices with the Vanderbilt SPC extension 3.1 on page 11

Supported devices with the Vanderbilt SPC extension 3.1

The SPC extension supports specific external Vanderbilt SPC devices.

The SPC extension 3.1 supports the following intrusion panels. For each device, the corresponding certification level is listed.

- **Certified:** The panel has been tested and validated by Genetec Inc.
- **Supported by design:** The panel shares the same design characteristics as a certified panel but has not been validated or tested by Genetec Inc.

Model	Device type	Requirements	Certification
SPC Panel series 4000	Intrusion panel	On-board IP connection	Supported by design
SPC Panel series 4200	Intrusion panel	On-board IP connection	Supported by design
SPC Panel series 4300	Intrusion panel	On-board IP connection	Supported by design
SPC4320	Intrusion panel	On-board IP connection	Certified
SPC Panel series 5200	Intrusion panel	On-board IP connection	Supported by design
SPC Panel series 5300	Intrusion panel	On-board IP connection	Supported by design
SPC Panel series 6300	Intrusion panel	On-board IP connection	Supported by design
SPC6330	Intrusion panel	On-board IP connection	Certified

Supported intrusion detection features

Discover the intrusion detection features that are supported in Security Center for an integration with Vanderbilt SPC intrusion panels.

The following table lists the standard features for all Security Center intrusion detection integrations. For each feature, one of the following is shown:

- **Yes:** Feature is offered by the intrusion panel, and is available in Security Center.
- **No:** Feature is offered by the intrusion panel, but is unavailable in Security Center.
- **Not applicable:** Feature is not offered by the intrusion panel.

Feature		Supported
Communications		
Serial connection		No
TCP/IP connection		Yes
Data encryption over TCP/IP		Yes
Status monitoring		
Report online and offline status of intrusion units in real time		Yes
Intrusion detection area states	Master armed	Yes
	Perimeter armed	Yes
	Alarm silenced	No
	Disarmed	Yes
	Ready-to-arm	Yes
	Intrusion alarm active	Yes
	Input trouble	Yes
	Entry delay	No
Near real-time status monitoring of inputs and outputs		Yes
Input entity states	Normal	Yes
	Active	Yes
	Trouble	Yes
	Alarm	Yes

Feature		Supported
	Bypassed	Yes
Event reporting		
Report events from offline units automatically upon reconnection		Yes
Intrusion detection unit events	Unit connected	Yes
	Unit lost	Yes
	AC fail	Yes
	Battery fail	Yes
	Tamper	Yes
Intrusion detection area events	Master armed	Yes
	Perimeter armed	Yes
	Disarmed	Yes
	Auto-arming postponed	No
	Forced arming	No
	Duress	Yes
	Entry delay started	No
	Intrusion alarm silenced	No
	Intrusion alarm activated	Yes
Controlling units and devices		
Trigger alarms on intrusion areas		Yes
Silence alarms from intrusion areas		No, but you can silence the physical alarm
Acknowledge alarms from intrusion areas		Yes
Arm areas	Instant master	Yes
	Delayed master	Yes
	Arming delay (Override default delay)	Yes
	Instant perimeter	Yes
	Delayed perimeter	Yes

Feature		Supported
	Forced	No
	Bypass	No
Set inputs to bypass mode		Yes
Trigger outputs on intrusion units		Yes
Configuration		
Authentication between intrusion unit and Intrusion Manager role		Not applicable
Create intrusion detection areas automatically		Yes
Create input entities automatically		Yes
Create output entities automatically		Yes
Link input entities to intrusion detection areas automatically		Yes
Associate custom events to incoming PIN events		No
Keep clock on panel synchronized with Security Center		No
Link cardholders to users on the intrusion unit		No
Modify user PIN credentials		No

License options for the Vanderbilt SPC extension

Before installing the Vanderbilt SPC extension, you must update your Security Center license to include a certificate for the extension. To update your license, contact us and provide the part numbers listed in this topic.

Use the following part numbers to get the license certificate for the extension.

Part number	Description	Requirements
GSC-1AP-CDC2-SPC	Vanderbilt SPC intrusion alarm panel connection Supports one panel	• Professional or Enterprise packages • Genetec™ Advantage

Does your Security Center license include all the options you need?

In addition to a certificate for your extension, ensure that your Security Center license includes all the options you expect to use in Security Center. For example, if you integrated a system that has visitors, you need the Visitors option in Security Center. If an option is missing, an error message is displayed when the server tries to create or modify the entity related to that option.

For a list of available license options, see "License options" in the *Security Center Administrator Guide*.

3

Installing the Vanderbilt SPC extension

This section includes the following topics:

Downloading and installing the Vanderbilt SPC extension

To integrate SPC intrusion panels into Security Center, you must install the Vanderbilt SPC extension on a Security Center expansion server and on all client workstations.

What you should know

You must also install the extension on all of the Security Center client workstations.

To install the SPC extension:

1. Open the GTAP Product Download page.
2. From the **Download Finder** list, select your version of Security Center.
3. Search for your package by name and download it.
4. Click the downloaded *.exe* file to unzip the file.

   By default, the file is unzipped to *C:\Genetec*.
5. Open the extracted folder, right-click the *setup.exe* file, and click **Run as administrator**.
6. Follow the installation instructions.
7. On the *Installation Wizard Completed* page, click **Finish**.

   IMPORTANT: The **Restart Genetec™ Server** option is selected by default. You can clear this option if you do not want to restart the Genetec™ Server immediately. However, you must restart the Genetec™ Server to complete the installation.
8. Close, and then open, any instances of Config Tool and Security Desk.

4

Configuring Vanderbilt SPC intrusion panels in Security Center

This section includes the following topics:

Best practices for connecting intrusion panels to the network

Intrusion detection panels are not 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 having the panel reconnect repeatedly, we recommend that you 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 network node configuration capabilities.

Granting user privileges for an intrusion panel integration

For administrators to install and configure the extension in Config Tool, and for operators to monitor intrusion detection units in Security Desk, the correct user privileges must be granted to their user accounts.

What you should know

This task lists the minimum privileges required to monitor and control intrusion detection units in Security Center.

You might require more privileges, depending on the tasks you want to perform in Config Tool and Security Desk. For a description of all user privileges, see Security Center Privileges.

To grant user privileges:

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

2 Select the relevant user, and click the **Privileges** tab.

3 Set the following privileges to **Allow**.

Privilege	Task
Application privileges	
Config Tool	To use Config Tool.
Security Desk	To use Security Desk.
Administrative privileges > Physical entities	
View intrusion detection area properties	To view the intrusion detection area configuration pages in Config Tool.
Modify intrusion detection area properties	To modify the intrusion detection area configurations in Config Tool.
Add and delete intrusion detection areas	To add or delete intrusion detection areas in Config Tool.
View intrusion detection unit properties	To view the intrusion detection unit configuration pages in Config Tool.
Modify intrusion detection unit properties	To modify the intrusion detection unit configurations in Config Tool.
Add and delete intrusion detection units	To add or delete intrusion detection units in Config Tool.
Administrative privileges > Alarm management	
View alarm properties	To view alarm configuration pages in Config Tool.
Modify alarm properties	To modify alarm configuration settings in Config Tool.
Add and delete alarms	To add or delete alarms in Config Tool.
Task privileges > Administration	
Intrusion detection	To use the *Intrusion detection* task in Security Desk.

Privilege	Task
Task privileges > Operation	
Monitoring	To use the *Monitoring* task in Security Desk.
Task privileges > Investigation	
Intrusion detection area activities	To use the *Intrusion detection area activities* task in Security Desk.
Task privileges > Maintenance	
Intrusion detection unit events	To use the *Intrusion detection unit events* task in Security Desk.
Task privileges > Alarm management	
Alarm monitoring	To use the *Alarm monitoring* task in Security Desk.
Alarm report	To use the *Alarm report* task in Security Desk.
Action privileges > Alarms	
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.
Action privileges > Intrusion detection	
Acknowledge intrusion alarm	To acknowledge alarms in intrusion detection areas in Security Desk.
Arm and disarm intrusion detection areas	To arm or disarm intrusion detection areas from Security Desk.
Silence intrusion alarm	To silence alarms in intrusion detection areas in Security Desk.
Trigger intrusion alarm	To trigger alarms in intrusion detection areas in Security Desk.

Configuring Vanderbilt SPC panels for IP communication

For Security Center to communicate with SPC intrusion panels through an IP network, you must configure the panel settings, using SPC Pro, before adding the unit in Security Center.

Before you begin

Read the Vanderbilt SPC quick start guide and installation guide that applies to your hardware.

To connect the panel using the SPC Pro application:

1 From the **Communications** tab, open the *FlexC* page.
2 In **Event profiles**, create a new event profile to include all events for all areas.
3 In **Command profiles**, create a new command profile to include all commands for all users.
4 In **FlexC ATS**, click the **Add single path ATS** button to open the *FlexC ATP Configuration* window.
5 In the **RCT URL or IP Address** field, enter the IP address of the Security Center server that manages the intrusion panels.

   NOTE: If a panel is being re-enrolled, the FlexC ATS value corresponding to the extension must be deleted and recreated.

   For more information about ATS creation, see your Vanderbilt SPC documentation.

6 Select the ATS that you just created from the list to open the *ATS Configuration* window.
7 In the *ATS Profile* section, select the event profile you just created so that Security Center can receive the events specified in that event profile from SPC.
8 Select the command profile you created so that you can use the commands defined in that command profile in Security Center.
9 In the **Advanced** tab, open the **Mapping Gates** page.
10 In *Mapping Gates List*, create mapping gates and assign outputs to them.

   IMPORTANT: Each entry in the *Mapping Gates List* must have a description because the description is used to name the output in Security Center.

11 Configure the panel settings, such as the intrusion areas, inputs (zones), outputs (relays), and other behavior.

   For more information about configuring the panel settings, see your Vanderbilt SPC documentation.

12 Configure the panel time. Set **Date/Time** to be the same as the Genetec™ Server that hosts Intrusion Manager role.

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.

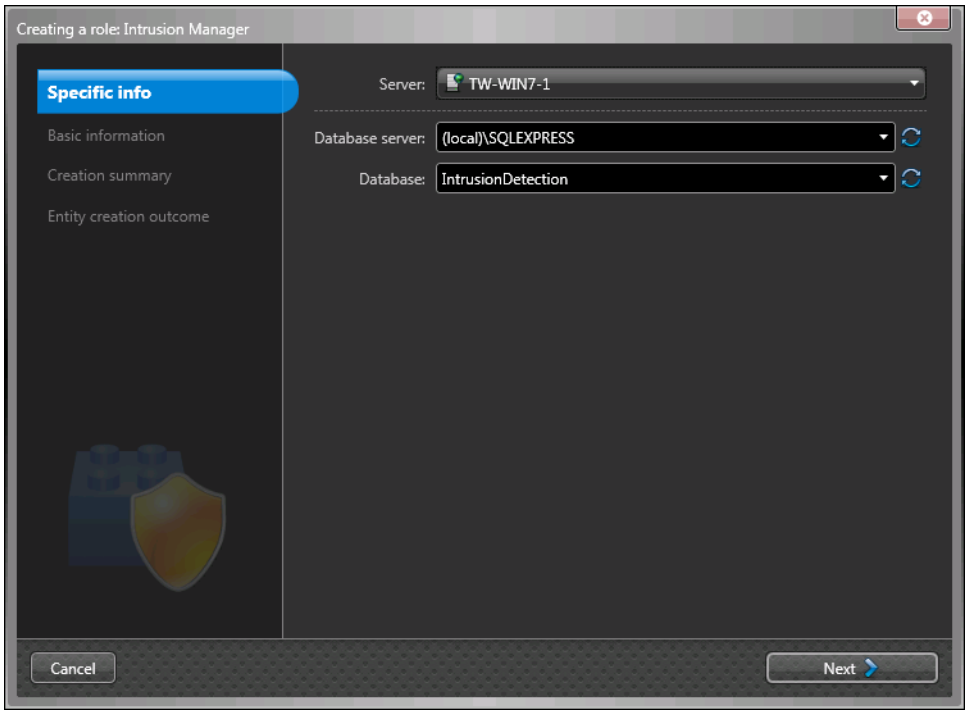
What you should know

You must create an Intrusion Manager role for each Vanderbilt SPC intrusion 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 click **Intrusion Manager**.
The *Creating a role: Intrusion Manager* window opens.



3 In the **Specific info** tab, 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 enter 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 In the **Basic information** tab, do the following:
a) Enter the **Entity name** (**Intrusion Manager**)
b) Optional: Enter an **Entity description** for the role.
c) Click **Next**.

5 In the **Creation summary** tab, 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 is displayed in your entity browser.

Related Topics

Creating the intrusion detection unit on page 26

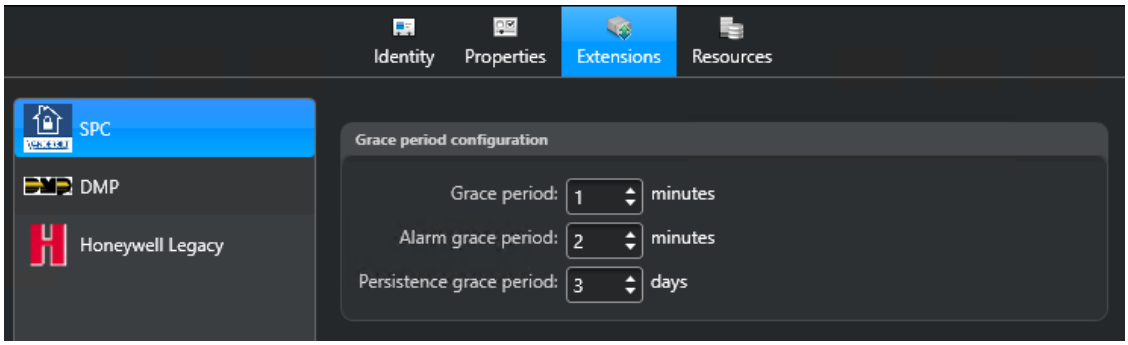
Configuring the Vanderbilt SPC extension properties

To use Vanderbilt SPC intrusion panels in Security Center, you must configure how the Intrusion Manager listens for SPC panel connections.

To configure the SPC extension properties:

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

2 Select the Intrusion Manager role, click the **Extensions** tab, and click the **SPC** page.



3 Configure the following options:

- **Grace period:** Select the period in which events can occur while the panel is offline, so that they are treated as normal events after the panel reconnects.

  Events from the panel that occurred within the *Grace period* are treated as normal events in Security Desk after the panel reconnects. The events appear in the event list in the *Monitoring* task, are recorded in the database, and event-to-actions that were set up for the event are triggered.

- **Alarm grace period:** Select the period in which alarms can occur while the panel is offline, so that they are treated as normal alarms after the panel reconnects.

  Alarms from the panel that occurred within the *Alarm grace period* are treated as normal alarms in Security Desk when the panel reconnects. They appear in the alarm list in the *Alarm monitoring* and *Monitoring* tasks, and are recorded in the database.

- **Persistence grace period:** Events and alarms from the panel that occurred within the *Persistence period* while the panel was offline, are only recorded in the database when the panel reconnects. Events and alarms that occur outside of the *Persistence period* are not recorded.

4 Click **Apply**.

Creating the intrusion detection unit

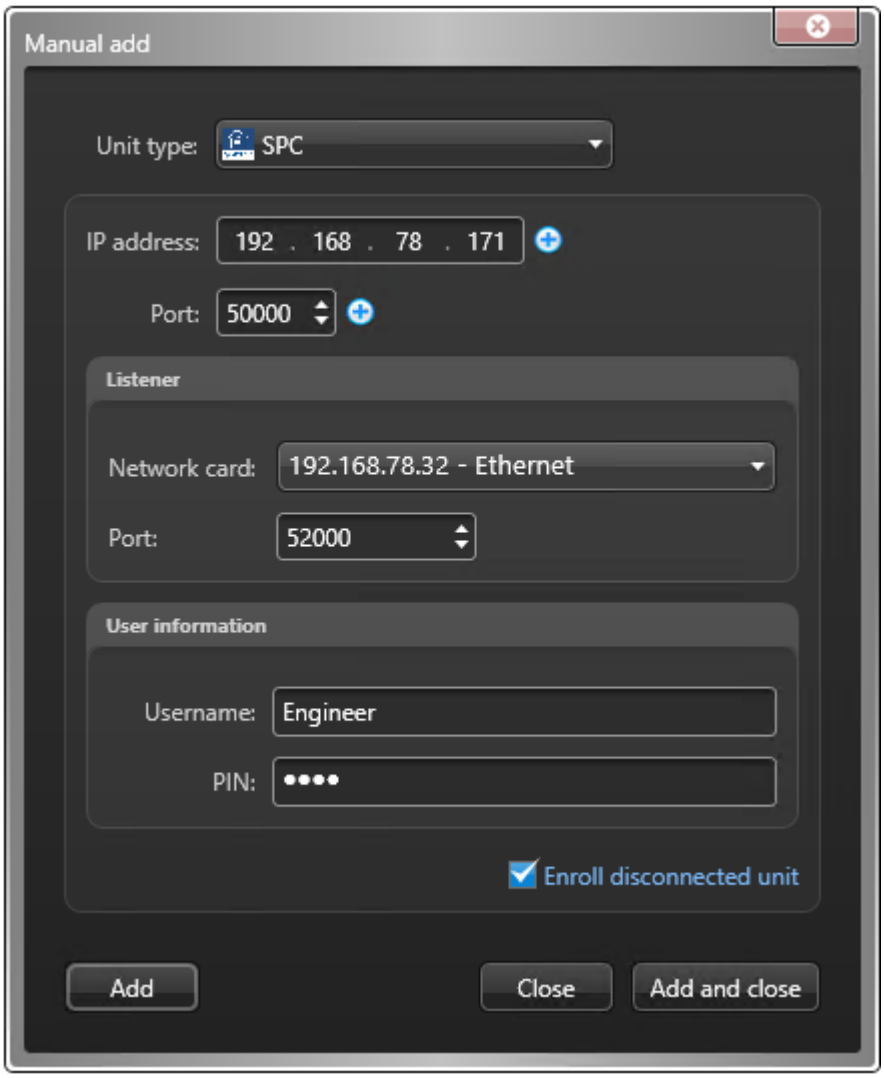
To be able to use an intrusion panel in Security Center, you must create the panel as an *intrusion detection unit* entity in Config Tool.

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 From the entity browser, select the Intrusion Manager role that will manage the intrusion panel.
3 Under the entity browser, click **Intrusion detection unit** ( ).
4 From the **Unit type** drop-down list in the *Manual add* dialog box, select **SPC**.



5 Enter the IP address of the intrusion panel.
6 In the **Port** field, select the port number configured in the panel.
50000 is the default value.
7 In the *Listener* section, configure the following settings:

- **Network card:** The Genetec™ Server network card used to communicate with SPC intrusion panels.

- **Port:** The Genetec™ Server TCP port used for SPC panel connections.

NOTE: Refer to the FlexC and ATS configuration in the SPC Pro application.

8 In the *User information* section, enter the following credentials:
   - **Username:** The name of the SPC panel user to connect the panel.
   - **PIN:** The PIN you configured on the panel for the selected user.
9 Select the **Enroll disconnected unit** check box to enroll the SPC intrusion panel, even if it is not yet physically connected.
10 Click **Add and close**.

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

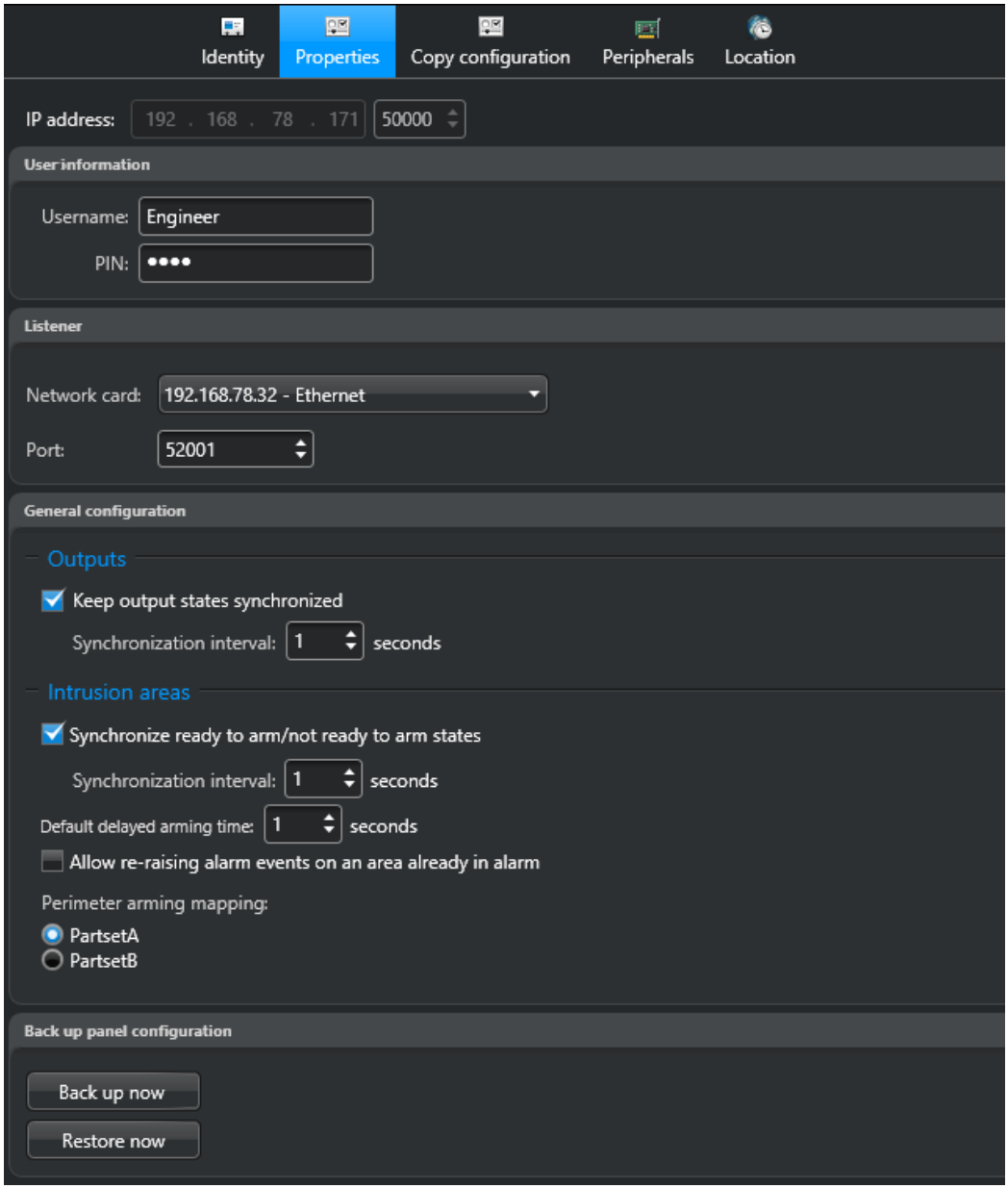
Configuring properties of intrusion detection units

To receive intrusion events and alarms from the SPC in Security Desk, you must configure the intrusion detection unit in Config Tool.

To configure the properties of an intrusion detection unit:

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

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



- **IP address:** The IP address of the selected intrusion detection unit.

User information

- **Username:** The name of the SPC panel user to connect the panel.
- **PIN:** The PIN you configured on the panel for the selected user.

Listener

- **Network card:** The Genetec™ Server network card used to communicate with SPC intrusion panels.
- **Port:** The Genetec™ Server TCP port used for SPC panel connections.

NOTE: Refer to the FlexC and ATS configuration in the SPC Pro application.

Outputs

- **Keep output states synchronized:** Select this option to keep the output states from the intrusion detection unit synchronized with Security Center.
- **Synchronization interval:** How often the output state of the intrusion detection unit gets synchronized with Security Center.

Intrusion areas

- **Synchronize ready to arm/not ready to arm states:** Select this option to synchronize the state of the intrusion detection area with the intrusion detection unit.
- **Synchronization interval:** How often the state of the intrusion detection area gets synchronized with Security Center.
- **Default delayed arming time:** The default duration of the delay used by the delayed arming command. If a custom delay is set on the Security Desk widget, this default time is not used.
- **Allow re-raising alarm events on an area already in alarm:** Select this option to allow Security Center to trigger another alarm on an area already in an *Active* alarm state. If this option is cleared, new alarms (for the same intrusion detection area) will only be triggered when the previous alarm has been acknowledged.
- **Perimeter arming mapping:** Select the Partset mode to be used by the intrusion detection unit when a perimeter arming command is used by Security Center. Partset A or Partset B can be used in SPC panel configuration.

Back up panel configuration

- **Back up now:** Click to back up the panel configuration. Select the local folder to start the backup.
- **Restore now:** Click to send a configuration file to the intrusion panel. Select the CFG file to start the restore.

3 Click **Apply**.

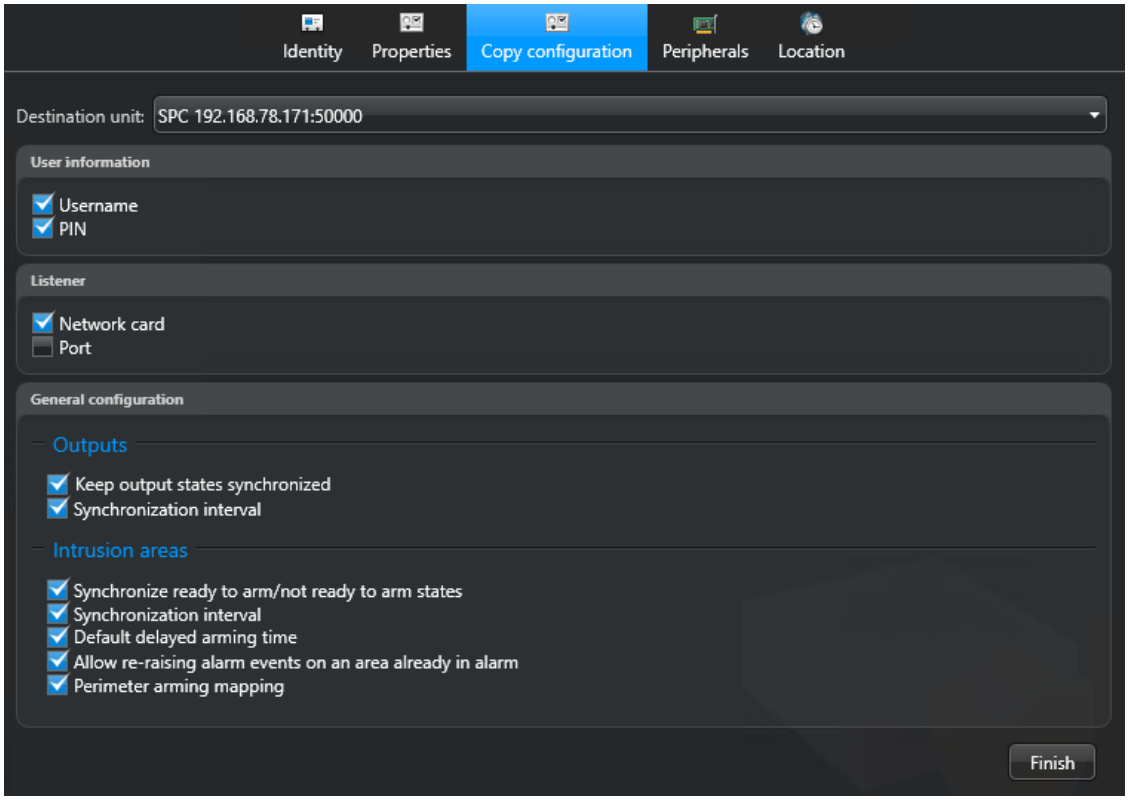
Copying properties of intrusion detection units

To facilitate the configuration of intrusion detection units in Security Center, you can copy the properties configured on one unit to another unit.

To copy properties from one intrusion detection unit to another:

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

2 Under the Intrusion Manager role in the entity browser, select the intrusion detection unit to copy from, and then click the **Copy configuration** tab.



3 From the **Destination unit** list, select the intrusion detection unit to which you want to copy configuration.

4 Select the check boxes for the properties you want to copy.

5 Click **Finish**.

The properties you selected are now copied over to the destination unit.

Configuring inputs and outputs

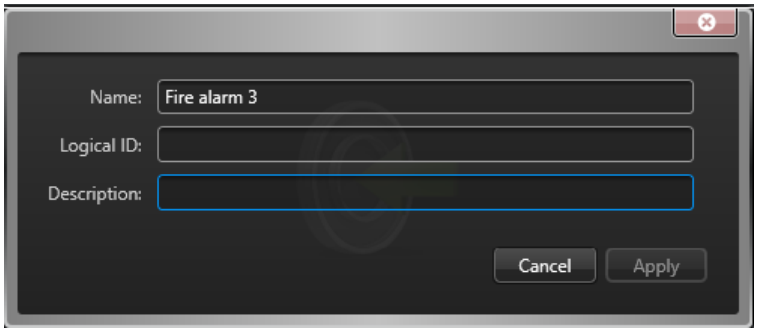
In the intrusion detection unit **Peripherals** tab, you can assign logical IDs and descriptions to the inputs (zones) and outputs (relays) controlled by the unit.

What you should know

Input types are configured on the panel itself; the input type cannot be configured in Security Center.

To configure inputs and outputs:

1 From the Config Tool home page, open the *Intrusion detection* task.
2 Select the intrusion detection unit to configure, and click the **Peripherals** tab.
3 Select an input, and at the bottom of the **Peripherals** tab, click .
4 In the **Name** field, the name of the input connected to the panel is displayed.



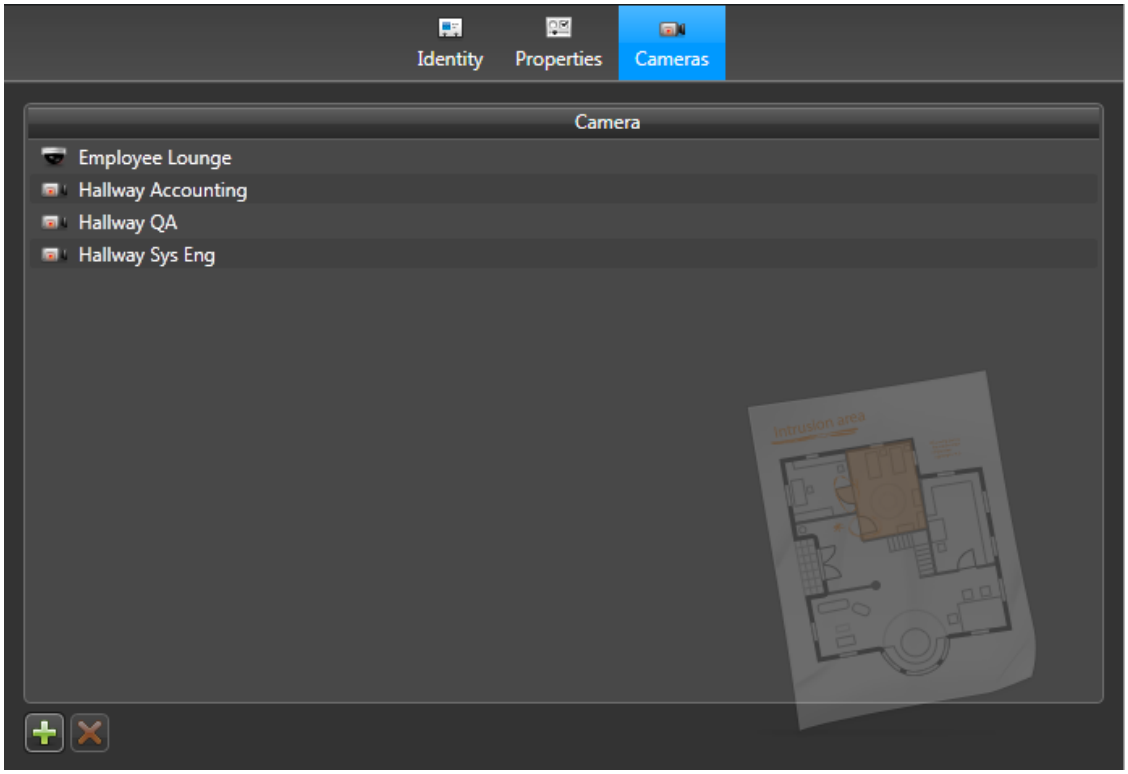
5 Enter a **Logical ID** for the input.
Setting a Logical ID helps you to easily identify the input in Security Center.
6 Enter a **Description** for the input.
7 Click **OK**, and then click **Apply**.
8 Select an output, and at the bottom of the **Peripherals** tab, click .
9 In the **Name** field, the name of the output connected to the panel is displayed.
10 Enter a **Logical ID** for the output.
Setting a Logical ID helps you to easily identify the output in Security Center.
11 Enter a **Description** for the output.
12 Click **OK**, and then click **Apply**.

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 *Area view* task.
2 Select the intrusion detection area to configure, then click the **Cameras** tab.
3 Click **Add an item** ( ).
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 intrusion 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 intrusion 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 .

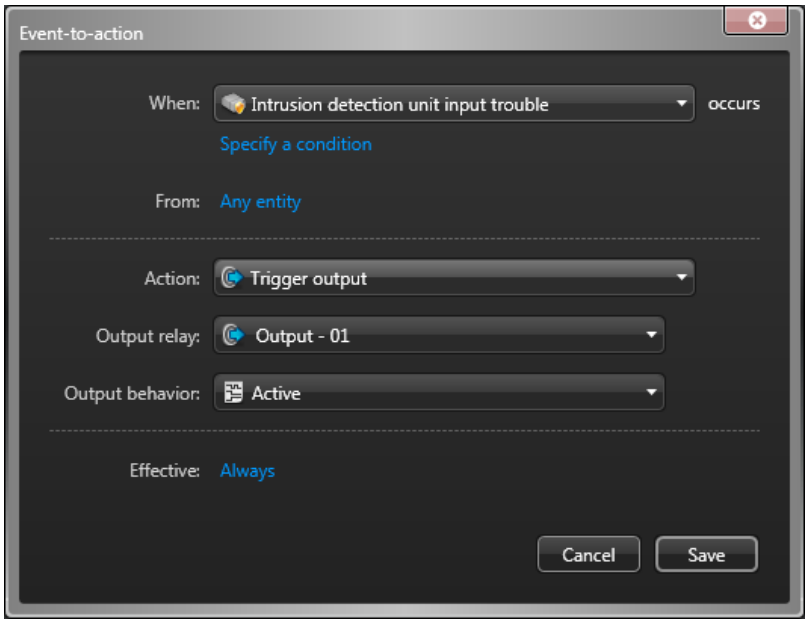
4 From the **When** drop-down list in the *Event-to-action* dialog box, select an event.

5 In the **From** option, select an **Intrusion detection unit** or **Intrusion detection area** that is the source of the event.

By default, the event-to-action occurs when **Any entity** triggers the event you selected.

6 From 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.



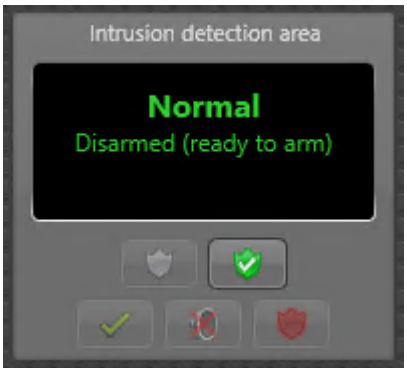
7 In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, then the action is not triggered. By default, the **Always** schedule is selected.

8 Click **Save**.

Intrusion detection area widget

When an intrusion detection area is displayed in a tile in Security Desk, you can arm or disarm the area, and interact with intrusion alarms using the *Intrusion detection area* widget.



The *Intrusion detection area* widget is described in the following table:

NOTE: Some commands might be unavailable if you lack a necessary privilege, or the command is not supported by the intrusion panel you are using.

Button	Command	Description
	Disarm	Disarms the intrusion detection area. Sensor activity in the area is ignored by the intrusion panel.
	Arm	Arms the intrusion detection area. The following options are available: • **Master:** Arms all sensors in the intrusion detection area. Any sensor can trigger the alarm when activated. • **Perimeter:** Arms only the sensors designated to be on the perimeter. Activity on sensors inside the area, such as motion detectors, is ignored. • **Instant:** Arms the area immediately. • **Delay:** Arms the area after a delay. If you do not specify a specific duration, the panel default is used. • **Force:** If the area is not ready for normal arming, this option forcefully arms the area. Force temporarily ignores active or troubled sensors during the arming sequence. If an ignored sensor ever returns to a normal state while armed, future activity can trigger the alarm. • **Bypass:** If the area is not ready for normal arming, this option automatically bypasses active or troubled sensors before arming the area. Sensors remain bypassed while the area is armed. Disarming the area removes the bypass.
	Trigger intrusion alarm	Trigger an intrusion alarm on the selected intrusion detection area.

Button	Command	Description
	**Silence alarm**	If there is an active alarm on the selected intrusion detection area, stop the siren on the intrusion panel from beeping. Depending on your intrusion panel and the type of alarm, clicking **Silence alarm** might also acknowledge the alarm. For example, with Bosch intrusion panels using Mode 2, *Burglary* alarms are acknowledged from Security Desk, but *Fire* alarms must be acknowledged on the panel keypad.
	**Acknowledge alarm**	Acknowledge the intrusion alarm on the selected intrusion detection area.

5

Additional resources

This section includes the following topics:

How Vanderbilt SPC events are mapped in Security Center

The extension automatically maps Vanderbilt SPC events with events and custom events in Security Center.

The extension creates new custom events as required by the integration. If new events are added in SPC, it is also possible to map them to custom events in Security Center.

Most SPC events are mapped to Security Center events of the same name. The following table only lists those that are mapped to events that are named differently in Security Center.

Vanderbilt SPC event	Security Center event
Burglary Alarm [Alarm Zone]	Intrusion detection area alarm activated
Burglary Alarm [Entry/Exit Zone]	
Burglary Alarm [Exit Term Zone]	
Burglary Alarm [Fire Exit Zone]	
Burglary Alarm [Seismic Zone]	
Burglary Alarm [Lock element Zone]	
Burglary Alarm [Glass Break Zone]	
Unset[1]	Intrusion detection area disarmed
[1]When an area is unset, in most cases, no alarm is triggered if an input (zone) is activated. In somes cases, a 24-hour input can trigger an alarm even if the area is unset. For more information about Unset mode, refer to Vanderbilt SPC documentation.	
User Duress[2]	Intrusion detection area duress
[2]The User Duress function activates a silent signal that is sent to alert security personnel. The User Duress event is triggered by incrementing the last digit of a user's PIN. This option must be configured by an SPC administrator. For more information about User Duress, refer to Vanderbilt SPC documentation.	
Entry Timer Started[3]	Intrusion detection area entry delay activated
[3]When the exit time period has expired, the system is set and opening an entry/exit input (zone) starts the entry timer. If the system is not unset before the entry timer expires, the alarm is activated. For more information about Entry Timer Started, refer to Vanderbilt SPC documentation.	
Fullset[4]	Intrusion detection area master armed
[4]When an area is set, an alarm is triggered when an input (zone) is activated. In Fullset mode, all inputs included in the area are able to trigger an alarm, if activated. In certain cases (for example, when a zone is already activated or in trouble), it is not possible to set an area. The area state displayed in this case is *Disarmed, not ready to arm*. For more information about Fullset mode, refer to Vanderbilt SPC documentation.	

Vanderbilt SPC event	Security Center event
Partset A or Partset B[5]	Intrusion detection area perimeter armed
[5]When an area is set, an alarm is triggered when an input (zone) is activated. In PartSet mode, only a few inputs included in the area are able to trigger an alarm, if activated. In certain cases (for example, when a zone is already activated or in trouble), it is not possible to set an area. The area state displayed in this case is *Disarmed, not ready to arm*. For more information about Partset mode, refer to Vanderbilt SPC documentation.	
Zone inhibit [Alarm Zone]	Intrusion detection unit input bypass activated
Zone inhibit [Entry/Exit Zone]	
Zone inhibit [Exit Term Zone	
Zone inhibit [Fire Zone]	
Zone inhibit [Fire Exit Zone]	
Zone inhibit [Line Zone]	
Zone inhibit [Panic Zone]	
Zone inhibit [Holdup Zone]	
Zone inhibit [Tamper Zone]	
Zone inhibit [Tech Zone]	
Zone inhibit [Medical Zone	
Zone inhibit [Keyarm Zone	
Zone inhibit [Unused Zone	
Zone inhibit [Shunt Zone]	
Zone inhibit [X-Shunt Zone]	
Zone inhibit [Detector Fault Zone]	
Zone inhibit [Lock Supervision Zone]	
Zone inhibit [Lock Supervision Zone]	
Zone inhibit [Seismic Zone]	
Zone inhibit [All Okay Zone]	
Zone inhibit [Holdup Fault Zone]	
Zone inhibit [Warning Fault Zone]	

Vanderbilt SPC event	Security Center event
Zone inhibit [Setting authorisation Zone]	
Zone inhibit [Lock element Zone]	
Zone inhibit [Glass Break Zone]	
Zone deinhibit [Alarm Zone]	Intrusion detection unit input bypass deactivated
Zone deinhibit [Entry/Exit Zone]	
Zone deinhibit [Exit Term Zone	
Zone deinhibit [Fire Zone]	
Zone deinhibit [Fire Exit Zone]	
Zone deinhibit [Line Zone]	
Zone deinhibit [Panic Zone]	
Zone deinhibit [Holdup Zone]	
Zone deinhibit [Tamper Zone]	
Zone deinhibit [Tech Zone]	
Zone deinhibit [Medical Zone	
Zone deinhibit [Keyarm Zone	
Zone deinhibit [Unused Zone	
Zone deinhibit [Shunt Zone]	
Zone deinhibit [X-Shunt Zone]	
Zone deinhibit [Detector Fault Zone]	
Zone deinhibit [Lock Supervision Zone]	
Zone deinhibit [Lock Supervision Zone]	
Zone deinhibit [Seismic Zone]	
Zone deinhibit [All Okay Zone]	
Zone deinhibit [Holdup Fault Zone]	
Zone deinhibit [Warning Fault Zone]	
Zone deinhibit [Setting authorisation Zone]	
Zone deinhibit [Lock element Zone]	

Vanderbilt SPC event	Security Center event
Zone deinhibit [Glass Break Zone]	
Zone alarm [Tamper Zone]	Intrusion detection unit input tamper
Zone tamper [Alarm Zone]	
Zone tamper [Entry/Exit Zone]	
Zone tamper [Exit Term Zone]	
Zone tamper [Fire Zone]	
Zone tamper [Fire Exit Zone]	
Zone tamper [Line Zone]	
Zone tamper [Panic Zone]	
Zone tamper [Holdup Zone]	
Zone tamper [Tamper Zone]	
Zone tamper [Tech Zone]	
Zone tamper [Medical Zone]	
Zone tamper [Keyarm Zone]	
Zone tamper [Unused Zone]	
Zone tamper [Shunt Zone]	
Zone tamper [X-Shunt Zone]	
Zone tamper [Detector Fault Zone]	
Zone tamper [Lock Supervision Zone]	
Zone tamper [Seismic Zone]	
Zone tamper [All Okay Zone]	
Zone tamper [Holdup Fault Zone]	
Zone tamper [Warning Fault Zone]	
Zone tamper [Setting authorisation Zone]	
Zone tamper [Lock element Zone]	
Zone tamper [Glass Break Zone]	
Zone alarm [Line Zone]	Intrusion detection unit trouble

Vanderbilt SPC event	Security Center event
Zone alarm [Holdup Fault Zone]	
Zone alarm [Warning Fault Zone]	
Trouble [Alarm Zone]	
Trouble [Entry/Exit Zone]	
Trouble [Exit Term Zone]	
Trouble [Fire Zone]	
Trouble [Fire Exit Zone]	
Trouble [Line Zone]	
Trouble [Panic Zone]	
Trouble [Holdup Zone]	
Trouble [Tamper Zone]	
Trouble [Tech Zone]	
Trouble [Medical Zone]	
Trouble [Keyarm Zone]	
Trouble [Unused Zone]	
Trouble [Shunt Zone]	
Trouble [X-Shunt Zone]	
Trouble [Detector Fault Zone]	
Trouble [Lock Supervision Zone]	
Trouble [Seismic Zone]	
Trouble [All Okay Zone]	
Trouble [Holdup Fault Zone]	
Trouble [Warning Fault Zone]	
Trouble [Setting authorisation Zone]	
Trouble [Lock element Zone]	
Trouble [Glass Break Zone]	
Zone Low battery	

Vanderbilt SPC event	Security Center event
Burglary Alarm [Alarm Zone]	Input alarm activated
Burglary Alarm [Entry/Exit Zone]	
Burglary Alarm [Exit Term Zone]	
Burglary Alarm [Fire Exit Zone]	
Burglary Alarm [Seismic Zone]	
Burglary Alarm [Lock element Zone]	
Burglary Alarm [Glass Break Zone]	
Burglary Restoral [Alarm Zone]	Input alarm restored
Burglary Restoral [Entry/Exit Zone]	
Burglary Restoral [Exit Term Zone]	
Burglary Restoral [Fire Exit Zone]	
Burglary Restoral [Seismic Zone]	
Burglary Restoral [Lock element Zone]	
Burglary Restoral [Glass Break Zone]	
Zone input open or closed	Input state changed: Input active
Zone input open or closed	Input state changed: Input normal
Zone input shorted	Input state changed: Input trouble
Zone input disconnected	
Zone input PIR masked	
Zone input fault	
Zone input unstable	
Zone input out of bounds	

How Vanderbilt SPC events are displayed in the System status task

When monitoring the status of your SPC panels in the *System status* task, Vanderbilt SPC events are displayed in columns.

The following table lists how Vanderbilt SPC events are displayed in the *System status* task. For more information on the *System status* task, refer to the *Security Desk User Guide*.

Vanderbilt SPC event	Column
PSU Mains Fault	AC fail
PSU Fault Fault	
PSU Battery Fault	Battery fail
Cabinet Tamper Fault	Tampered
AUX 1 Tamper Fault	
AUX 2 Tamper Fault	
Bell Tamper Fault	
Antenna Tamper Fault	
XBUS Tamper Fault	
X-BUS Antenna Tamper Fault	

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These 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. 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 customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec™ TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec™ Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: Genetec™ Assurance Description and Genetec™ Advantage Description.

Additional resources

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

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on 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/support/training/training-calendar.

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).

Hardware product issues and defects

Please contact GTAC at https://gtap.genetec.com to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.