Integrating the DSC PowerSeries Neo panel with KT controllers using a DSC communicator 5.3x with type 2 encryption

This application note includes instructions on how to integrate a DSC PowerSeries Neo intrusion panel with KT-400 and KT-1 controllers using an IP connection, or with KT-1-M and KT-1-PCB controllers using an RS-232 connection or an IP connection. The DSC alarm communicator 5.3x can connect up to four KT-400 or KT-1 controllers.

Requirements

You require the following items to integrate the DSC PowerSeries Neo with KT controllers:

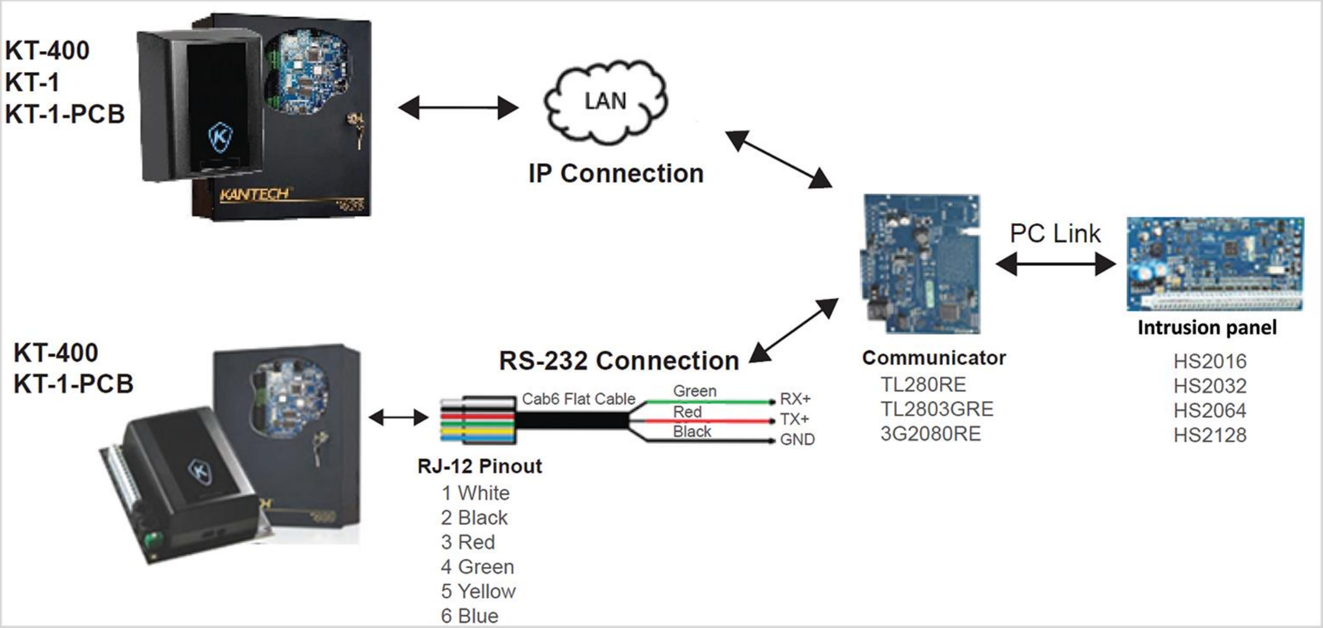
- **EntraPass Special, Corporate or Global Edition**: 7.50 or higher
- Use any of the following Kantech controllers:
  - **KT-400**: firmware 1.25 or higher
  - **KT-400 rev 1**: firmware 2.02 or higher
  - **KT-1-M or KT-1-PCB**: firmware 2.03 or higher
- Use the following DSC devices:
  - **PowerSeries Neo intrusion panel HS2016, HS2032, HS2064 or HS2128**: firmware 1.33 or higher
  - **Alarm communicator TL280(R)(E), TL2803GR(E) or 3G2080R(E)**: firmware 5.30 or higher
  - **PowerSeries keypad HS2LCD**: firmware 1.40 or higher

  To check the firmware of the DSC devices, see *Verifying the firmware of DSC devices*.

Connections diagram

Figure 1 shows the RS-232 and the IP connections between the controllers and an alarm communicator.

Figure 1: Connections diagram



Verifying the firmware of DSC devices

To verify the firmware of the DSC devices, complete the following steps:

1. On the HS2LCDN keypad, enter [*8] and then enter your four-digit installer code.
2. On the system-programming menu,
   - To verify the firmware of the intrusion panel, enter [900]-[100].
   - To verify the firmware of the alarm communicator, enter [900]-[460].
   - To verify the firmware of the keypad, enter [900]-[001].

Configuring the DSC PowerSeries Neo

To configure the DSC PowerSeries Neo intrusion panel, complete the following tasks:

1. *Activating the alarm communicator settings*
2. *Retrieving the integration identification number*
3. *Configuring the DSC PowerSeries Neo sessions*

You can connect up to four KT-400 or KT-1 controllers to a DSC TL280(R)(E) or TL2803GR(E) alarm communicator. To integrate the KT controllers with a DSC alarm communicator, choose one of the following options:

- One RS-232 connection and three IP connections.
- Four IP connections.

The DSC alarm communicators, 5.30 and higher, require different sessions for each RS-232 or IP connection. The 3G2080R(E) alarm communicator can have only one RS-232 session.

Activating the alarm communicator settings

To activate the DSC alarm communicator settings, complete the following steps:

1. On the HS2LCD keypad, enter [*8] and then enter your four-digit installer code.
2. On the system-programming menu, enter [382].
3. Under **Communicator Option 3**, turn on option **5**.

Retrieving the integration identification number

To retrieve the integration identification number, complete the following steps:

1. On the HS2LCD keypad, enter [*8] and then enter your four-digit installer code.
2. On the system-programming menu, enter [851]-[422].
3. Make a note of the integration identification number to enter in EntraPass. The first six digits only are visible. Use the arrow keys to see all twelve digits.

   For information on how to enter the integration identification number in EntraPass, see *Programming the integration in EntraPass*.

Configuring the DSC PowerSeries Neo sessions

To configure the sessions, use the HS2LCD keypad, and complete the steps in the following tables:

Note: To integrate one KT controller only, do not complete the steps to program sessions 2, 3, or 4.

Table 1: Session 1

Step		Input	Task
a. RS-232		[*8] – [installer code] – [851] – [425]	Ensure that only bits 1 and 5 are on.
b. IP		[*8] – [installer code] – [851] – [425]	Ensure that bits 3 and 5 are on.
		[*8] – [installer code] – [851] – [428]	Enter the panel KT-400 or KT-1 IP address.
	Port	[*8] – [installer code] – [851] – [429]	Take note of the outbound port (default 0x0C00 or 3072).
	UDP	[*8] – [installer code] – [851] – [426]	Ensure that bits 1, 3, and 4 are on.
	TCP	[*8] – [installer code] – [851] – [426]	Ensure that bit 3 is on.
c. Integration access code	Type 1 encryption	[*8] – [installer code] – [851] – [423]	Capture all 8 hex values. In EntraPass, enter the digits as the outgoing encryption key. The first four digits only are visible. Use the arrow keys to see the other digits.
	Type 2 encryption	[*8] – [installer code] – [851] – [700]	Capture all 32 hex values. In EntraPass, enter the digits as the integration access code lines 1 and 2. 16 digits only are visible in a row.
		[*8] – [installer code] – [851] – [425]	Ensure that bit 4 is on.

Table 2: Session 2

Step		Input	Task
a. IP		[*8] – [installer code] – [851] – [452]	Ensure that bits 3 and 5 are on.
		[*8] – [installer code] – [851] – [455]	Enter the panel KT-400 or KT-1 IP address.
	Port	[*8] – [installer code] – [851] – [456]	Take note of the outbound port (default 0x0C19 or 3097).
	UDP	[*8] – [installer code] – [851] – [453]	Ensure that bits 1, 3, and 4 are on.
	TCP	[*8] – [installer code] – [851] – [453]	Ensure that bit 3 is on.
b. Integration access code	Type 1 encryption	[*8] – [installer code] – [851] – [450]	Capture all 8 hex values. In EntraPass, enter the digits as the outgoing encryption key. The first four digits only are visible. Use the arrow keys to see the other digits.
	Type 2 Encryption	[*8] – [installer code] – [851] – [701]	Capture all 32 hex values. In EntraPass, enter the digits as the integration access code lines 1 and 2. 16 digits only are visible in a row.
		[*8] – [installer code] – [851] – [452]	Ensure that bit 4 is on.

Table 3: Session 3

Step		Input	Task
a. IP		[*8] – [installer code] – [851] – [479]	Ensure that bits 3 and 5 are on.
		[*8] – [installer code] – [851] – [482]	Enter the panel KT-400 or KT-1 IP address.
	Port	[*8] – [installer code] – [851] – [483]	Take note of the outbound port (default 0x0C1D or 3101).
	UDP	[*8] – [installer code] – [851] – [480]	Ensure that bits 1, 3, and 4 are on.
	TCP	[*8] – [installer code] – [851] – [480]	Ensure that bit 3 is on.
b. Integration access code	Type 1 encryption	[*8] – [installer code] – [851] – [477]	Capture all 8 hex values. In EntraPass, enter the digits as the outgoing encryption key. The first four digits only are visible. Use the arrow keys to see the other digits.
	Type 2 Encryption	[*8] – [installer code] – [851] – [702]	Capture all 32 hex values. In EntraPass, enter the digits as the integration access code lines 1 and 2. 16 digits only are visible in a row.
		[*8] – [installer code] – [851] – [479]	Ensure that bit 4 is on.

Table 4: Session 4

Step		Input	Task
a. IP		[*8] – [installer code] – [851] – [506]	Ensure that bits 3 and 5 are on.
		[*8] – [installer code] – [851] – [509]	Enter the panel KT-400 or KT-1 IP address.
	Port	[*8] – [installer code] – [851] – [510]	Take note of the outbound port (default 0x0C20 or 3104).
	UDP	[*8] – [installer code] – [851] – [507]	Ensure that bits 1, 3, and 4 are on.
	TCP	[*8] – [installer code] – [851] – [507]	Ensure that bit 3 is on.
b. Integration access code	Type 1 encryption	[*8] – [installer code] – [851] – [504]	Capture all 8 hex values. In EntraPass, enter the digits as the outgoing encryption key. **Note:** The first four digits only are visible. Use the arrow keys to see the other digits.
	Type 2 Encryption	[*8] – [installer code] – [851] – [703]	Capture all 32 hex values. In EntraPass, enter the digits as the integration access code lines 1 and 2. 16 digits only are visible in a row.
		[*8] – [installer code] – [851] – [506]	Ensure that bit 4 is on.

Note: After you program the DSC PowerSeries Neo, perform a power cycle on the communicator.

Programming the integration in EntraPass

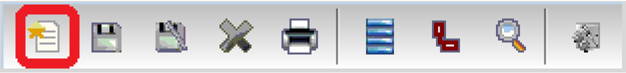
In EntraPass, program a new integration for every session. For example, if you connect four controllers to one DSC PowerSeries Neo panel, program the integration in EntraPass four times. For information on how to hide the intrusion panel duplicates that result from this process, see *Hiding panel duplicates in EntraPass*.

Note: The KT-400 and the KT-1 controllers must have static IP addresses to communicate over IP with the DSC PowerSeries Neo intrusion panel.

To program the integration in EntraPass, complete the following steps:

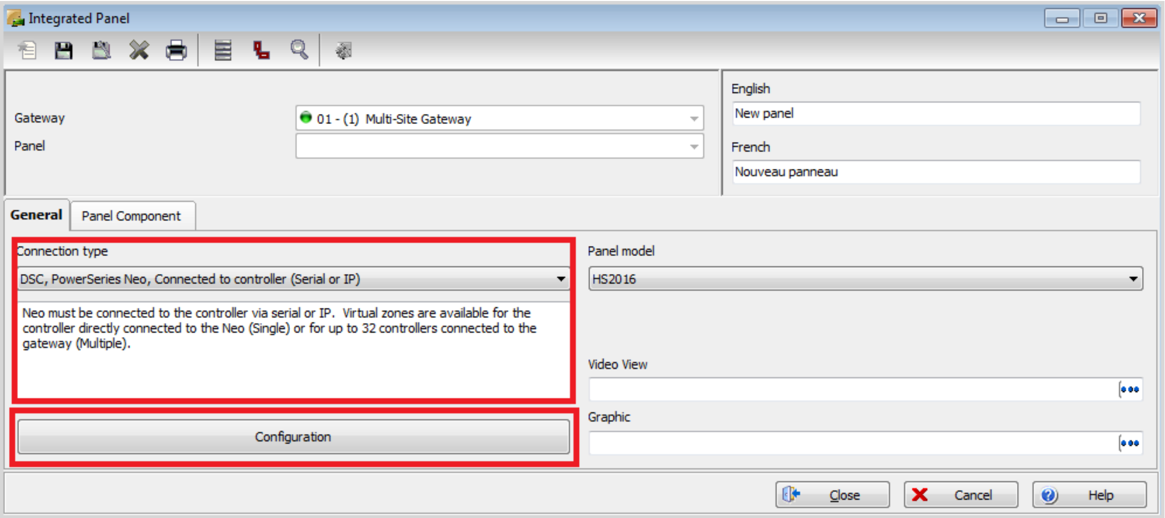
1. Log on to the EntraPass workstation.
2. On the **Devices** tab, click **Integrated Panel**.
3. In the **Integrated Panel** window, click the **New** icon, as Figure 2 shows.

Figure 2: New icon



4. In the **English** text box, enter an appropriate name for the panel.
5. On the **General** tab, from the **Connection type** list, select **DSC, PowerSeries Neo, Connected to controller (Serial or IP)**, as Figure 3 shows.

Figure 3: Integrated panel window



Gateway: 01 - (1) Multi-Site Gateway

Panel:

English: New panel

French: Nouveau panneau

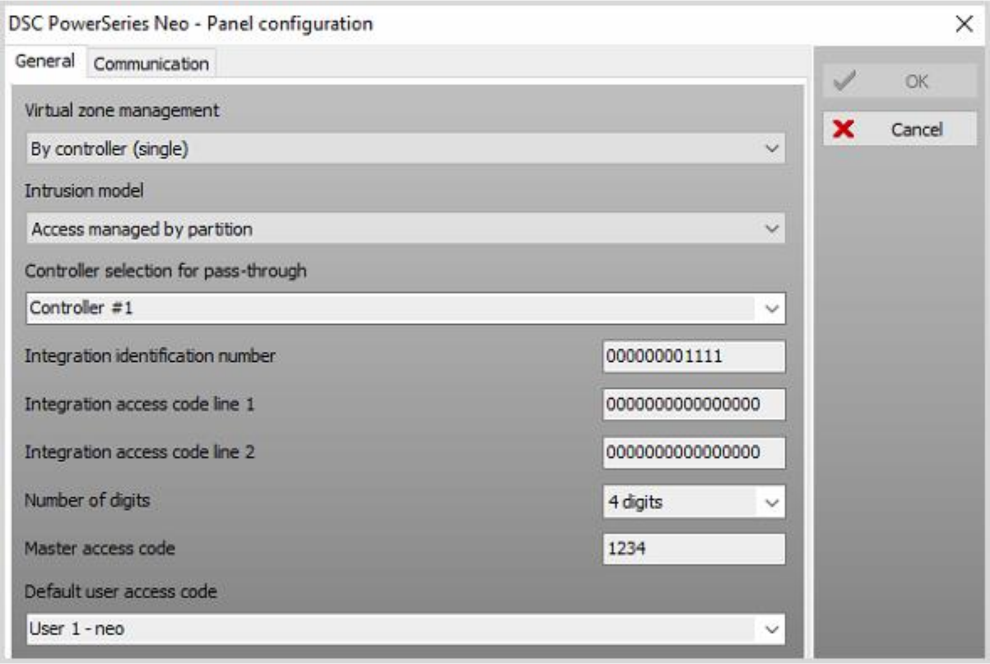
Connection type: DSC, PowerSeries Neo, Connected to controller (Serial or IP)

Neo must be connected to the controller via serial or IP. Virtual zones are available for the controller directly connected to the Neo (Single) or for up to 32 controllers connected to the gateway (Multiple).

Panel model: HS2016

6. From the **Panel model** list, select the correct panel model and encryption type.
7. Click **Configuration**.
8. In the **DSC PowerSeries Neo – Panel configuration** window, on the **General** tab, from the **Controller selection for pass-through** list, select the controller that is connected to the panel, as Figure 4 shows.
9. In the **Integration identification number** field, enter the integration identification number. For information on retrieving the integration identification number, see *Configuring the DSC PowerSeries Neo*.
10. In the **Integration access code line 1** and **line 2** fields, enter the integration access code. The GUI displays between 8 and 32 digits, depending on the encryption type. For information on retrieving the integration access code, see *Configuring the DSC PowerSeries Neo*.
11. In the **Master access code** field, enter the master access code. The default master access code for a DSC intrusion panel is 1234. Use the master access code to receive programming from the intrusion panel and to update the intrusion panel with new user codes.

Figure 4: Panel configuration window



Virtual zone management: By controller (single)

Intrusion model: Access managed by partition

Controller selection for pass-through: Controller #1

Integration identification number: 000000001111

Integration access code line 1: 0000000000000000

Integration access code line 2: 0000000000000000

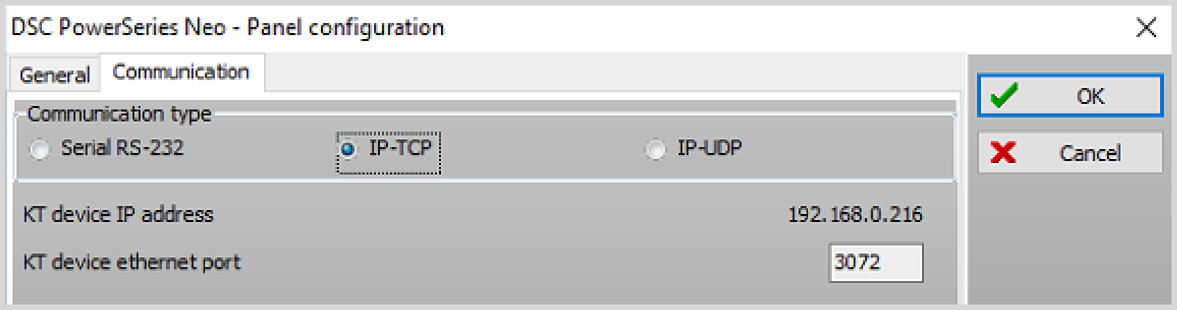
Number of digits: 4 digits

Master access code: 1234

Default user access code: User 1 - neo

12. On the **Communication** tab, in the **Communication type** area, click **Serial RS-232** or **IP-TCP**, as Figure 5 shows. If you use IP-TCP, make a note of the KT-400 or KT-1 controller IP address so that you can enter it when you configure the DSC PowerSeries Neo sessions. For more information, see *Configuring the DSC PowerSeries Neo*.

Figure 5: Panel communication tab



DSC PowerSeries Neo - Panel configuration

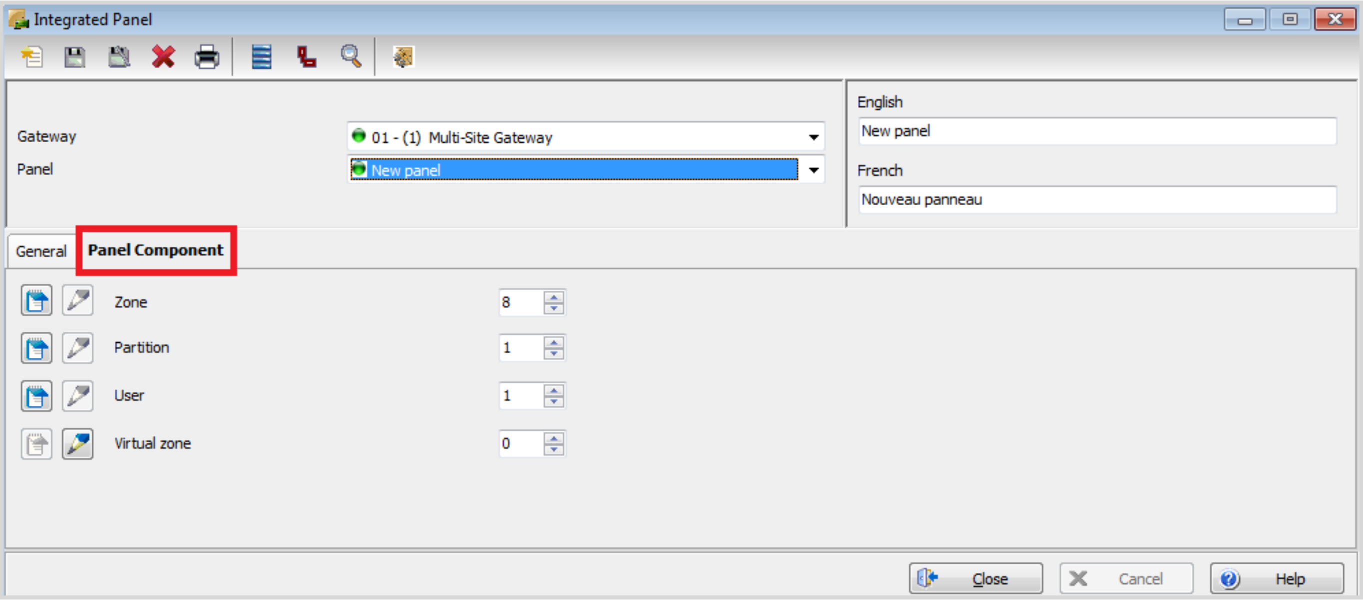
Communication type: ○ Serial RS-232 ● IP-TCP ○ IP-UDP

KT device IP address: 192.168.0.216

KT device ethernet port: 3072

13. Click **OK**.
14. In the **Integrated Panel** window, on the **Panel Component** tab, select the number of zones, partitions, and users to include in the integration, as Figure 6 shows.
15. Click the **Save** icon.
16. In the **DSC PowerSeries Neo – Panel configuration** window, on the **General** tab, from the **Default user access code** list, select the default user access code, as Figure 4 shows.
17. Click **OK**. The intrusion panel takes two to four minutes to upload, depending on the programming. During the upload, the intrusion panel is in programming mode.
18. **Optional**: To check if the upload completes, on the **Desktops** tab, click **Desktop 1**. In the **Messages list** window, look for the message **Panel components upload completed**.

Figure 6: Panel component tab



Integrated Panel

Gateway: 01 - (1) Multi-Site Gateway

Panel: New panel

English: New panel

French: Nouveau panneau

Zone: 8

Partition: 1

User: 1

Virtual zone: 0

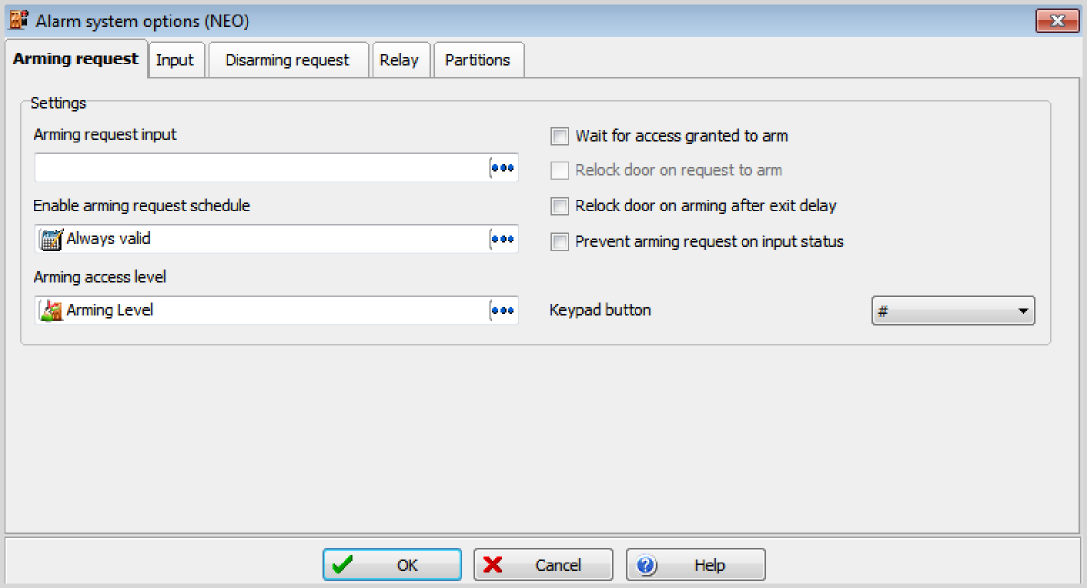
Arming and disarming a single partition using a reader

To arm a single partition using a reader, complete the following steps:

1. Log on to the EntraPass workstation.
2. On the **Devices** tab, click **Door**.
3. In the **Door** window, from the **Door** list, select the door that you want to use to arm and disarm the partition.

4. On the **Options and alarm system** tab, click **External alarm system options**.
5. In the **Alarm system options (NEO)** window, on the **Arming request** tab, from the **Enable arming request schedule** list, select when cardholders can arm the intrusion system, as Figure 7 shows.
6. From the **Arming access level** list, select a single access level or a group of access levels to determine which cardholders can arm the intrusion system.
7. On the **Disarming request** tab, from the **Postpone or disarm access level** list, select a single access level or a group of access levels to determine which cardholders can disarm the intrusion system, as Figure 8 shows.
8. On the **Partitions** tab, from the **Partition to arm** list, select the partition to associate with the door.
9. To disarm during an exit delay, select the **Authorize disarming during exit delay** check box.
10. Click **OK**.

Figure 7: Arming request tab



Settings

Arming request input:

Enable arming request schedule: Always valid

Arming access level: Arming Level

□ Wait for access granted to arm

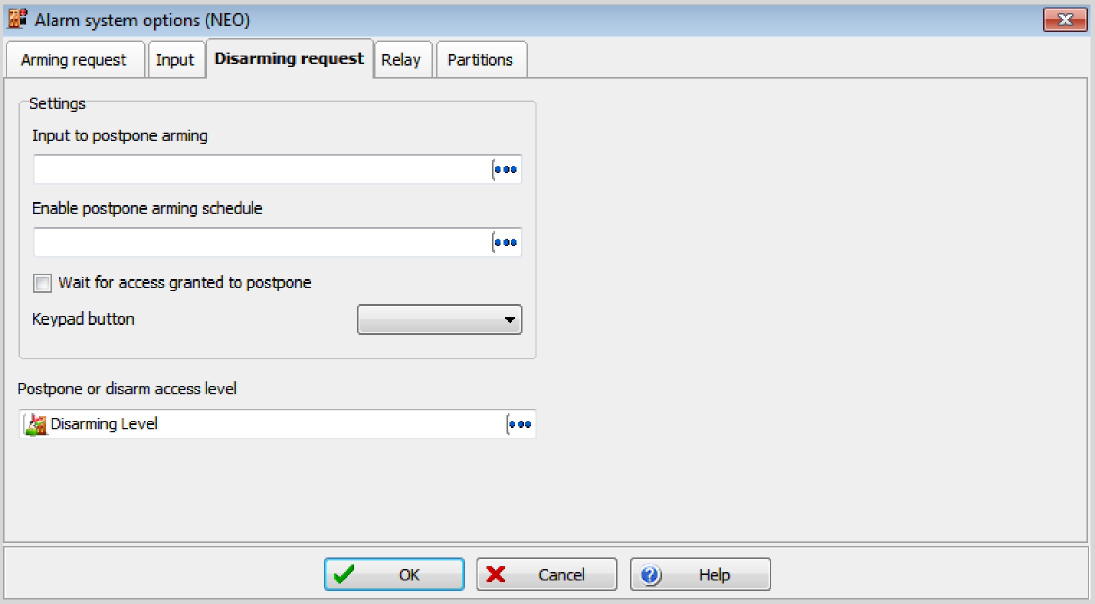
□ Relock door on request to arm

□ Relock door on arming after exit delay

□ Prevent arming request on input status

Keypad button: #

Figure 8: Disarming request tab



Settings

Input to postpone arming:

Enable postpone arming schedule:

□ Wait for access granted to postpone

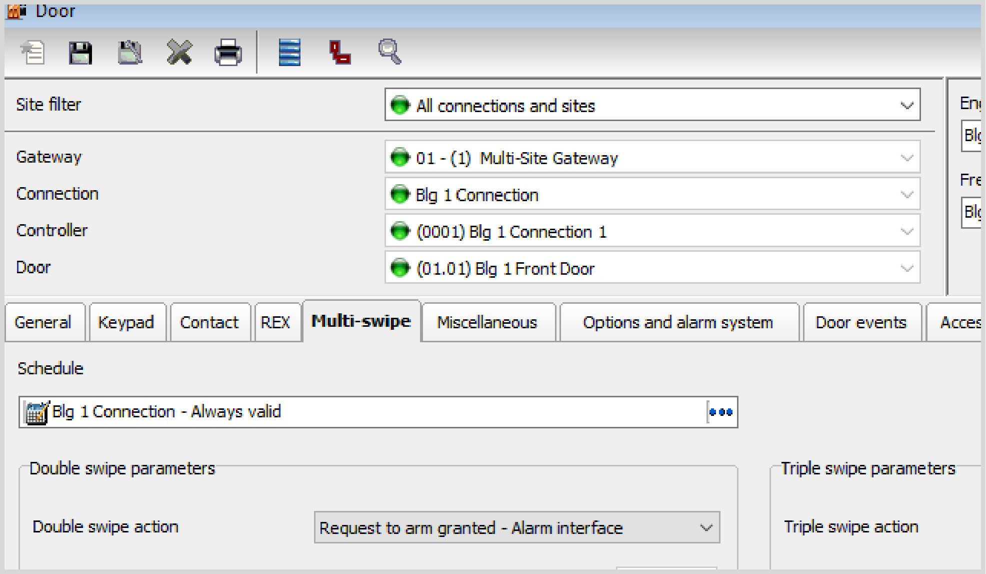
Keypad button:

Postpone or disarm access level: Disarming Level

11. In the **Door** window, on the **General** tab, select the **Enable Multi-swipe** check box. The **Multi-swipe** tab appears.

12. On the **Multi-swipe** tab, from the **Schedule** list, select **Always valid**, as Figure 9 shows.
13. From the **Double swipe action** list, select **Request to arm granted – Alarm interface**.
14. To save the door, click the **Save** icon.
15. On the EntraPass workstation, on the **Users** tab, click **Card**.
16. For each of the cardholders, on the **Miscellaneous** tab, select the **Allow Multi-Swipe (KT-400 and KT-1 Only)** check box, as Figure 10 shows.

Figure 9: Door configuration window



Site filter: All connections and sites

Gateway: 01 - (1) Multi-Site Gateway

Connection: Blg 1 Connection

Controller: (0001) Blg 1 Connection 1

Door: (01.01) Blg 1 Front Door

Schedule: Blg 1 Connection - Always valid

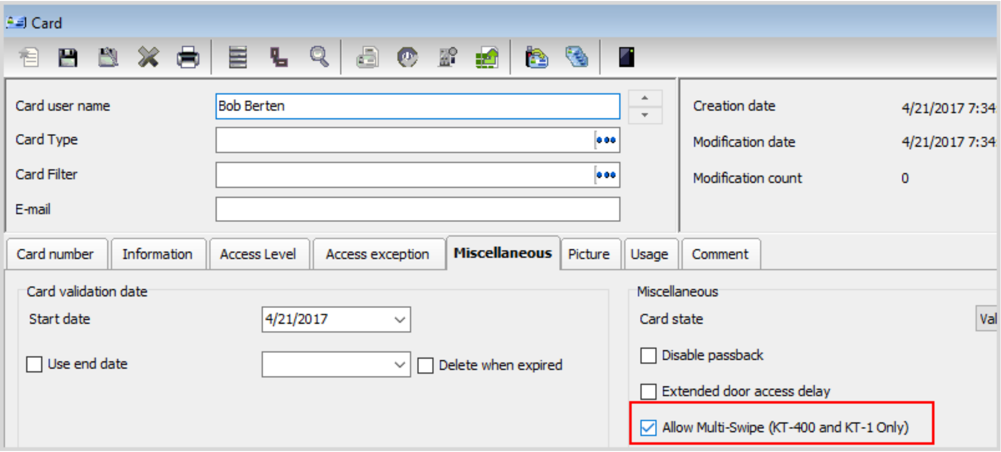
Double swipe parameters

Double swipe action: Request to arm granted - Alarm interface

Triple swipe parameters

Triple swipe action

Figure 10: Card configuration window



Card user name: Bob Berten

Card Type

Card Filter

E-mail

Creation date: 4/21/2017 7:34

Modification date: 4/21/2017 7:34

Modification count: 0

Card validation date

Start date: 4/21/2017

□ Use end date

□ Delete when expired

Miscellaneous

Card state: Val

□ Disable passback

□ Extended door access delay

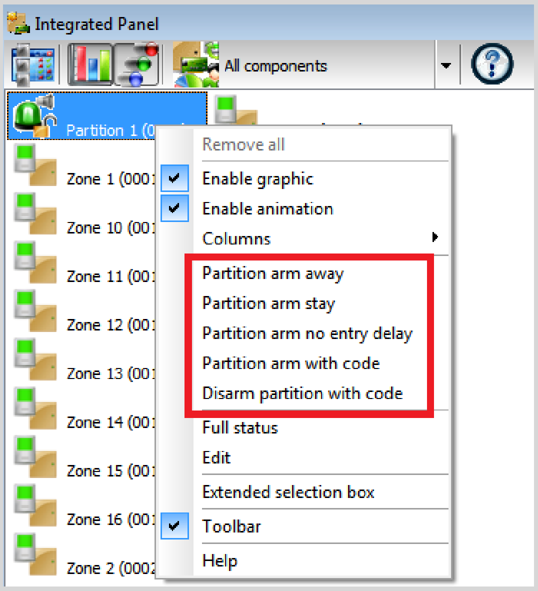
☑ Allow Multi-Swipe (KT-400 and KT-1 Only)

Arming and disarming partitions manually

To arm and disarm partitions manually, complete the following steps:

1. Log on to the EntraPass workstation.
2. On the **Operation** tab, click **Integrated Panel**.
3. In the left pane, select the correct intrusion panel.
4. Select the partition that you want to arm or disarm.
5. Right-click on the partition and select a task, as Figure 11 shows.

Figure 11: Arming and disarming partitions manually



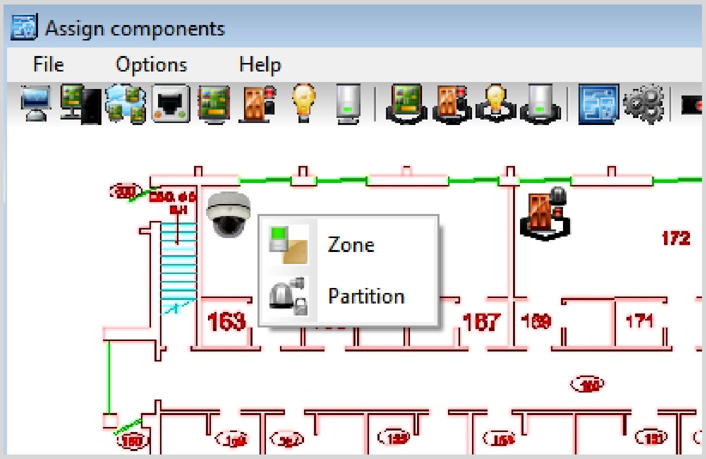
Adding components to the graphics setup

If you add a virtual keypad or an intrusion panel to the graphics setup, you can add zones and partitions to the graphic, you can arm and disarm partitions by setting default double-click functions on the graphic, and you can view the graphics on the graphic desktop.

To add a virtual keypad or an intrusion panel to the graphics setup, complete the following steps:

1. Log on to the EntraPass workstation.
2. On the **Definition** tab, click **Graphic**.
3. From the **Graphic** list, select the correct graphic, or to create a new graphic, click the **New** icon.
4. Click **Click here to create, edit or modify a graphic**.
5. From the **Icon** menu, drag the **Panel component** icon to the graphic map. When you release the **Panel component** icon, a list box appears.
6. From the list box, select **Keypad**.
7. Close the **Assign components** window.
8. Click the **Save** icon.

Figure 12: Assign components window



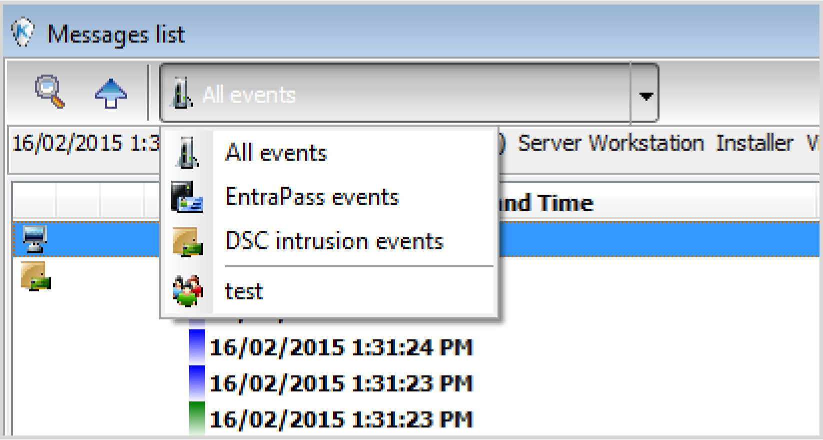
Viewing events and reports

Based on intrusion events, you can generate reports and video triggers, and set up real-time email notifications and alarm acknowledgements. You can search for different types of events by using the filter function, as Step 4 shows.

To view DSC intrusion events and reports, complete the following steps:

1. Log on to the EntraPass workstation.
2. On the **Desktops** tab, click **Desktop 1**.
3. In the **Messages list** window, view all the access and intrusion events.
4. To filter the view to see only DSC intrusion events, from the **All events** list, select **DSC intrusion events**, as Figure 13 shows.

Figure 13: Events and reports lists



Programming virtual zones on a single panel

You can assign up to 32 virtual zones to the DSC PowerSeries Neo intrusion panel. Using virtual zones, you can trigger alarm, trouble, or tamper events with the Kantech inputs, doors, or controllers. Using virtual zones, a Kantech door controller can cause events on a DSC PowerSeries Neo intrusion panel without any wiring, and the controller can transmit events to the monitoring central station.

To set up virtual zones, you need the following firmware:

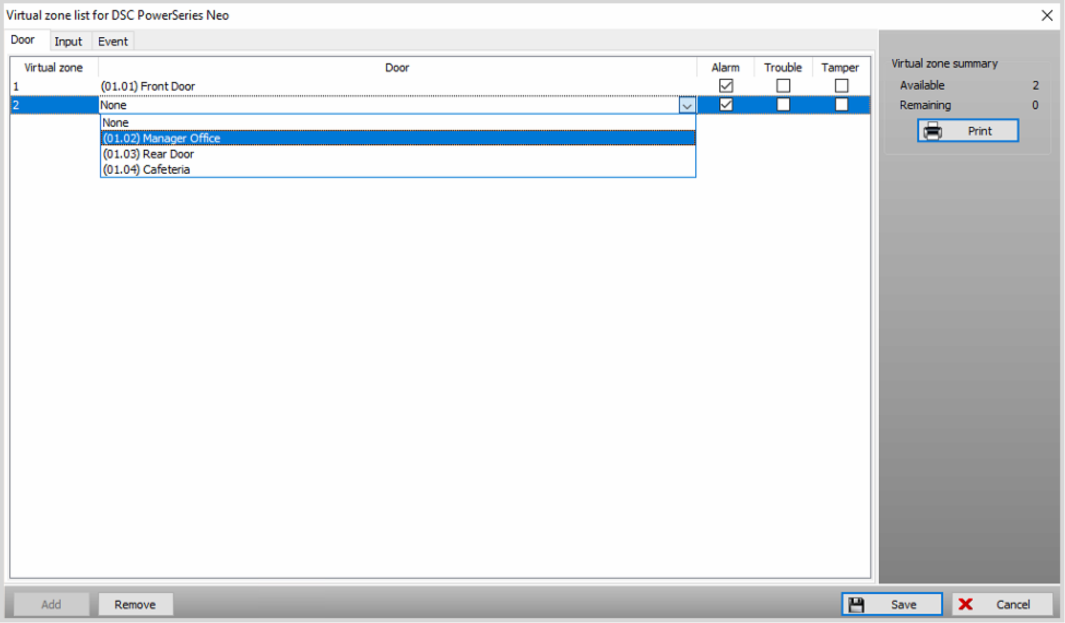
- **KT-400**: firmware 1.17 or higher
- **KT-400 rev1**: firmware 1.23 or higher
- **KT-1-M or KT-1-PCB:** firmware 1.03 or higher

To program a single panel as a virtual zone, complete the following steps:

1. To assign a DSC virtual zone to a DSC physical zone, complete the following steps:
   a. Using the HS2LCD keypad, enter [*8] and then enter your four-digit installer code.
   b. On the system-programming menu, enter [560].
   c. Scroll to the correct virtual zone and press [*].
   d. Select the correct physical zone to link to the virtual zone. For example, 009.
   e. Press [#].
2. Log on to the EntraPass workstation.
3. On the **Devices** tab, click **Integrated Panel**.
4. From the **Panel** list, select the intrusion panel that you programmed previously. For more information, see *Programming the integration in EntraPass*.
5. On the **General** tab, click **Configuration**.
6. From the **Virtual zone management** list, select **Managed by controller (single)**.

7. Click **OK**.
8. On the **Panel Component** tab, in the **Virtual zone** list, select the number of virtual zones that you have, as Figure 6 shows.
9. Click the **Save** icon.
10. In the **Virtual Zone** list area, click the **Pencil** icon.
11. In the **Virtual zone list for DSC PowerSeries Neo** window, click the **Door**, **Input** or **Event** tab, as Figure 14 shows.
12. To add virtual zones, click **Add**.
13. In the **Virtual zone** list, select the virtual zone that you want to work in.
14. From the **Door** list, select the correct component or event.
15. Click **Save**.
16. **Optional**: Repeat this process to configure all the virtual zones.

Figure 14: Virtual zone list window



Virtual zone	Door	Alarm	Trouble	Tamper
1	(01.01) Front Door	☑	□	□
2	None	☑	□	□

Virtual zone summary

Available	2
Remaining	0

Programming virtual zones on multiple panels

You can use the virtual zone-mapping window to program multiple panels as virtual zones. To link components from multiple controllers, the gateway supervises the events of all controllers, except the controller that uses the DSC PowerSeries Neo intrusion panel.

The virtual zone-mapping window populates with the appropriate devices.

When mapping components to a virtual zone, the system bases the list of components on the devices that are on the same gateway and that are on the same account that uses the DSC PowerSeries Neo intrusion panel. For example, the list of doors includes all doors that connect to controllers using the same gateway and all doors that connect to the DSC PowerSeries Neo intrusion panel.

The gateway monitors events from the other controllers and sends commands to the KT’s DLL to update the virtual zone. The gateway sends commands to the DSC PowerSeries Neo intrusion panel through a KT-1 or a KT-400 controller, which ensures that it can interact with all types of KT controllers on that gateway, even if they connect through an RS-485 bus.

Figure 15 shows the connections between the DSC PowerSeries Neo intrusion panel and the KT controllers.

Figure 15: Component connectivity

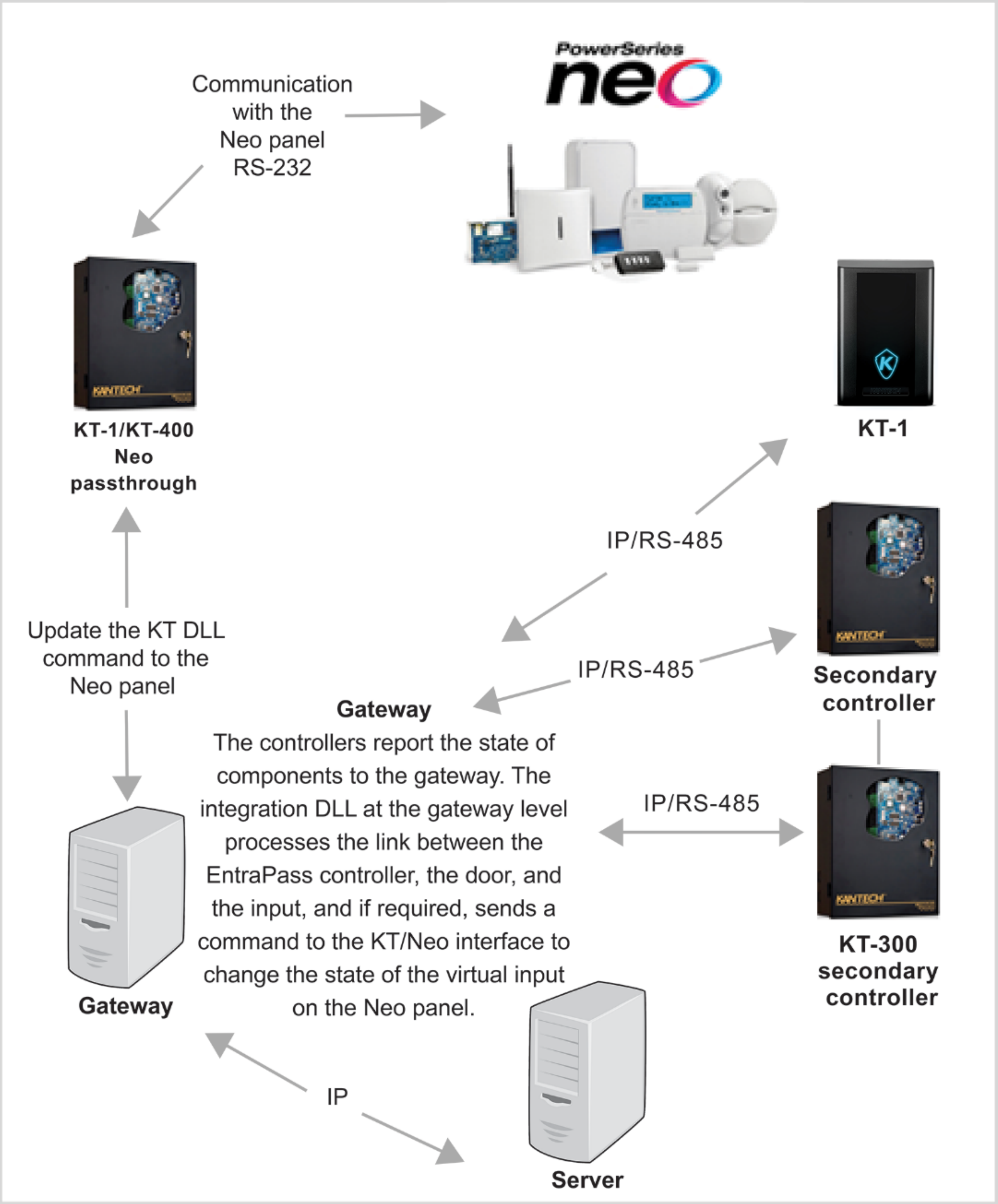

Communication
with the
Neo panel
RS-232
PowerSeries neo
KT-1/KT-400
Neo
passthrough
KT-1
IP/RS-485
Update the KT DLL
command to the
Neo panel
IP/RS-485
Secondary
controller
Gateway
The controllers report the state of components to the gateway. The integration DLL at the gateway level processes the link between the EntraPass controller, the door, and the input, and if required, sends a command to the KT/Neo interface to change the state of the virtual input on the Neo panel.
IP/RS-485
KT-300
secondary
controller
Gateway
IP
Server

Table 5: EntraPass events to DSC virtual zones status

EntraPass		**DSC PowerSeries Neo**		
	EntraPass events	**Report alarm**	**Report trouble**	**Report tamper**
Input	Input in alarm	X		
	Input in trouble (Double EOL only)		X	
	Input tamper in alarm (Double EOL only)			X
Door	Open/Close (door contact status)	X		
	Door forced open	X		
	Door alarm on relock	X		
	Door pre-alarm open too long	X		
	Door open too long	X	X	
	Door lock device failure		X	
Events				
Duress	Duress feature (timed reset)	X		
Controllers	Controller AC power failed/controller AC power restored		X	
Controllers	Tamper switch in alarm/tamper switch restored			X
Controllers	Controller auxiliary power failed/controller auxiliary power restored		X	
Controllers	Controller reader power failed/controller reader power restored		X	
Controllers	Controller battery power failed/controller battery power restored		X	
Controllers	Controller module communication failed/ controller module communication restored		X	
Controllers	Controller DC power failed/controller DC power restored		X	
Controllers	Controller lock power failed/controller lock power restored		X	
Controllers	Controller power trouble (KT-1)		X	
Door	Door forced open/door forced open restored	X		
Door	Door open too long/door open too long restored		X	
Door	Door lock device failed/door lock device failed restored		X	
Access Denied	Access denied – bad card status (timed reset)			X

General information

Arming and disarming requests

- To arm or disarm a partition by using a card, link the intrusion panel partition to a reader or readers. When a cardholder presents a card and presses the correct button on the reader, the KT controller sends an arming request to the intrusion panel. When a cardholder presents a card and opens the doors, the KT controller sends a disarming request to the intrusion panel. The EntraPass software supports single partition management for each reader.

- To make disarming requests, the default user code must be valid. To program the default user code, on the EntraPass workstation, on the **Devices** tab, click **Integrated Panel**, and set the default user code.
- You can force the card and the PIN to disarm only. After you disarm the card, you can use the card for regular access without a PIN.
- To disarm, you must wire a door contact back to the KT controller.

Uploading intrusion panel programming to EntraPass

- During the first upload only, upload the names of the partitions and the zones from the intrusion panel to EntraPass. Use the partitions and the zones for various actions, such as operator operations.
- During the first upload, upload the users' codes from the intrusion panel to EntraPass. After this, you can modify existing users' codes only in EntraPass. If you modify codes in the intrusion panel, the modifications do not upload to EntraPass.

Viewing intrusion panel events in EntraPass

- On the **Desktops** tab, in the **Messages list** window, you can view intrusion panel events. You can include these events in reports about standard access events. Use intrusion panel events to trigger video recordings, pop-up alarms, email notifications, and other actions.

Operating on partitions manually in EntraPass

- The operator can perform operations on partitions manually in EntraPass. The operator can perform operations such as partition arm away, partition arm stay, partition arm no entry delay, partition arm with code, and disarm with code.

Setting up intrusion components as graphics in EntraPass

- Use the uploaded zones and partitions as part of the graphic floor plan to visualize the location of each zone, partition, and traditional access control component. The operator can view the status of each component and perform operations on partitions.

Hiding panel duplicates in EntraPass

- On the **System** tab, click **Workspace** and hide the DSC intrusion panel duplicates.

Virtual zones

- If you use virtual zones and if you use multi-sessions with the controllers, plan your virtual zones accordingly. Each controller must have its own door contacts.
- A virtual zone follows the status of the door to which it is assigned. When a door triggers, the virtual zone activates, regardless of how the door triggers.

Virtual keypad

- This integration does not support the virtual keypad.

Contact telephone numbers: 1 450 444 2030. Toll free: 1 888 222 1560. www.kantech.com

D29010661R002