KANTECH™

APPLICATION NOTE

DN1913-1005

SETTING UP DSC INTEGRATION THROUGH A KT-400 CONTROLLER

The purpose of this application note is to configure the EntraPass system to integrate with the DSC PowerSeries [tm] intrusion panel.

With EntraPass Version 4.03, the intrusion panel may be connected directly to the KT-400. The integration will allow you to receive events from the intrusion panel, receive partition and zone names, program user codes, manual arming and disarming of partitions, and viewing a virtual keypad. Furthermore, with the KT-400 integration we can arm and disarm via a reader using cards.

Table of Contents:

Requirements:

- EntraPass Special Edition, Corporate Edition or EntraPass Global Edition (version 4.03 and above) installed
- If using EntraPass Global Edition, a Corporate gateway or Global Gateway with a dual gateway feature
- DSC PowerSeries [tm] alarm panel and an IT-100 module
- Door contact connected on KT-400
- Arming Input or reader/keypad
- RS-232 cable and 740-1047 adapter (p/n CBLK-IT100)
- KT-400 Firmware 1.02 and above

tyco

Hardware Setup:

To connect the IT-100 to the KT-400 and the DSC PowerSeries [tm] intrusion panel, follow the steps below: (For more information please refer to the DSC IT-100 manual)

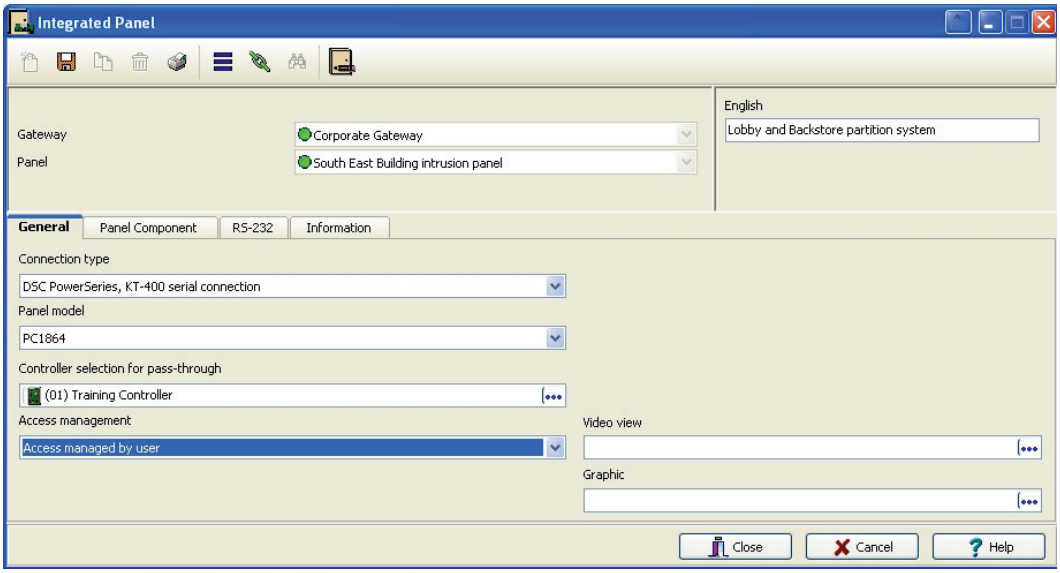
1) To wire the IT-100 to the alarm panel:
   a. Power down the alarm panel.
   b. Connect the IT-100 module using a 4-wire KEYBUS connection to the PowerSeries[tm] intrusion panel. Connect the RED, BLK, YEL and GRN terminals to the KEYBUS terminals of the PowerSeries[tm] intrusion panel.
   c. Power up the alarm panel.
2) To connect the IT-100 to the KT-400, refer to last page.

The IT-100 can be connected at a maximum distance of 98.4ft (30m) at 9600 baud rate from the KT-400.

EntraPass Setup:

1) Go to the **Devices** tab and select the **Integrated Panel** button.
   a. In the **Integrated Panel** tab, make sure the **View component hierarchy** button is pressed.
   b. Choose the gateway that the intrusion panel is connected to under the **Gateway** drop down list.
   c. Press on the **New** button and in the **English** text box, name the device accordingly.

   d. In the **Connection Type** drop down list, select **DSC PowerSeries, KT-400 Serial Connection**.
   e. In the **Panel model** drop down list, select the type of panel you have.
   f. In the **Controller selection for pass-through** select the KT-400 controller that is connected to the IT-100.
   g. In the **Access management** drop down list, select if the controller will manage a single partition (Access managed by partition) or multiple partitions (Access managed by user).



h. In the **Panel Component** tab, select the number of zones, partitions and users to be included in the intrusion panel.

i. In the **Information** tab, enter the master code in the **Master code** textbox.

NOTE: This code will be used for receiving the programming and updating the alarm panel with the new user codes. The default **Master code** in a DSC intrusion panel is 1234.

j. Check the **Use 6 digit pins** if the intrusion panel is using 6 digit pins.

k. Save the configuration.

NOTE: The uploading of the intrusion panel may take 2-3 minutes depending on the programming. During this time, the intrusion panel will be in programming mode. Once the intrusion panel uploading has been completed, an event called **Panel components upload completed** will occur on the message list.

2) Once the intrusion panel has finished uploading the information:

a. Select a user code under **Default user access code**. This user code will be used for all arming and disarming operations.

b. Save the configuration.

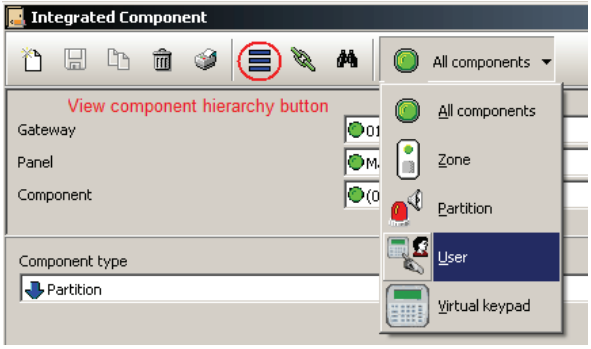
NOTE: if the user code does not have access to disarm a partition, the intrusion panel will not arm that partition even if it is requested by the operator.

Programming user codes:

1) To program new user codes or to modify existing ones, go to the **Devices** tab and select **Integrated Component.**

a. In the **Integrated component** tab, make sure the **View component hierarchy** button is pressed.

b. To better manage the components, click on the **All Components** button and select **Users.**



c. Select the Corporate gateway that the intrusion panel is connected to under the **Gateway** drop down list.

d. From the **Panel** drop down list, select the previously created intrusion panel.

e. From the **Component** drop down list, select a user and name the user accordingly.

f. In the **Default user access code,** enter the user code that will be used.

g. Save the configuration.

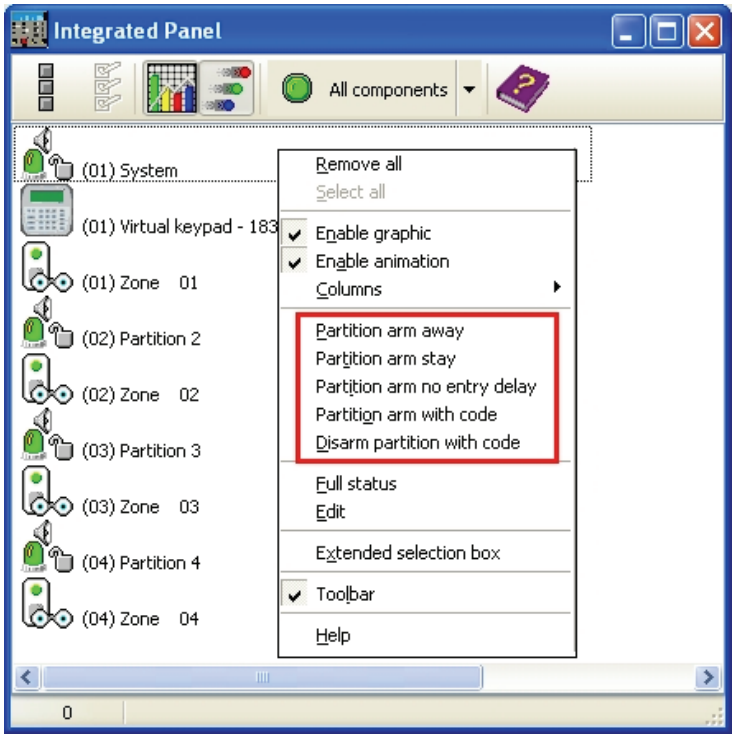
Note that there is an icon in the **Component type** list box. This icon represents the status of the component

	Component is waiting to be uploaded from the intrusion panel. This scenario only occurs during the first upload from the intrusion panel.
	Component is waiting to be downloaded to the intrusion panel. This icon occurs when an operator changes a user code.
	Component is ready to be used.

NOTE: The EntraPass system can only download information from the intrusion panel while it is disarmed. If the intrusion panel is armed, EntraPass will buffer the modification until the intrusion panel disarms.

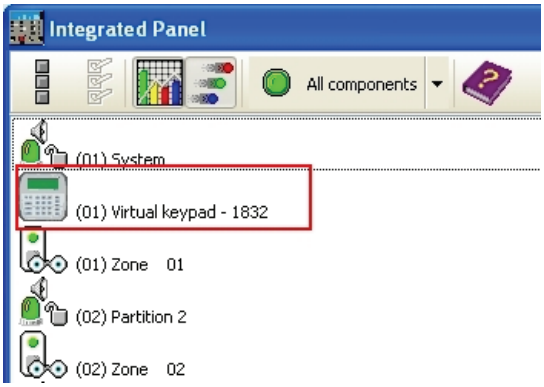
Arming and disarming via manual operations:

1) To request an arming or disarming of partitions, go to the **Operation** tab and select **Integrated component.**
   a. If shown, on the left pane select the proper intrusion panel.
   b. On the right pane, select the partition you wish to arm or disarm.
   c. Right click on the partition and select a task.

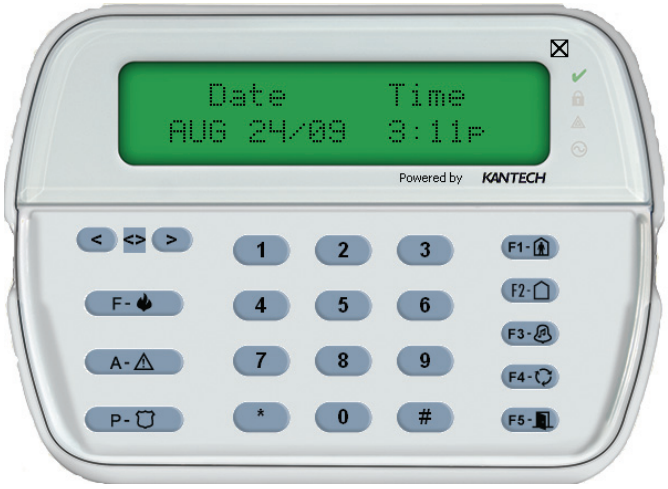


Viewing the virtual keypad:

1) To view and use the virtual keypad, go to the **Operation tab** and select the **Integrated Panel** button.
   a. If shown on the left pane, select the proper intrusion panel.



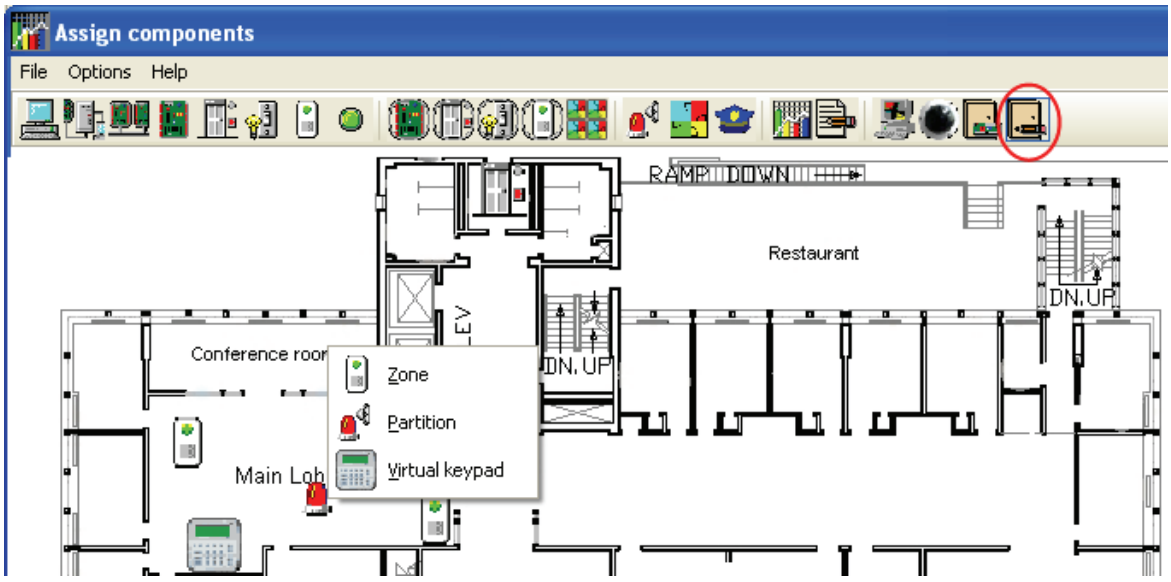
b. On the right pane, select the virtual keypad and right click on it.
c. Select virtual keypad.



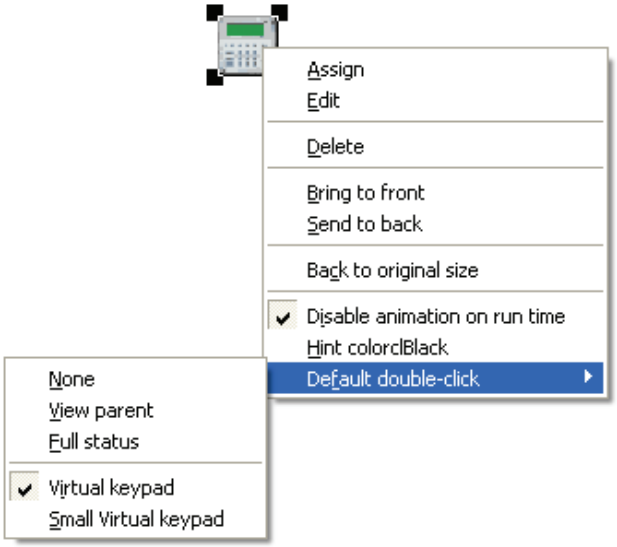
Using the mouse, you can click on any buttons on the Virtual Keypad as if you were using a standard keypad. You can also use the computer keyboard to simulate the button pressing.

Intrusion on Graphics:

1) To view a virtual keypad or intrusion components from a graphic, go to the **Definition** tab and select the **Graphic** button
   a. Create a new graphic or choose the appropriate graphic from the **Graphic** drop down list.
   b. Click on the **Click here to create, edit or modify a graphic** button.
   c. Drag and drop the **Panel component** icon on the graphic screen.
   d. Select the **Keypad** from the list box.



e. From the **Keypad** icon, right click and select **Default Double Click** as Virtual Keypad.



NOTE: You may also add zones and partitions on the graphic. You may arm and disarm partitions by setting default double click functions.

f. Close the window by clicking on the X at the top.

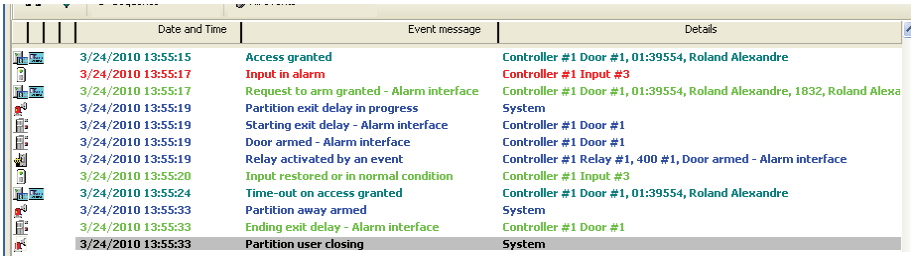
g. Save the graphic.

h. You may view a graphic from the graphic desktop.

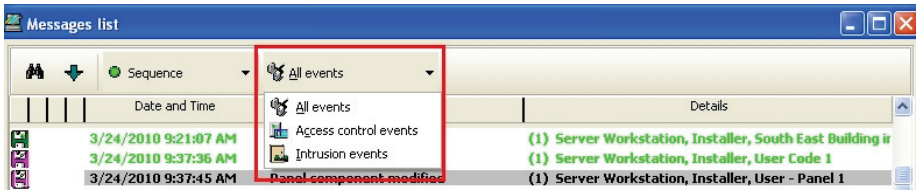
Viewing events and reports:

1) To view intrusion events, go to the **Desktop** tab and select **Desktop 1** Button.

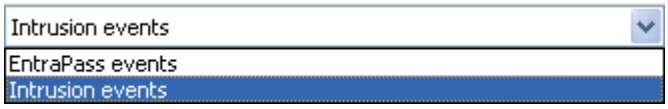
   a. From the **Message list,** you can view all the access and intrusion events.



   b. To view only access or intrusion events, click on the **All Events** button and select the proper event type.



2) You may generate reports, video trigger, real time email notifications and alarm acknowledgments based on intrusion events. You can better search for events by sorting by access control events or intrusion events in the above mentioned windows.



Single partition management (by partition) via a reader:

1) To arm a single partition via a reader, go to the **Devices** tab and click on the **Door** button.

   a. Make the appropriate Gateway, Site and Controller selections, and select the door used for arming/disarming the partition.

   b. Go to the **Options and alarm system** tab and click on **External alarm system options** button.

   c. In the **Alarm system options** window:

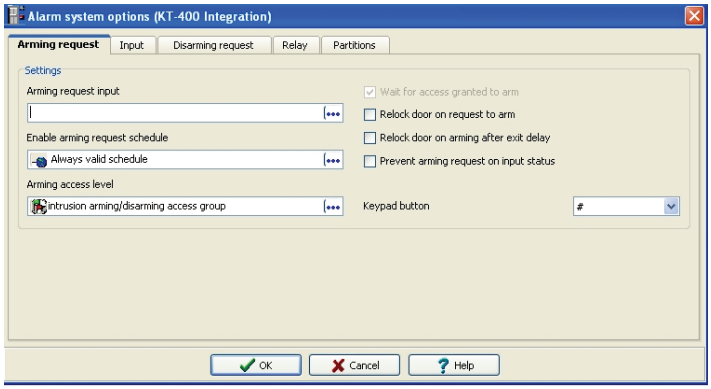
      i. For arming:

         1. If you are arming via card and pushing button, choose the appropriate input in the **Arming request Input**

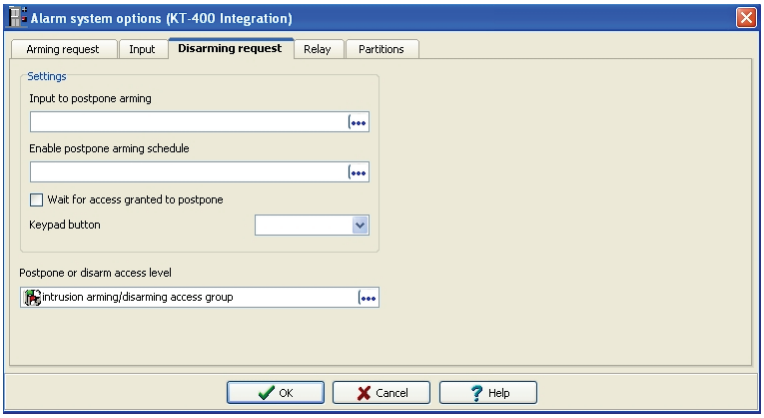
         2. If you are arming via card and keypad button, choose the appropriate button to be used as an arming request in the **keypad button** drop down list

      ii. Choose when cardholders will be able to arm the intrusion system by choosing a schedule in the **Enable Arming Request schedule** textbox.

      iii. Choose which card holder will be able to arm the intrusion system by choosing a single access level or group of access levels in the **Arming access level** textbox.

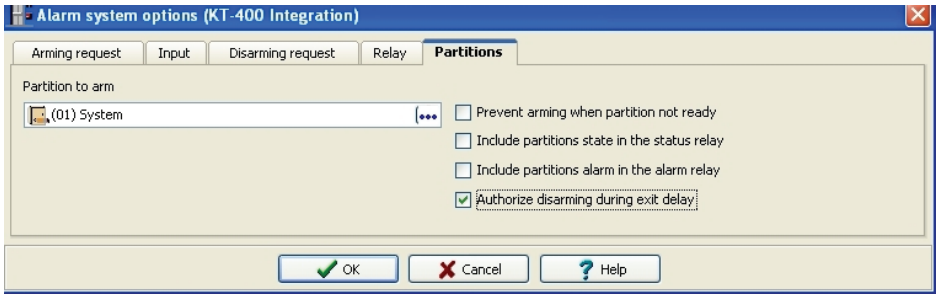


iv. Go to the **Disarming request** tab and choose which card holder will be able to disarm the intrusion system by choosing a single access level or group of access levels in **Postpone or disarm access level** textbox.



v. Go to the **Partitions** tab and under the **Partition to arm** textbox select the partition associated to this door.

vi. Check the **Authorize disarming during exit delay** if you want to be able to disarm during an exit delay.

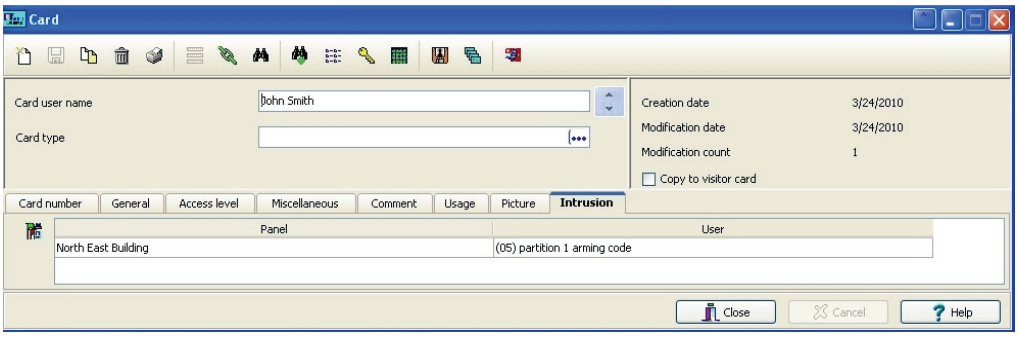


vii. Press **Ok** and save the door.

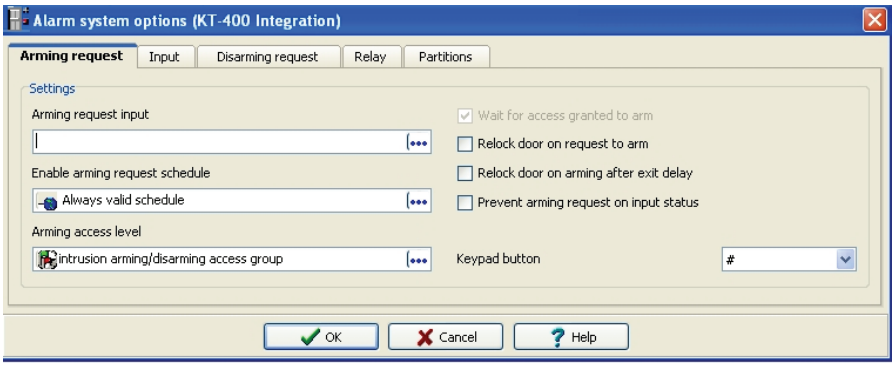
NOTE: The default user code programmed earlier in step 2.f is used as the user code for arming and disarming of the partitions.

Multiple partitions management (by user) via reader:

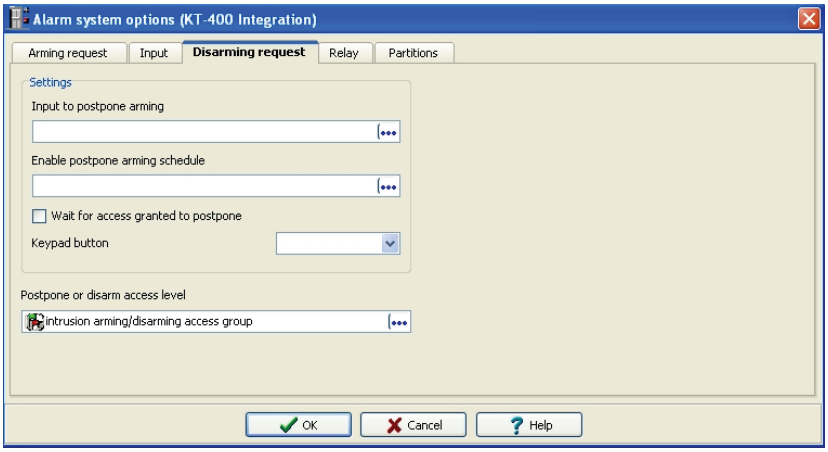
1) Go to the **Users** tab and click on the **Card** button.
   a. Select a card or create a new one.
   b. Go to the **Intrusion** tab and select a user code for the intrusion panel that will be associated to the card holder.
   c. Save the cardholder.



2) To arm multiple partitions via a reader, go to the **Devices** tab and click on the **Door** button.
   a. From the **Door** drop down list, select the door used for the arming.
   b. Go to the **Options and alarm system** tab and click on **External alarm system options** button.
   c. In the **External alarm system options** window:
      i. For arming:
         1. If you are arming via card and pushing button, choose the appropriate input in the **Arming request Input**
         2. If you are arming via card and keypad button, choose the appropriate button to be used as an arming request in the **keypad button** drop down list
      ii. Choose when then cardholders will be able to arm the intrusion system by choosing a schedule in the **Enable Arming Request schedule** textbox.
      iii. Choose which card holder will be able to arm the intrusion system by choosing a single access level or group of access levels in the **Arming access level** textbox.

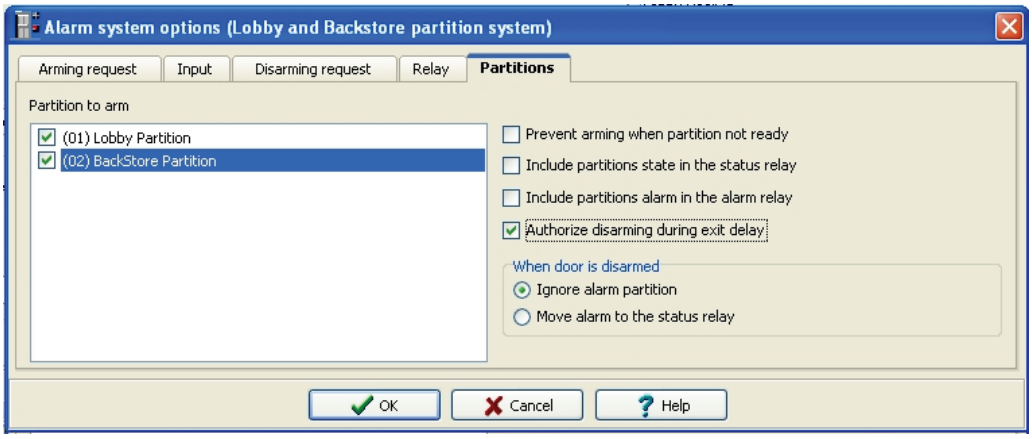


iv. Go to the **Disarming request** tab and choose which card holder will be able to disarm the intrusion system by choosing a single access level or group of access levels in **Postpone or disarm access level** textbox.



v. Go to the **Partitions** tab and select which partitions in the **Partition to arm** list box are associated to this door.

vi. Check the **Authorize disarming during exit delay** if you want to be able to disarm during an exit delay.



vii. Press **Ok** and save the door.

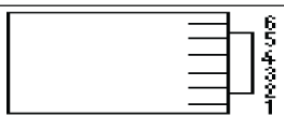
NOTE: With multiple partition management, a partition cannot be disarmed if another partition in that door is disarmed.

NOTE: The intrusion panel user code must have access to disarm partitions.

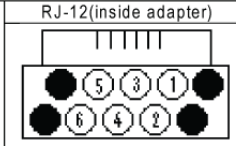
NOTE: To request the disarming of a partition, the cardholder must swipe the card at the reader and open the door.

IT-100 to KT-400

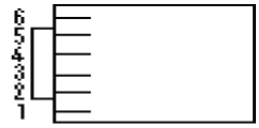
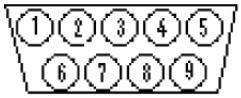
Option #1: RJ-12 Cable + 740-1047 adapter:

RJ-12 Male(clip down)(Fig.1)		RJ-12 Male(clip down)
		
1	To	6
2	To	5
3	To	4
4	To	3
5	To	2
6	To	1

740-1047 (Fig.2)

DB9-Male (outside adapter)		RJ-12(inside adapter)
		
2	To	3
3	To	4
5	To	2

Option #2: RJ-12 Male to DB9 Male Cable:

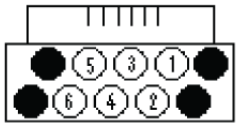
RJ-12 Male(clip down)		DB9-Male(outside adapter)
		
2	To	5
3	To	2
4	To	3

IT-100 to Corporate Gateway

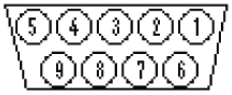
Option #1: RJ-12 Cable + 740-1047 & 740-1026 adapters:

Refer to Fig.1 for the RJ-12 cable and to Fig.2 for the 740-1047.

740-1026

DB9-Female(outside adapter)		RJ-12(inside adapter)
		
2	To	4
3	To	3
5	To	5

Option #2: Straight Serial Cable:

DB9-Female (outside adapter)		DB9-Male (outside adapter)
		
2	To	2
3	To	3
5	To	5