Integra Antipassback

RBH Access Technologies Inc.
2 Automatic Road, Suite 108
Brampton, Ontario
Canada L6S 6K8

Table of Contents

Abstract

This document explains three types of antipassback systems: local, timed, and global. Terminology is included to further help understand the basic concept of antipassback. A complete example of setting up each type of Integra system antipassback is shown.

1. Introduction

Antipassback is an access control feature that prevents cardholder misuse, by putting certain restrictions on the use of their cards. When the antipassback feature is enabled, cardholders must present their card for entry to and exit from all areas. Antipassback prevents a cardholder from using his/her card twice at the same access point.

It can be used to maximize security, prevent fraudulent use of cards, and maintain an accurate record of the number of people who are currently in any one area (possibly for safety reasons). Integra32™ access control systems support a variety of methods of implementing antipassback and this document describes the different types of antipassback and how they are used with Integra system.

2. Antipassback Concepts

With any antipassback system the concept of reader "disposition" is introduced. This simply means being able to identify whether a particular reader is an 'entry', 'exit', 'internal' or 'don't care' reader. When readers are designated as entry or exit, the system becomes able to record whether a user is inside or outside at any time by simply noting the last place their credential was used. If the last time it was used was at an 'exit' reader then the system knows that they are outside; if the last time it was used was at an 'entry' reader then the system knows that they are inside.

2.1 Reader APB

Selecting only an Entering Area will setup Reader APB. In Reader APB the Entering Area is compared to the cardholder's current location. If they match there is an APB violation.

2.2 Area APB

By adding an Exiting Area you setup Area APB. Area APB not only check that the area the cardholder is entering isn't the area they are in, but also verifies that the area they are exiting is the area they currently are in, providing a higher level of APB.

2.3 Timed Antipassback

Timed antipassback refers to a system where users are automatically forgiven after a certain period of time. For example, they might enter a car-park and then the system records that they are inside for the next 30 minutes which stops them from allowing their card to be used to let their friend into the car-park. After 30 minutes their antipassback status is set to 'unknown' again to allow them to re-enter. This eliminates the need for an exit reader which can reduce costs in some cases.

2.4 "Hard" Antipassback

Because readers are designated as entry/exit/don't care then the system knows whether users are inside or outside. Hard antipassback stops them from using their card to enter the premises if they are already inside, or exiting if they are already outside. Thus with hard antipassback implemented, users are unable to 'pass back' their credential to let their friend gain entry because once they have entered the system knows that they are inside and won't let them re-enter unless they first exit. Hard antipassback maintains a high level of security but can cause inconvenience as users who forget to use their card to enter or exit (by following someone else in for example) will have their status confused in the system – it will think that they are outside when they are actually inside, and so won't let them leave.

2.5 "Soft" Antipassback

With soft antipassback the system records the status of each user, thus knowing whether they are inside or outside at any stage, but doesn't "enforce" the status. Thus if they are inside and attempt to re-enter the system will grant them access. This increases convenience; the system still knows whether users are inside or outside based on their last reader used but may be less accurate because it hasn't enforced that users must enter before exiting and vice versa. It also therefore reduces security; the system knows where a person is but doesn't stop them from entering twice. This type of system is often used with time and attendance applications.

2.6 Forgiving a User

Users can have three possible states with an antipassback system – inside, outside or unknown. "Forgiving" a user simply means setting their antipassback status back to 'unknown' so that the next time they attempt to enter or exit they will be granted access.

2.7 Tailgating

Tailgating refers to a user following another user through a door or boom-gate without presenting a credential. They follow closely enough that they can get through the door or gate before it closes. Only the first user is recorded as being inside or outside.

2.8 Pass-Back Violation

A pass-back violation simply refers to a user attempting to gain access when their antipassback status is incorrect i.e. they are attempting to enter when the system records that they are already inside, or exit when the system records that they are already outside.

2.9 Global Antipassback

Within each Integra controller in the network the antipassback status of each user is recorded (they are either IN or they are OUT). In global antipassback the Integra software takes charge and tracks the users. Access granted messages are sent from the panels and the software. The software then determines if the cardholder should be allowed in the access point. If allowed the software will send a command to the panel to grant access. For global antipassback to work the Integra32™ Server must be running.

2.10 Muster Report

A muster report is simply a report of users indicating where their antipassback status is recorded. Muster reports are often used in situations where it is required to know who is inside at any given time in the event of an emergency. The muster report becomes an 'evacuation list'

3. Integra32™ and Antipassback

Integra32™ software support Local and Global, and Timed antipassback.

3.1 Local Antipassback

3.1.1 Local Antipassback with Two Doors and Two Readers

Setup local APB between two Areas: IN and OUT as shown in Figure 1.

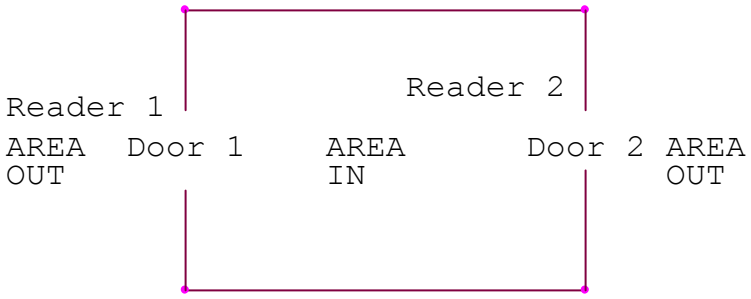


Figure 1: Local Antipassback – Two Doors

In Figure 1, there are two areas: IN and OUT. Door 1 is controlled by Reader 1 on side A of the panel and Door 2 is controlled by Reader 2 on side B of the panel.

Hardware Setup

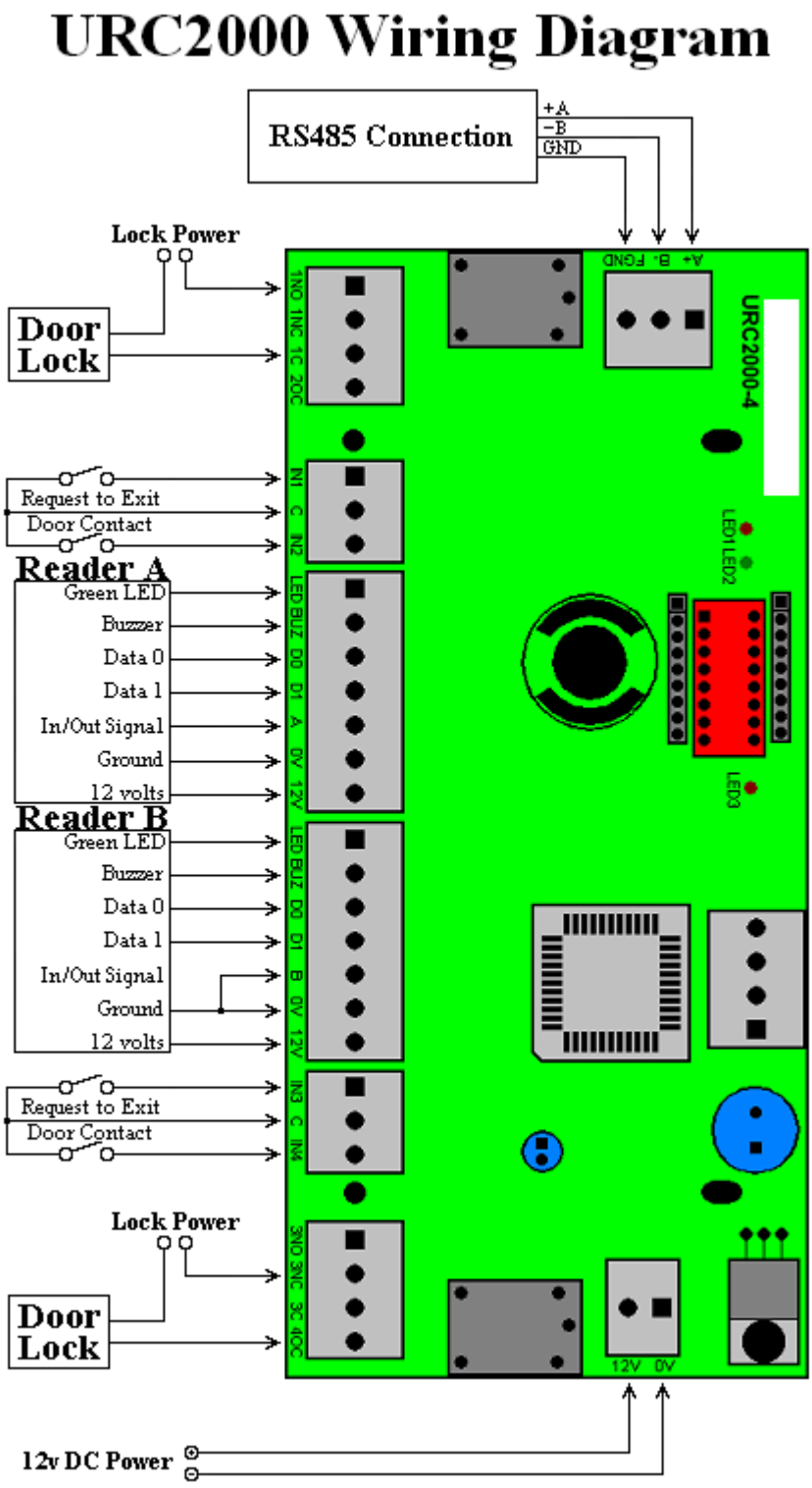


Figure 2: Connect Reader B In/Out Signal to Ground

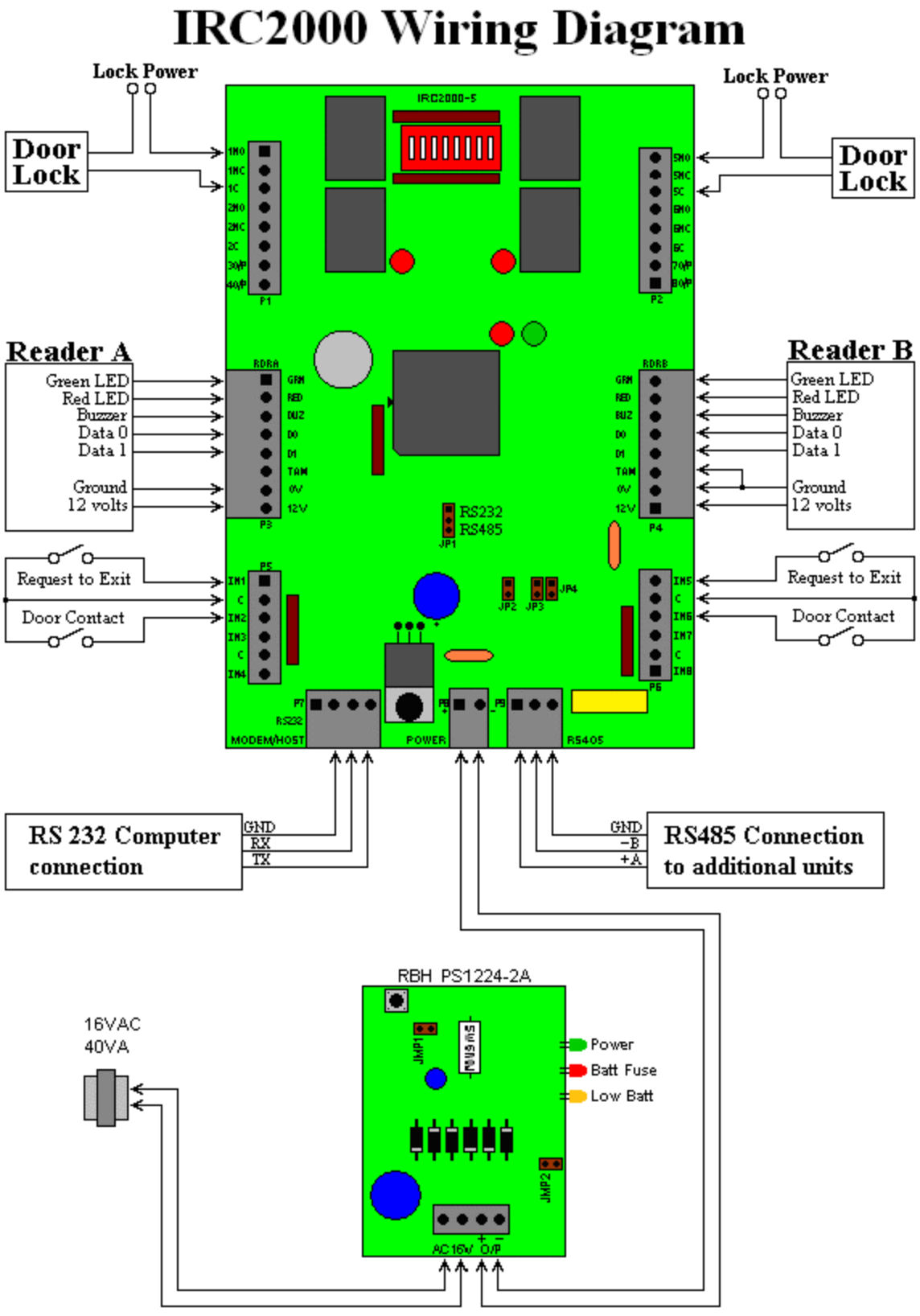


Figure 3: Connect Reader B Terminal TAM to Ground

Software Setup

Step 1

Create two areas: Area IN and Area OUT.

In the *Configure Window* right click on *Area* and select *Add Area*. Create two new areas. (Figure 4)

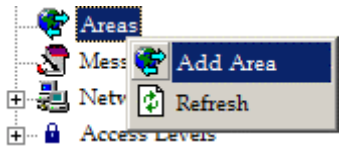


Figure 4: Create Two New Areas

Right click on *New Area* and select *Properties* as shown in Figure 5.

Figure 5: Open Properties Window

The *Area Properties* dialog box will pop up. (Figure 6)

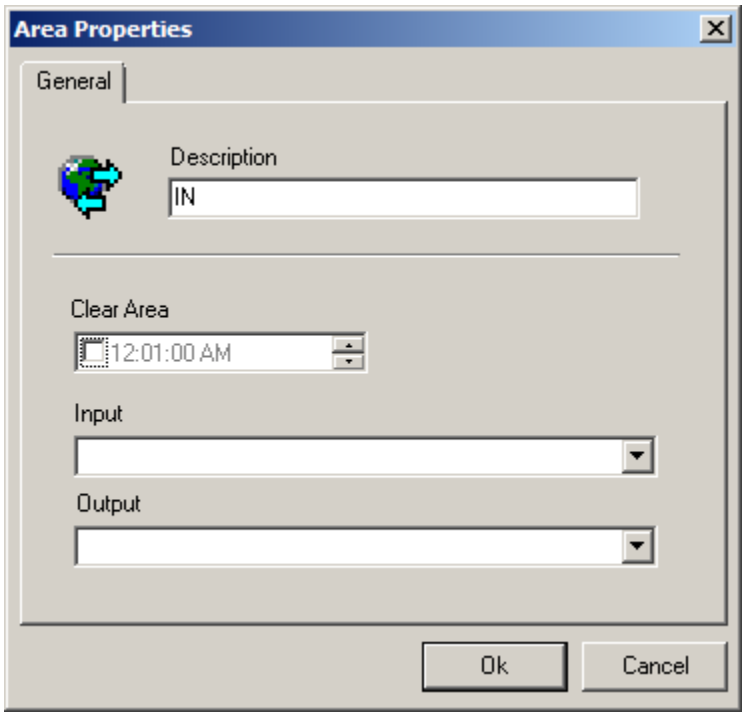


Figure 6: Area Properties Window

Enter Area name 'IN' in the Description textbox. Click OK button. Do the same for the other area naming it 'OUT'.

Step 2

Setup APB for readers.

Reader A APB Settings:

In *Configure Window*, right click on Reader 1 and select properties. (Figure 7)

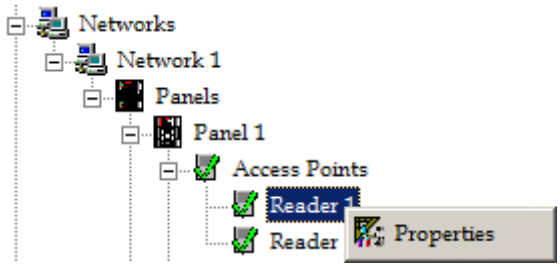


Figure 7: Opening Reader Properties

Reader 1 *Properties* dialog box will pop up. (Figure 8)

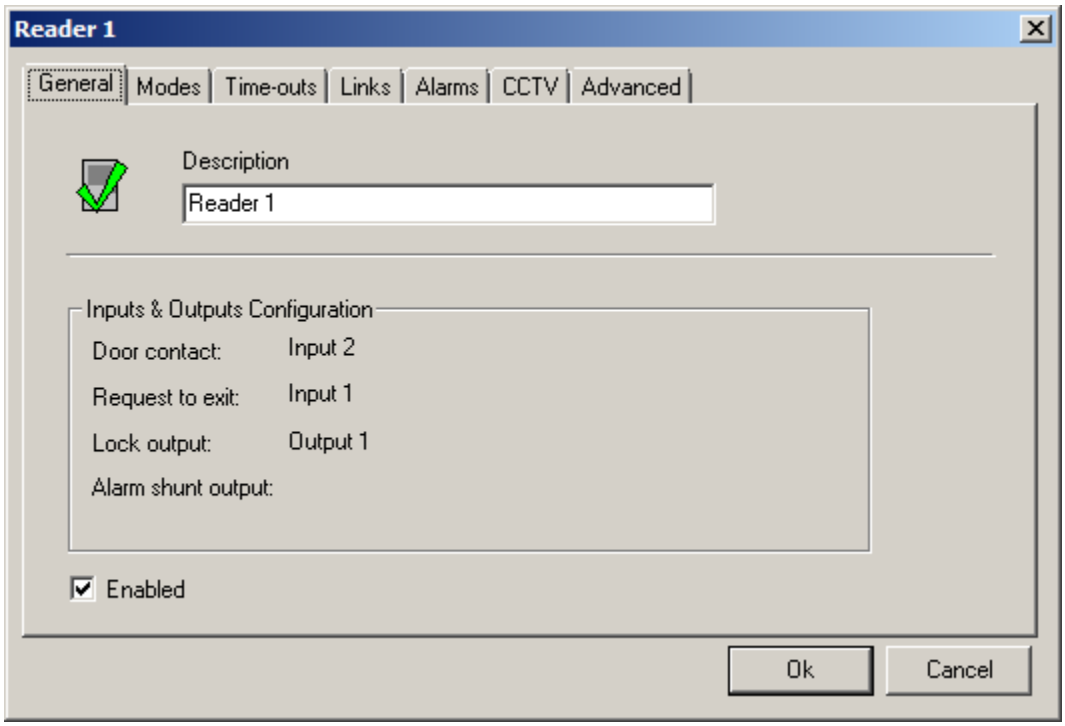


Figure 8: Reader 1 Properties Window

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 9.

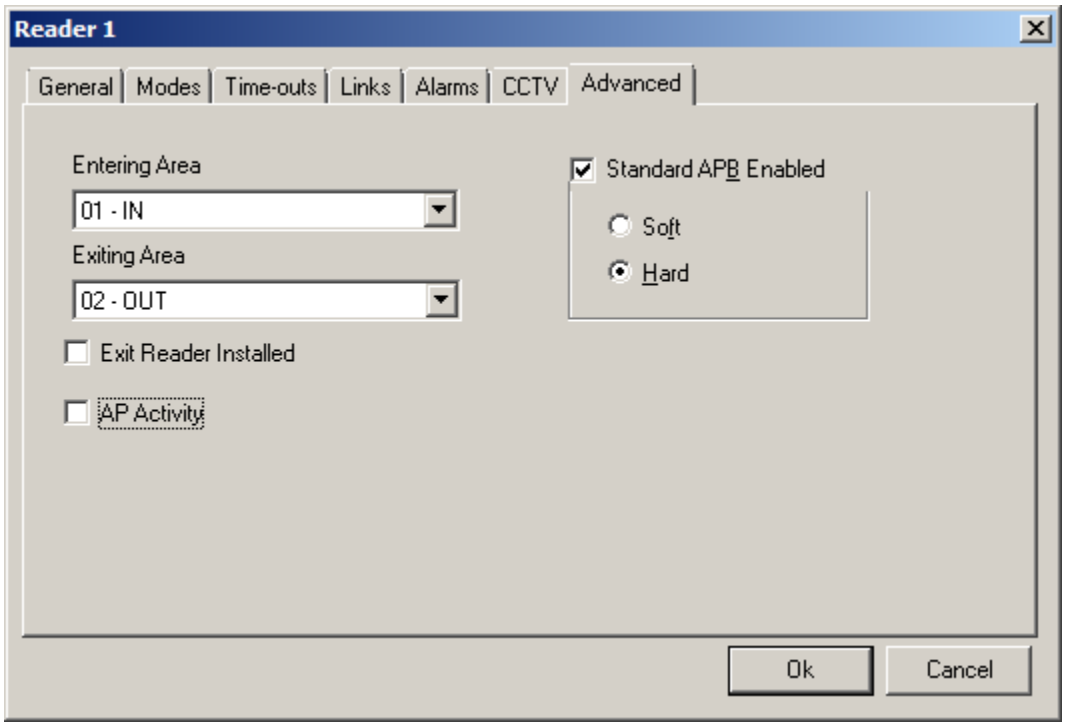


Figure 9: Selecting APB Properties on Reader 1

Select *Entering Area* IN and *Exiting Area* OUT.

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Reader B APB Settings:

In *Configure Window*, right click on Reader 2 and select properties. Reader 2 *Properties* dialog box will pop up.

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 10.

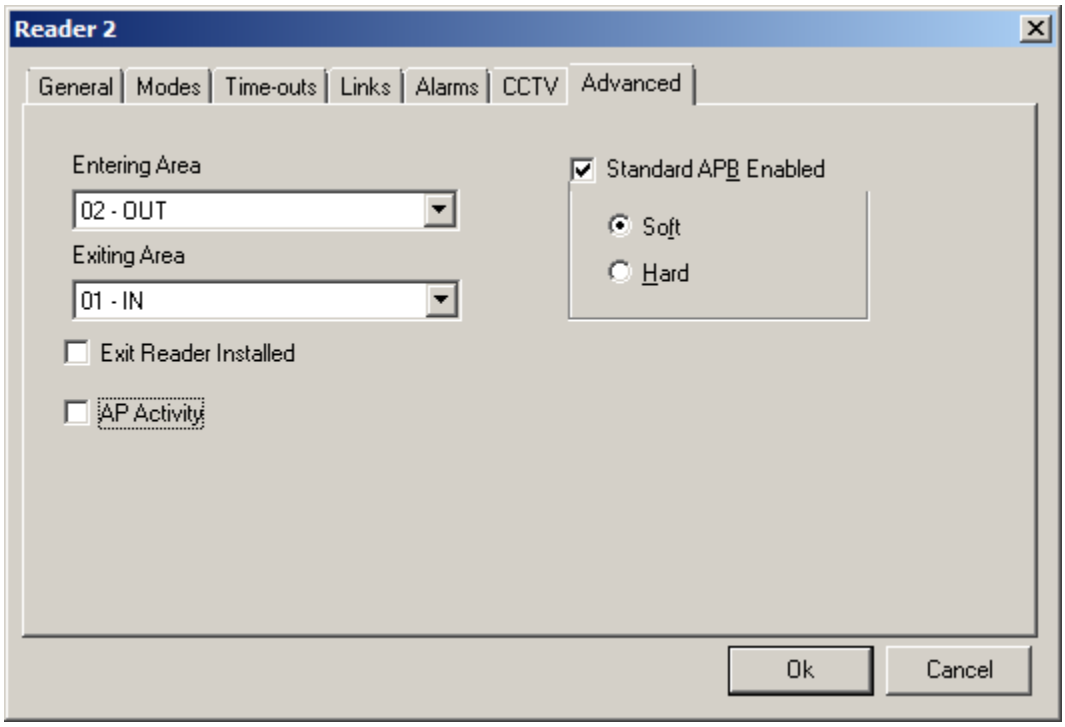


Figure 10: Selecting APB Properties on Reader 2

Select *Entering Area* OUT and *Exiting Area* IN

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Step 3

In the *Device Status* window, right click on Panel 1, and select *Download* ▸ *All Files*. (Figure 11)

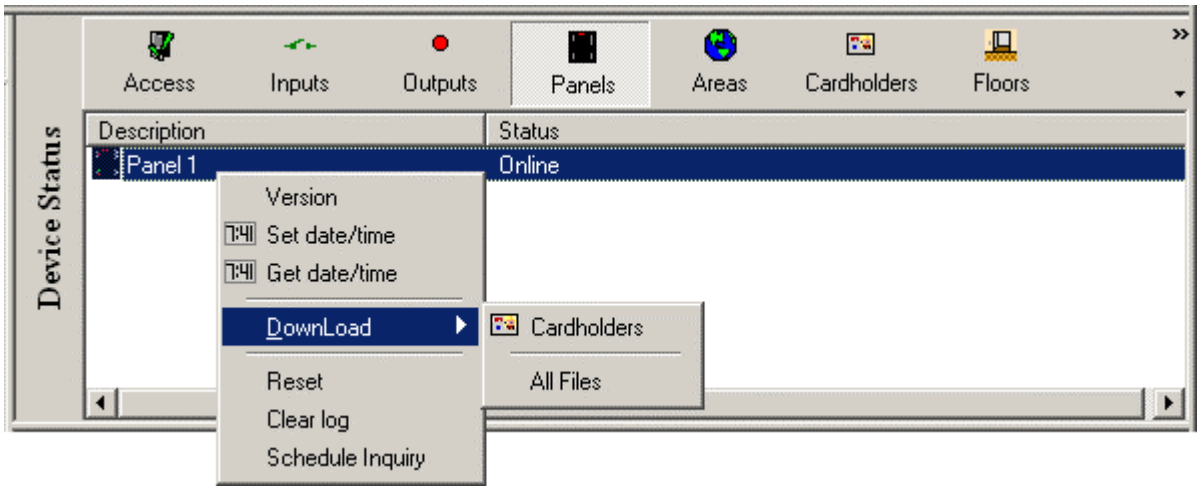


Figure 11: Download Database Files to the Panel

Test Procedure

1. Present card on Panel 1 Reader 1.
2. Present card on Panel 1 Reader 2.
3. Present card on Panel 1 Reader 2 again.
4. Present card on Panel 1 Reader 1.
5. Present card on Panel 1 Reader 1 again.

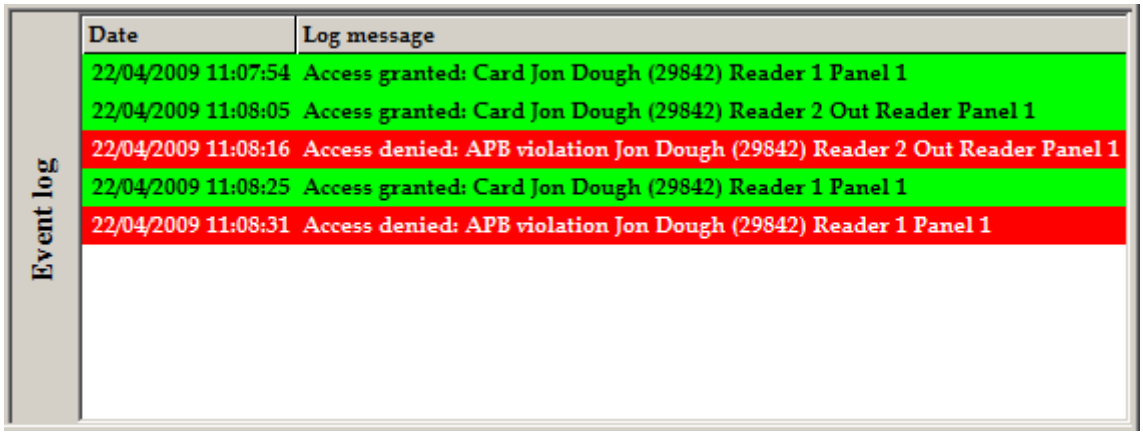


Figure 12: Local Antipassback Test

Discussion

1. Access is granted on Reader 1 and the appropriate message will be posted on the *Event Log* screen.
2. Access is granted on Reader 2 and the appropriate message will be posted on the *Event Log* screen.
3. Since the user presented their card on Reader 2 again, access will be denied and an APB violation message for Reader 2 will appear on the *Event Log* screen.
4. Access is granted on Reader 1 and the appropriate message will be posted on the *Event Log* screen.
5. Since the user presented their card on Reader 1 again, access will be denied and an APB violation message for Reader 1 will appear on the *Event Log* screen.

3.1.2 Local Antipassback with One Door and Two Readers

Setup local APB between two areas: IN and OUT, using two readers on one panel.

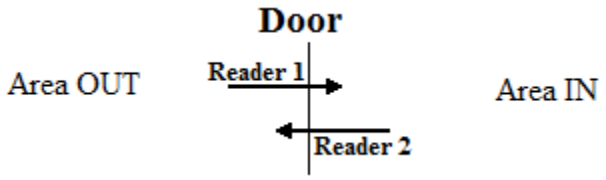


Figure 13: Local Antipassback Setup on Single Door

In Figure 13, there are two areas: IN and OUT, which are separated with a door. The door is controlled by two readers (Reader 1 on side A and Reader 2 on side B) on the same panel.

The side B reader in essence becomes an elaborate request-to-exit device for the A side.

- ✓ **Except for the lock output the side B inputs and outputs can be set to general purpose because they won't be needed by the access point.**

Hardware Setup

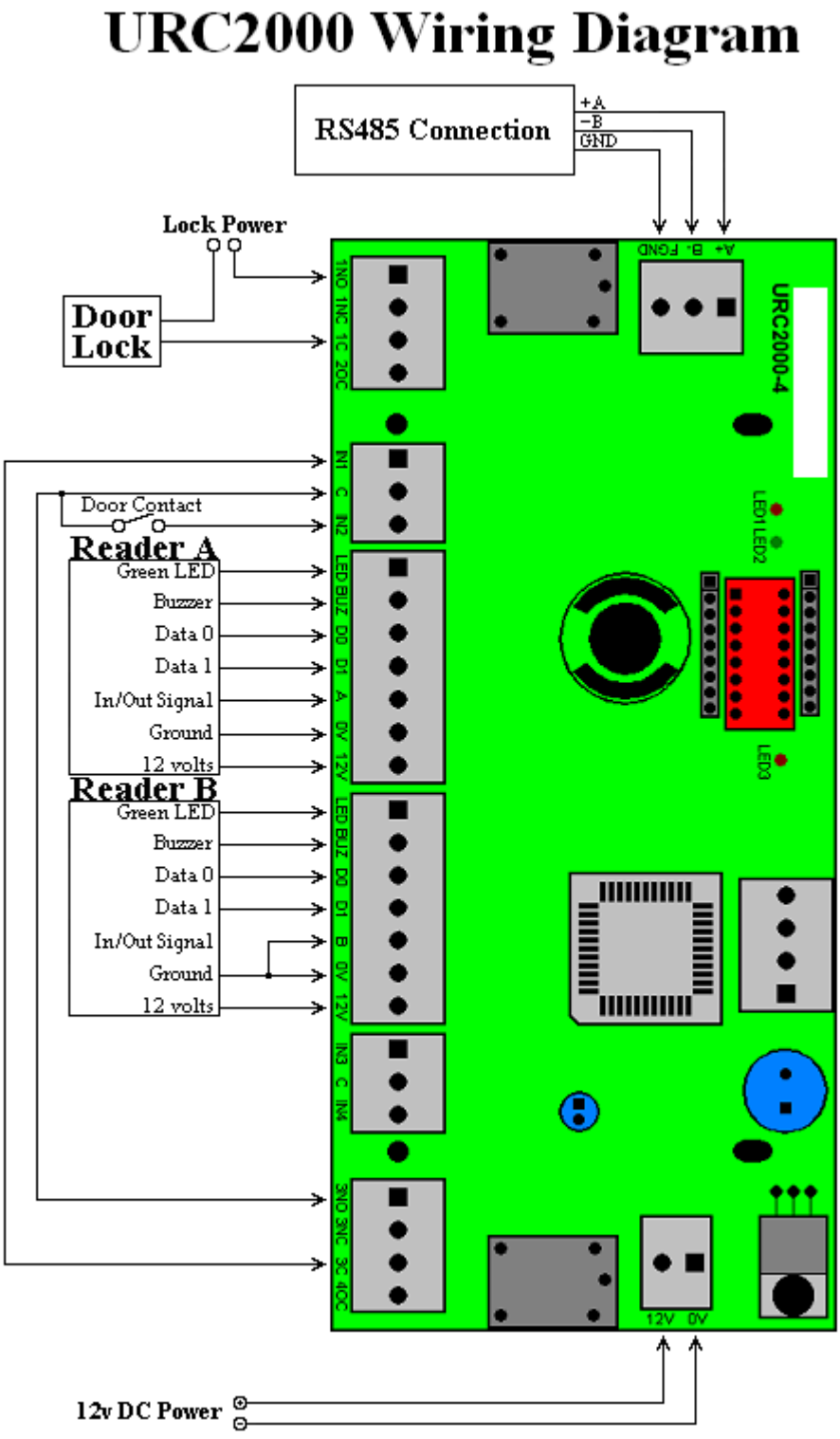


Figure 14: Connect Lock Output for Side B to RTE of Side A

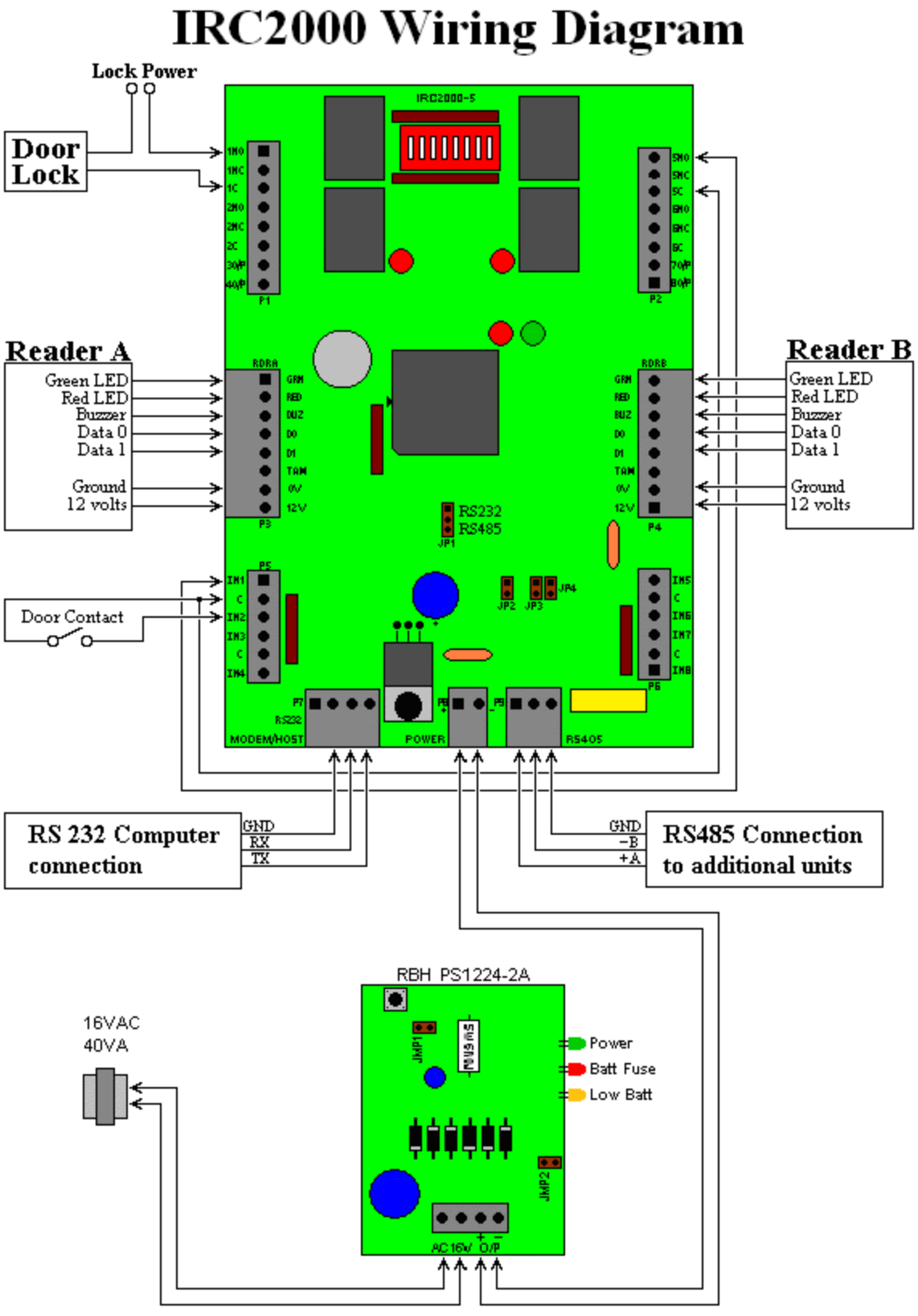


Figure 15: Connect Lock Output for Side B to RTE of Side A

Software Setup

Step 1

Create two areas: Area IN and Area OUT.

In the *Configure Window* right click on *Area* and select *Add Area*. Create two new areas. (Figure 16)

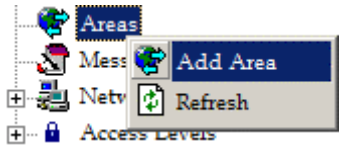


Figure 16: Create Two New Areas

Right click on *New Area* and select *Properties* as shown in Figure 17.

Figure 17: Open Properties Window

The *Area Properties* dialog box will pop up (Figure 18)

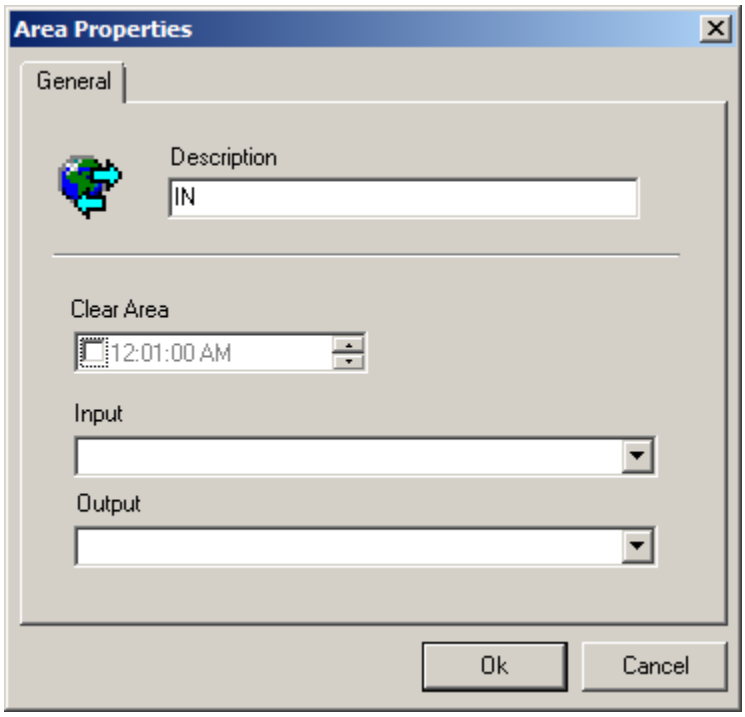


Figure 18: Area Properties Window

Enter Area name 'IN' in the Description textbox. Click OK button. Do the same for the other area naming it 'OUT'

Step 2

Setup APB for readers.

Reader A APB Settings:

In *Configure Window*, right click on Reader 1 and select properties. (Figure 19)

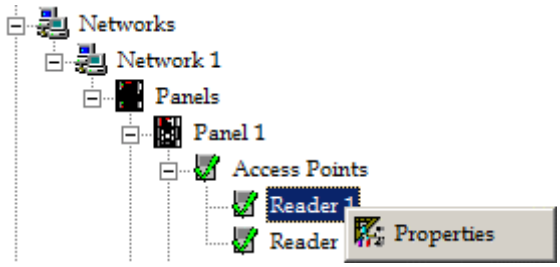


Figure 19: Opening Reader Properties

Reader 1 *Properties* dialog box will pop up. (Figure 20)

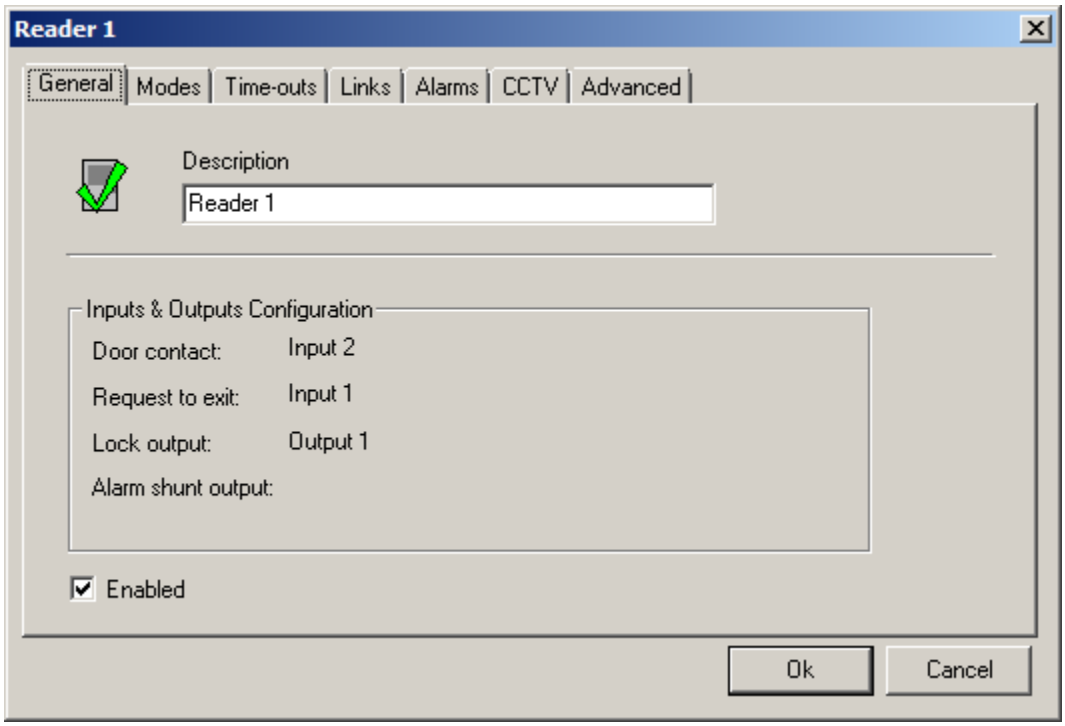


Figure 20: Reader 1 Properties Window

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 21.

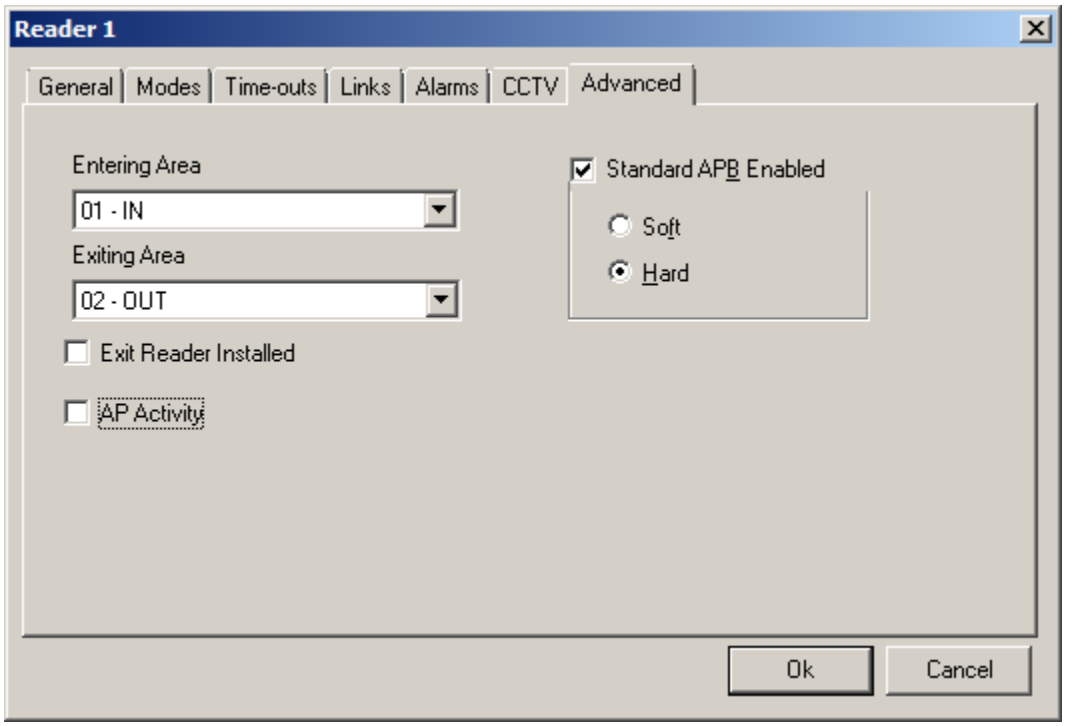


Figure 21: Selecting APB Properties on Reader 1

Select *Entering Area* IN and *Exiting Area* OUT

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Reader B APB Settings:

In *Configure Window*, right click on Reader 2 and select properties. Reader 2 *Properties* dialog box will pop up.

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 22.

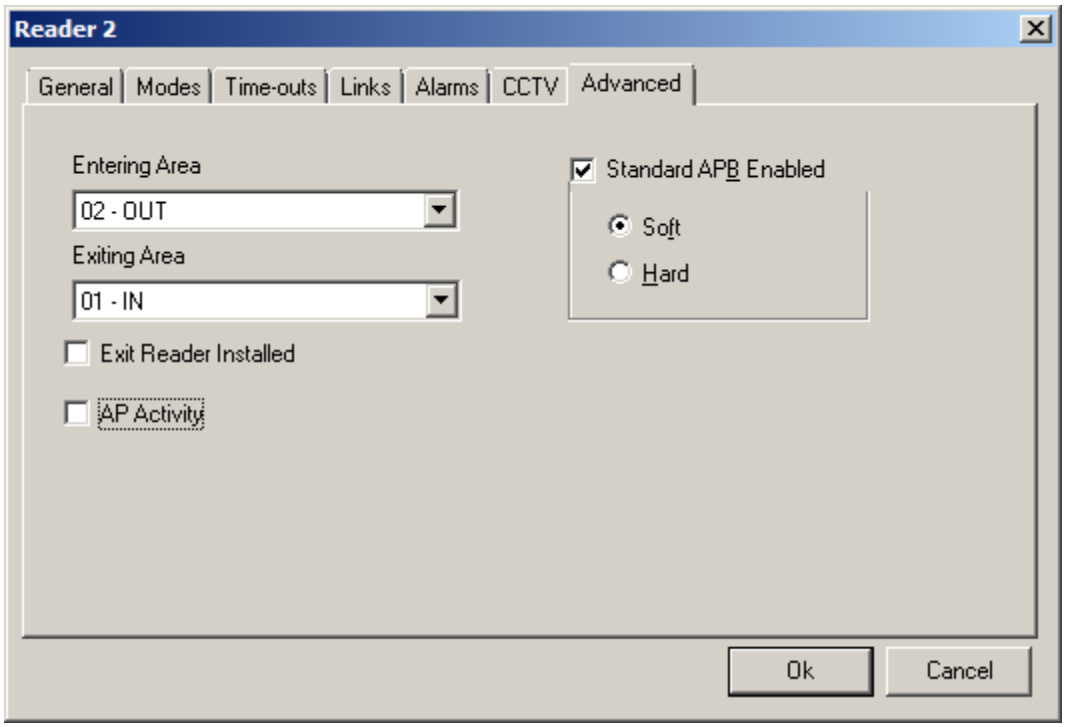


Figure 22: Selecting APB Properties on Reader 2

Select *Entering Area* OUT and *Exiting Area* IN

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Step 3

Down load to the panel and test the system to confirm operation.
See Step 3 of 'Local antipassback with two doors and two readers.

3.2 Local Antipassback with Exit Reader Module

Draw an Area and Reader layout.

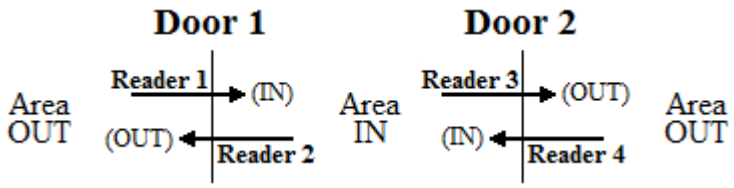


Figure 23: Lay Out For Local Antipassback with Exit Reader Module

In Figure 23, there are two areas: IN and OUT. Door 1 is controlled by Reader 1 and Reader 2 which are connected to side A of the panel. Door 2 is controlled by Reader 3 and Reader 4 which are connected to side B of the panel.

Hardware Setup

Exit Reader Module

The EXITRDR board enhances the IRC2000 and URC200 panels by allowing the connection of two readers to a single reader port. A single reader port can now have an 'In' and an 'Out' reader.

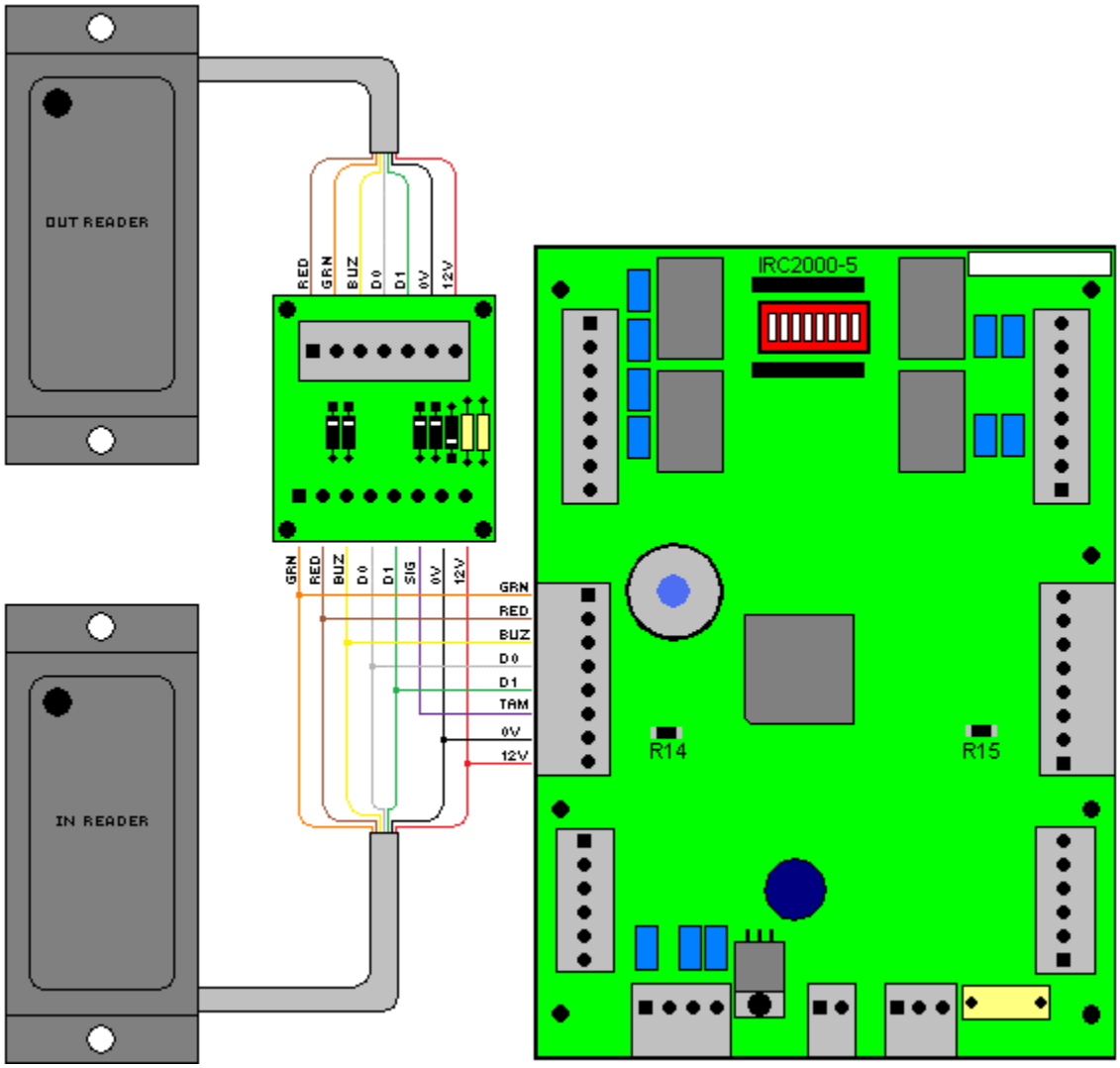


Figure 24: Exit Reader Module Wiring Diagram for IRC-2000 Panel

- ✓ **SIG signal is connected to the TAM terminal of the panel.**

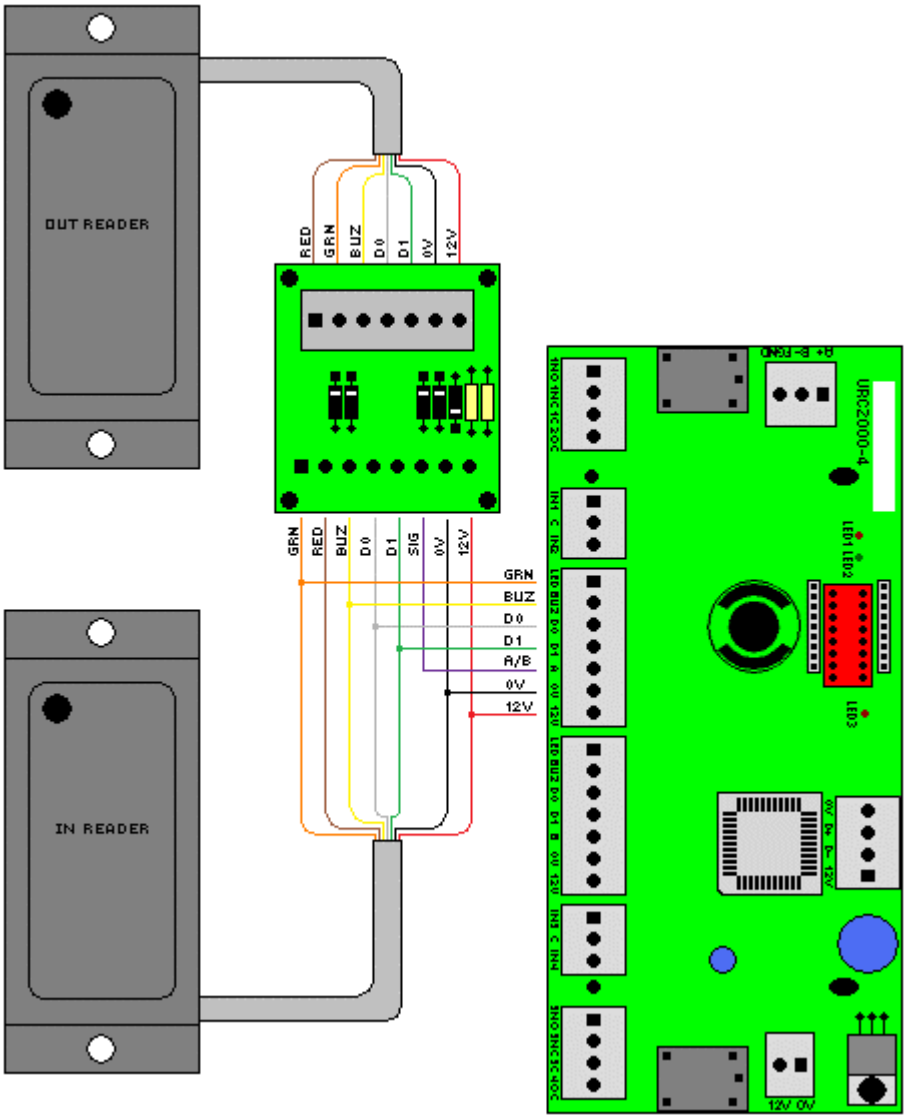


Figure 25: Exit Reader Module Wiring Diagram for IRC-2000 Panel

- ✓ **SIG signal is connected to the TAM terminal of the panel.**

Software Setup

Step 1

Create two areas: Area IN and OUT.

In the *Configure Window* right click on *Area* and select *Add Area*. Create two new areas. (Figure 26)

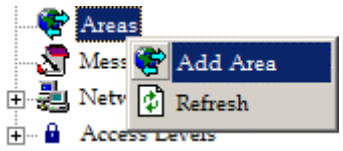


Figure 26: Create Two New Areas

Right click on *New Area* and select *Properties* as shown in Figure 27.

Figure 27: Open Properties Window

The *Area Properties* dialog box will pop up (Figure 28)

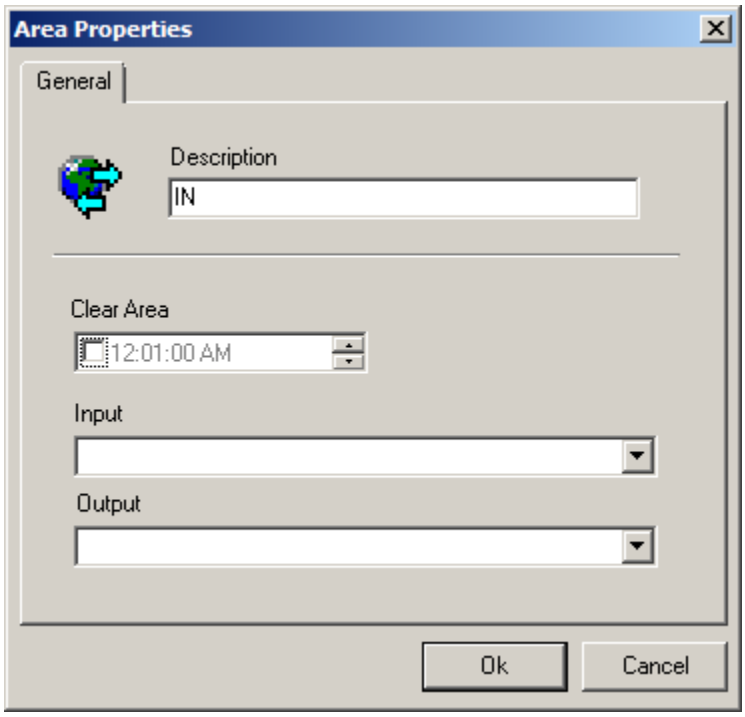


Figure 28: Area Properties Window

Enter Area name 'IN' in the Description textbox. Click OK button. Do the same for the other area naming it 'OUT'.

Step 2

Setup APB for readers.

Reader A APB Settings:

In *Configure Window*, right click on Reader 1 and select properties. (Figure 29)

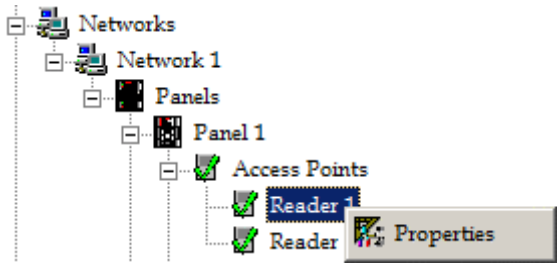


Figure 29: Opening Reader Properties

Reader 1 Properties dialog box will pop up. (Figure 30)

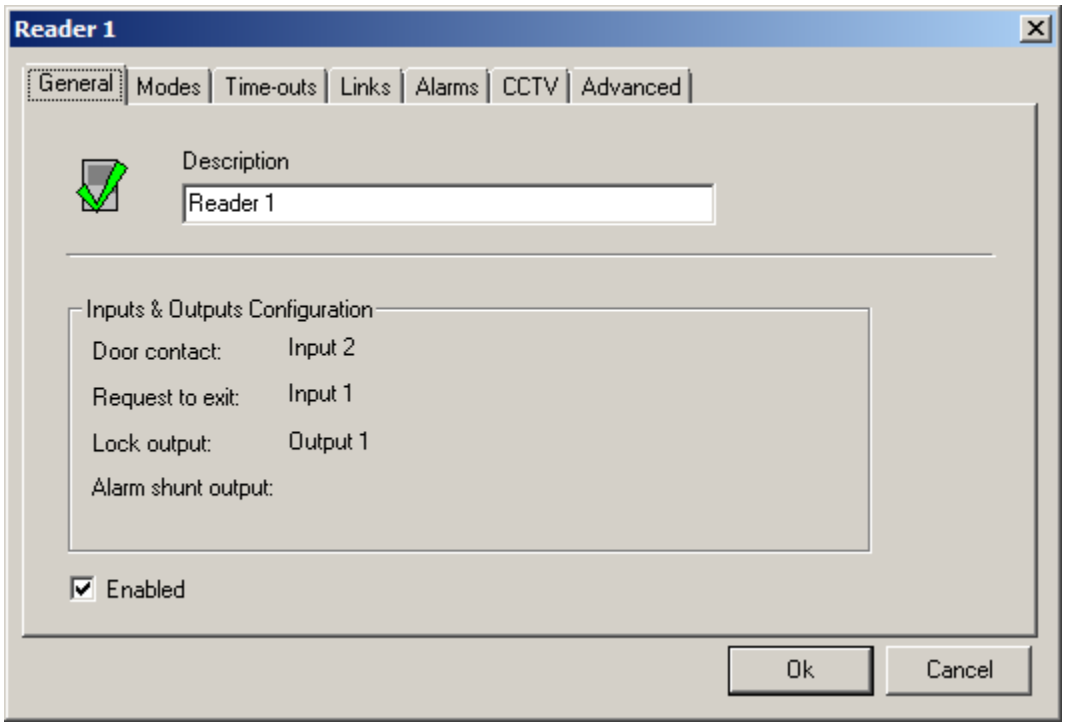


Figure 30: Reader 1 Properties Window

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 31.

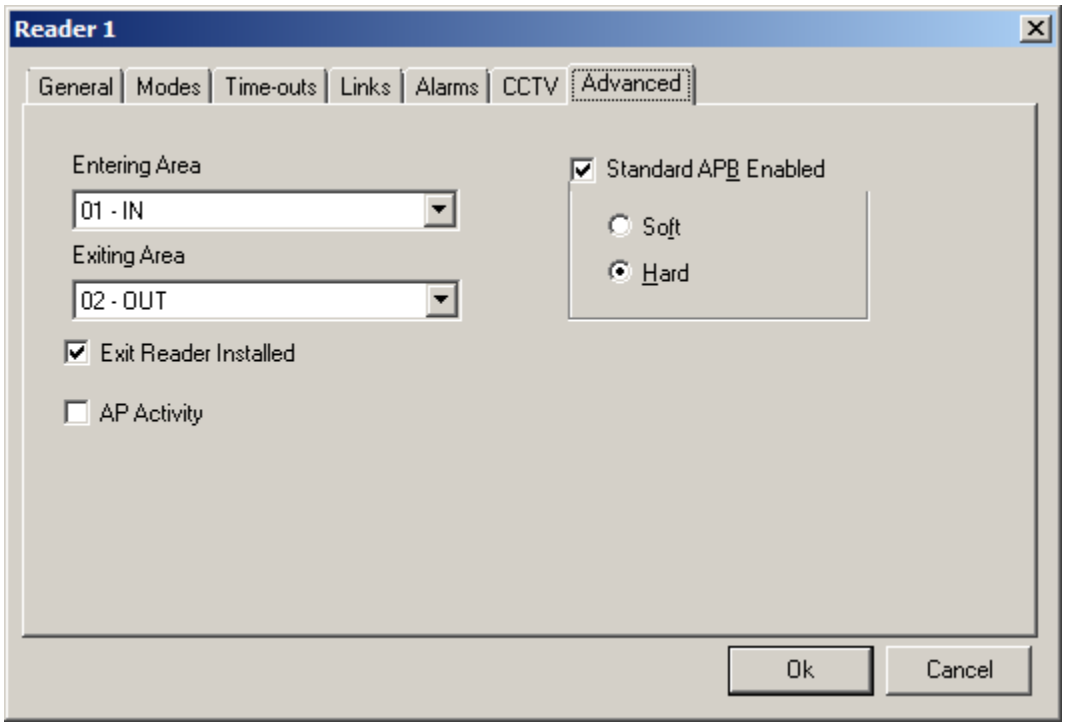


Figure 31: Selecting APB Properties on Reader 1

Select *Entering Area* IN and *Exiting Area* OUT.

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Reader B APB Settings:

In *Configure Window*, right click on Reader 2 and select properties. Reader 2 *Properties* dialog box will pop up.

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 32.

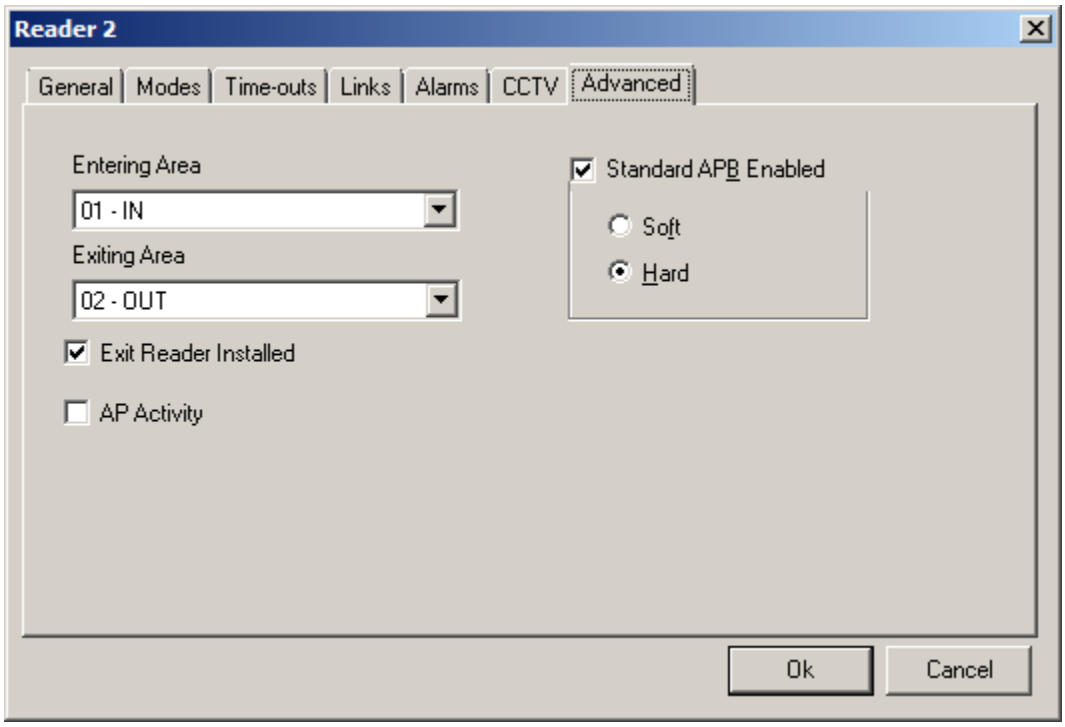


Figure 32: Selecting APB Properties on Reader 2

Select *Entering Area* OUT and *Exiting Area* IN.

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Step 3

In the *Device Status* window, right click on Panel 1, and select *Download* ▸ *All Files*. (Figure 33)

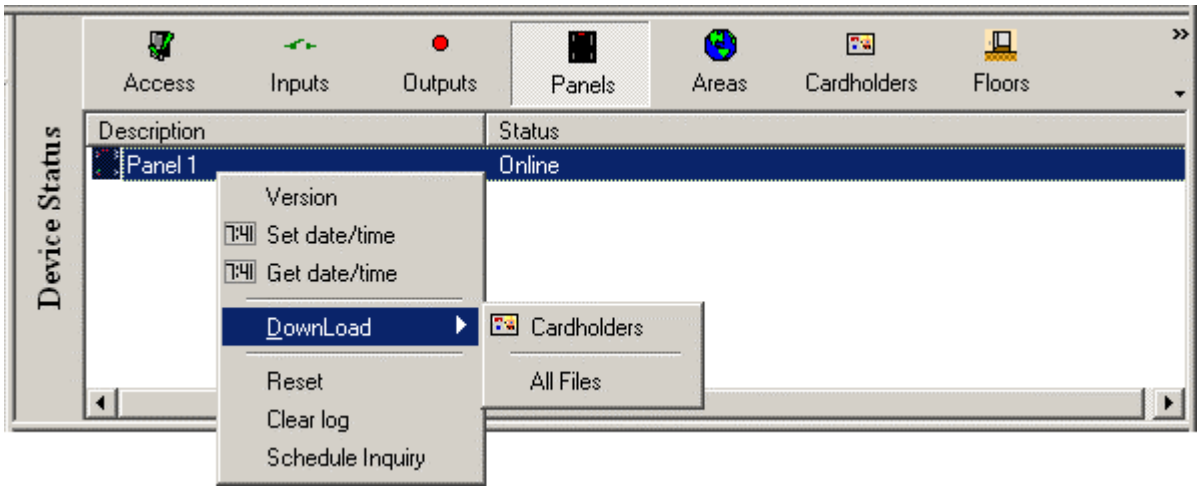


Figure 33: Download Database Files to the Panel

Test Procedure

1. Present the card on Side A IN reader.
2. Present the card on Side B OUT reader.
3. Present the card on Side A IN reader.
4. Present the card on Side A OUT reader.
5. Present the card on Side B IN reader.
6. Present the card on Side A IN reader.
7. Present the card on Side A OUT reader.

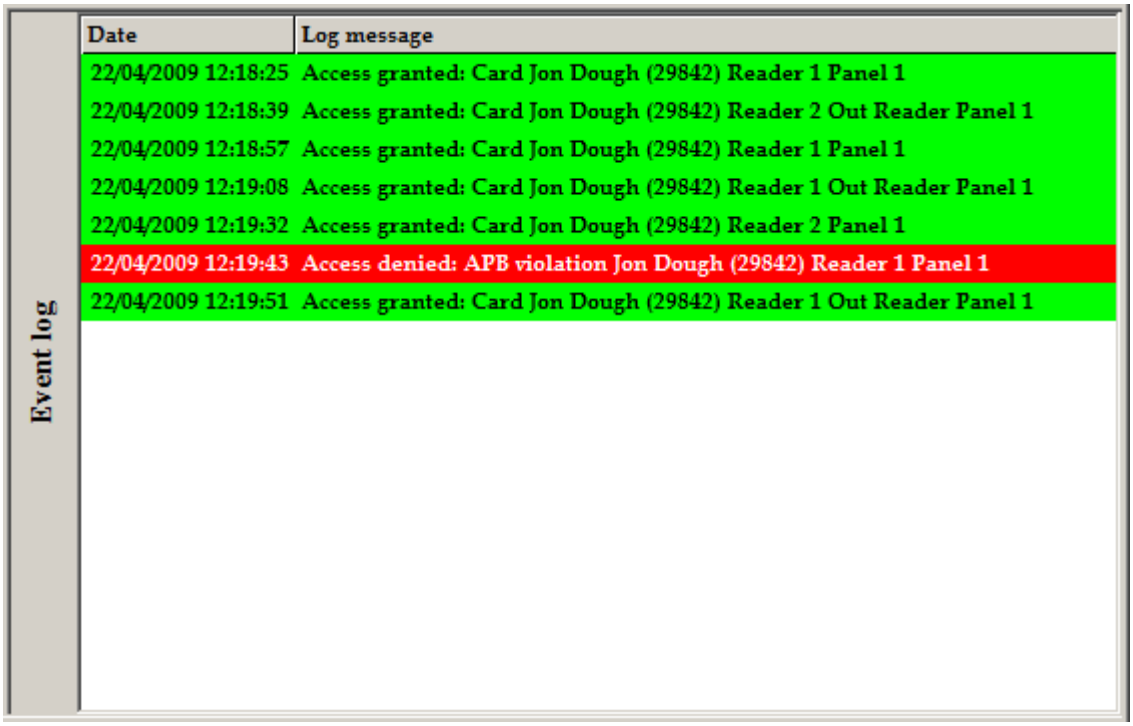


Figure 34: Test Results

Discussion

1. When the user presents the card on side A IN reader, the system grants the access, and the user enters the IN area. To go out, the user exits from side B through the OUT reader.
3. Then the user enters into the IN area again via the side A IN reader.
4. The user then goes out from the side A OUT reader.
5. Then user enters back inside through the side B IN reader. At this time the user is in the IN area, so if he wants to go out he needs to present his card at either the side A reader or the side B OUT reader.
6. However, as shown with a red message the user presented his card on the side A IN reader, and system denied the access.
7. The next green message shows that the user was able to go out by presenting his card on the side A OUT reader.

3.3 Global Antipassback

For *Global Antipassback*[1] to work the Integra32™ system must be online, and *PC Decision Required* must be turned on in the *Modes* tab of the *Reader Properties*' window for all of the appropriate readers; otherwise the panel will default to *Local Antipassback*[2] (within an IRC-2000). Global Antipassback allows a cardholder's area to be reset/cleared, meaning they are not logged into any area. With Local Antipassback the cardholder is either 'In' or 'Out' (never neither, always one or the other). Local Antipassback may be used with or without the Exit Reader Interface.

Figure 35 shows an example of how to set up global antipassback between panels. There are three rooms: room 1, room 2, and room 3. Room 1 and room 2 are divided with door 1, and door 1 is controlled with two readers (reader 1 and reader 2). Reader 1 and reader 2 are connected to panel 1 side A and side B respectively. Similarly, room 2 and room 3 are divided with door 2, and door 2 is controlled with two readers (reader 3 and reader 4). Reader 3 and reader 4 are connected to panel 2 side A and side B respectively. Since it is an antipassback system with more than one panel, it must be a global antipassback system.

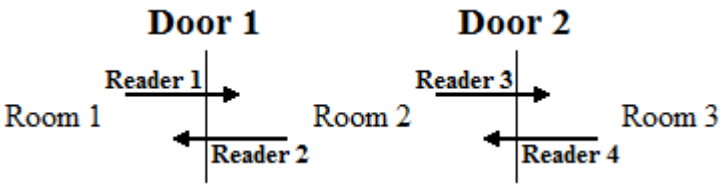


Figure 35: Layout of Global Antipassback

[1] *Antipassback tracked across multiple panels is Global Antipassback.*
[2] *Antipassback tracked within one panel is Local Antipassback.*

Hardware Setup

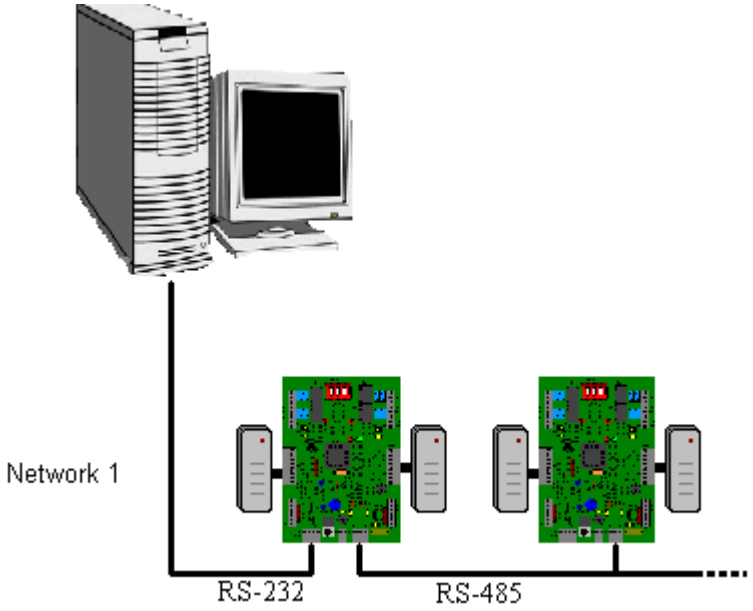


Figure 36: Global Antipassback Requires Normal Hardware Settings for Panels

- ✓ Don't connect reader's TAM (tamper terminal) to ground as we did for local APB. The side B lock output could be connected to the side A request-to-exit if both readers of one panel are to control the same door (as shown in Hardware Setup for 'local antipassback with one door and two readers').

Software Setup

Step 1

Create three areas Room 1, Room 2, and Room 3.

In the *Configure Window* right click on Area select *Add Area* and *New Area* will appear under the Area option. (Figure 37)

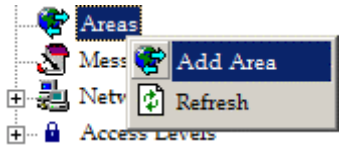


Figure 37: Create Three New Areas

Right click on *New Area* and select *Properties* as shown in Figure 38.

Figure 38: Open Properties Window

The *Area Properties* dialog box will pop up. (Figure 39)

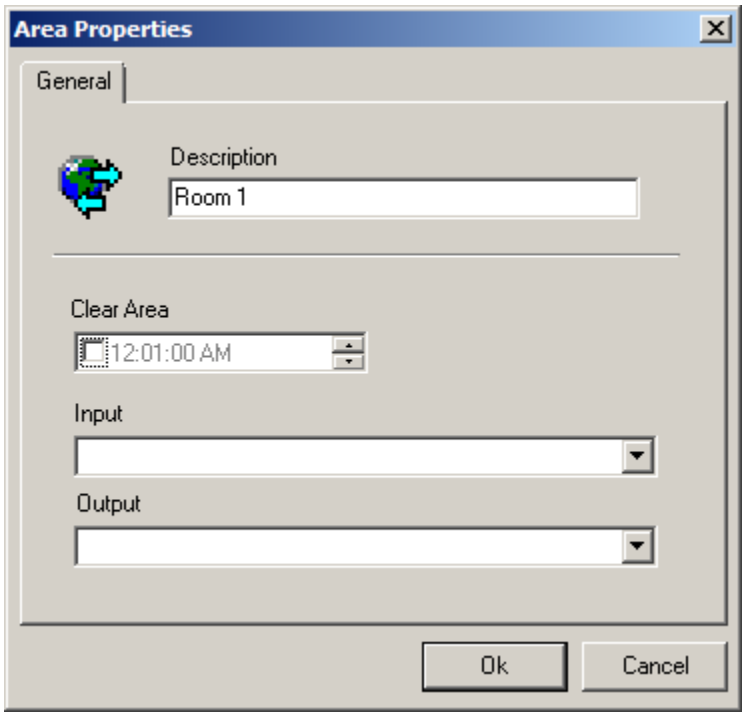
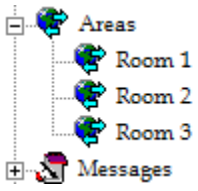


Figure 39: Area Properties Window

Enter area name ‘Room 1’ in the *Description* textbox. Click OK button. Do the same for the other two areas naming them ‘Room 2’ and ‘Room 3’.



Step 2

Setup APB for readers.

Panel 1 Reader A APB Settings:

In *Configure Window*, right click on Reader 1 and select properties. (Figure 40)

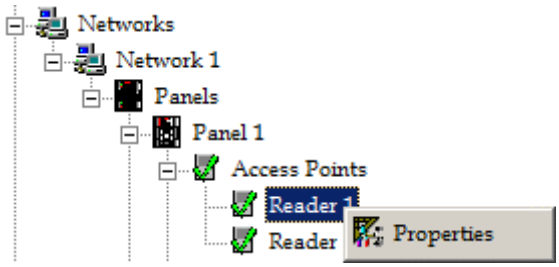


Figure 40: Opening Reader Properties

Reader 1 *Properties* dialog box will pop up. (Figure 41)

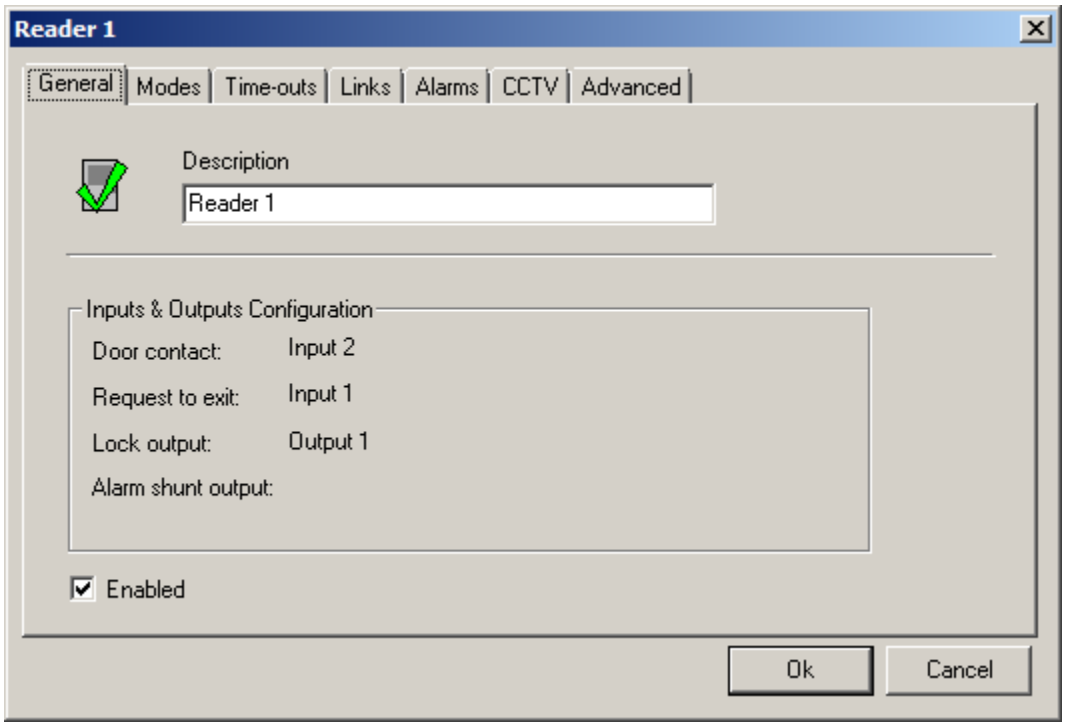


Figure 41: Reader 1 Properties Window

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 42.

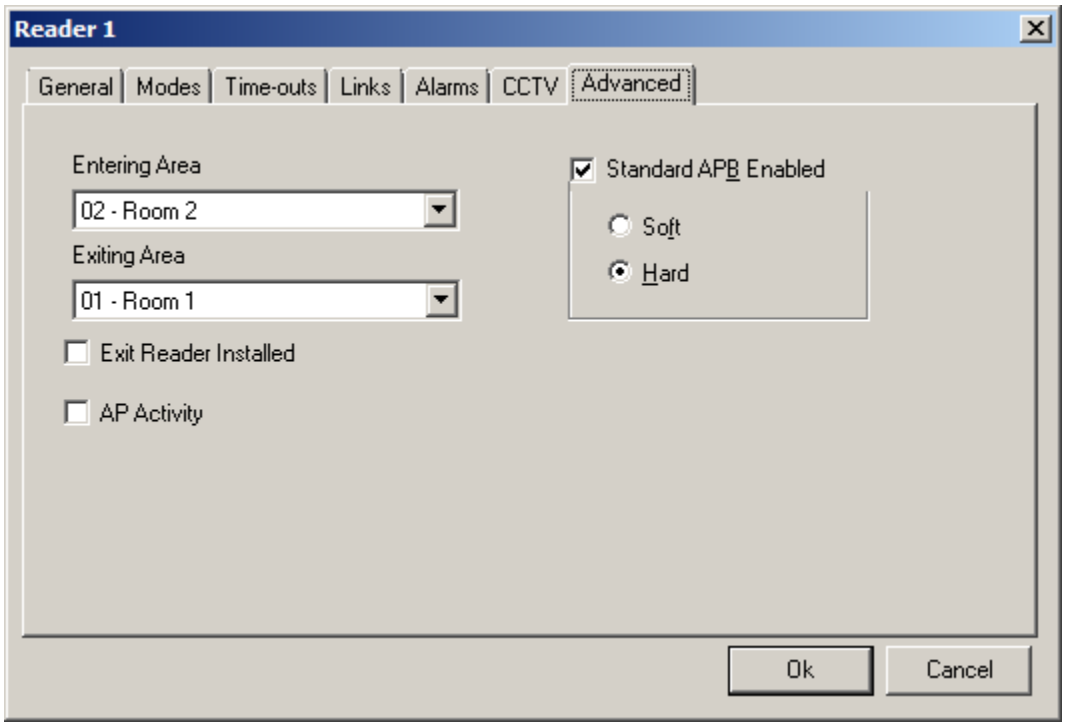


Figure 42: Selecting APB Properties on Reader 1

Select *Entering Area* Room 2 and *Exiting Area* Room 1.

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Panel 1 Reader B APB Settings:

In *Configure Window*, right click on Reader 2 and select properties. Reader 2 *Properties* dialog box will pop up.

Click on *Advanced* tab to open the form for APB settings, which is shown in Figure 43.

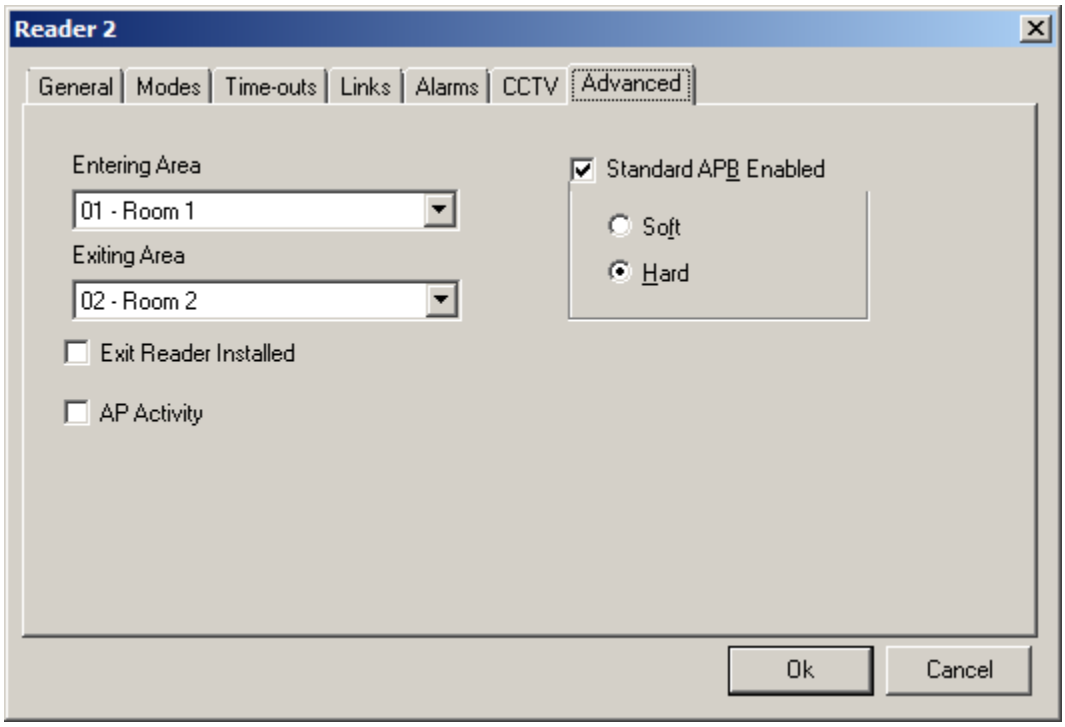


Figure 43: Selecting APB Properties on Reader 2

Select *Entering Area* Room 1 and *Exiting Area* Room 2

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Panel 2 Reader A APB Settings:

In *Configure Window*, right click on Reader 1 and select properties. (Figure 43)

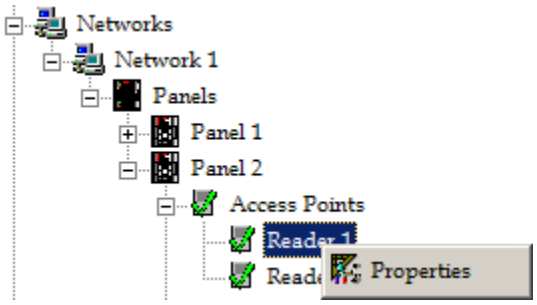


Figure 44: Opening Reader Properties

Reader 1 Properties dialog box will pop up. (Figure 45)

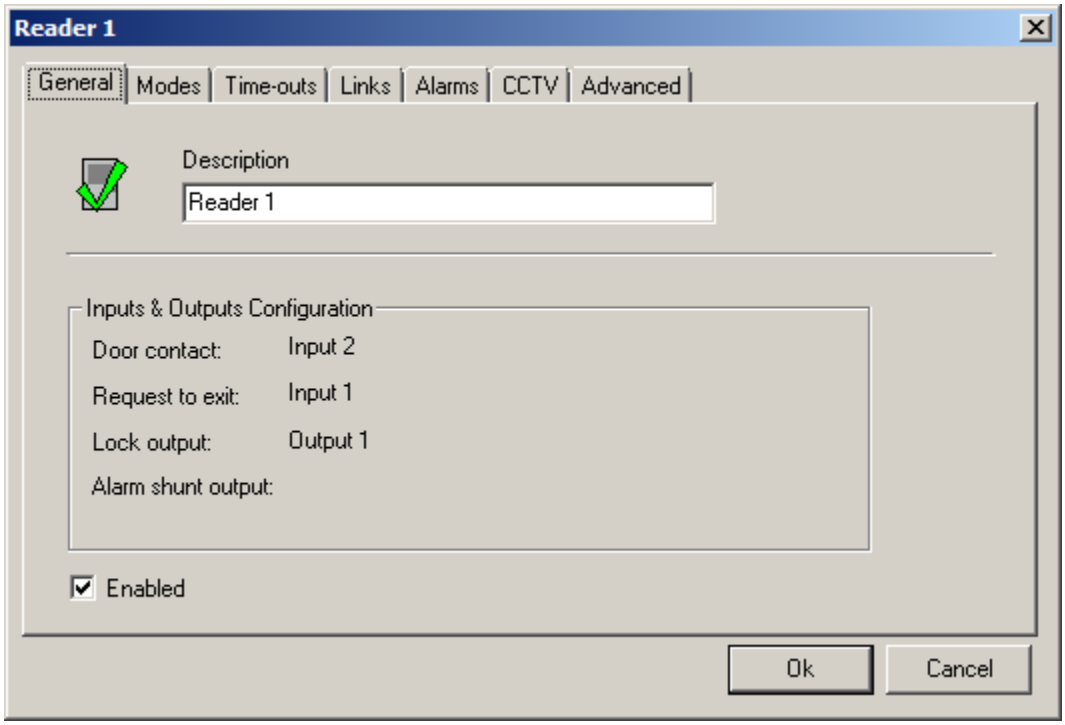


Figure 45: Reader 1 Properties Window

Rename the reader to Reader 3 and click on *Advanced* tab to open the form for APB settings, which is shown in Figure 46.

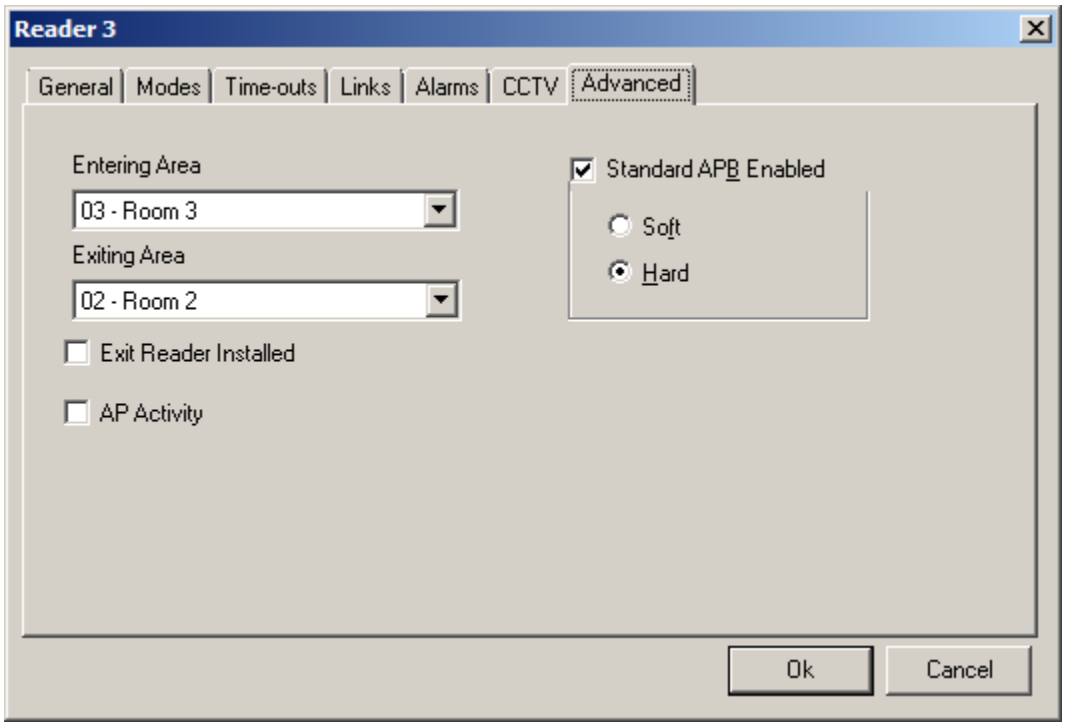


Figure 46: Selecting APB Properties on Reader 1

Select *Entering Area* Room 3 and *Exiting Area* Room 2.

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Panel 1 Reader B APB Settings:

In *Configure Window*, right click on Reader 2 and select properties. Reader 2 *Properties* dialog box will pop up.

Rename the reader to Reader 4 and click on the *Advanced* tab to open the form for APB settings, which is shown in Figure 47.

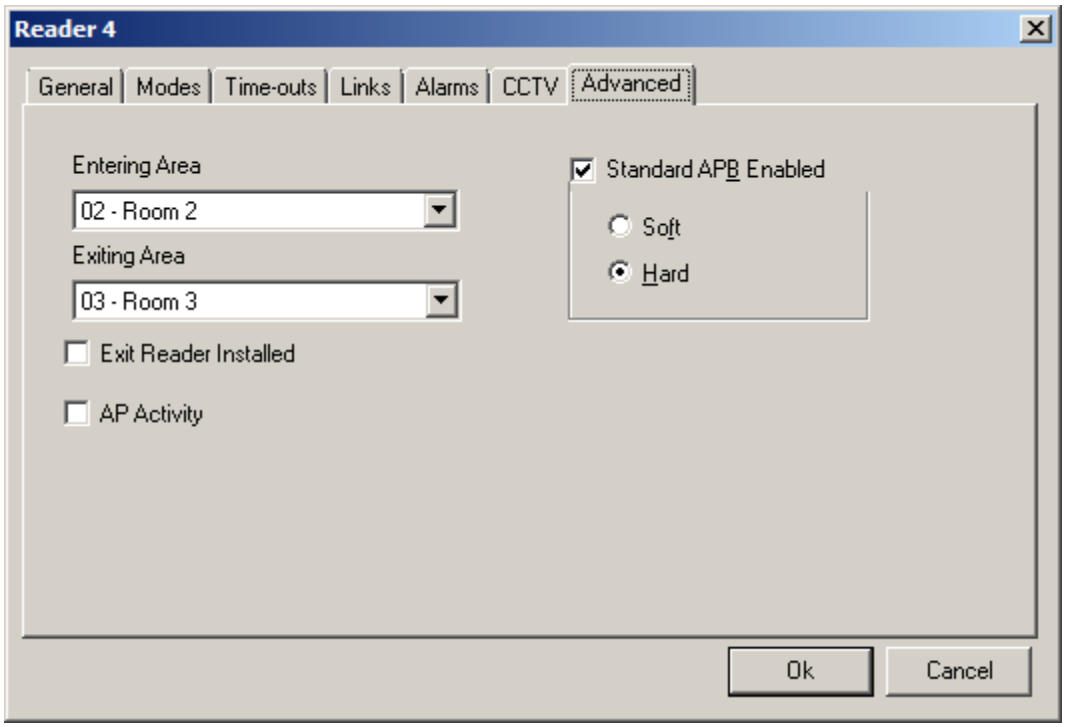


Figure 47: Selecting APB Properties on Reader 2

Select *Entering Area* Room 2 and *Exiting Area* Room 3.

Check *Standard APB Enabled*, and then select the Soft radio button or the Hard radio button. Click OK.

✓ **Recall that Soft antipassback will still grant access even though APB has been violated, Hard APB will not.**

Check PC Decision Required option for Reader.

In *Configure Window* right click on each reader and select properties. The reader's properties dialog box will pop up (Figure 48). Select the *Modes* tab.

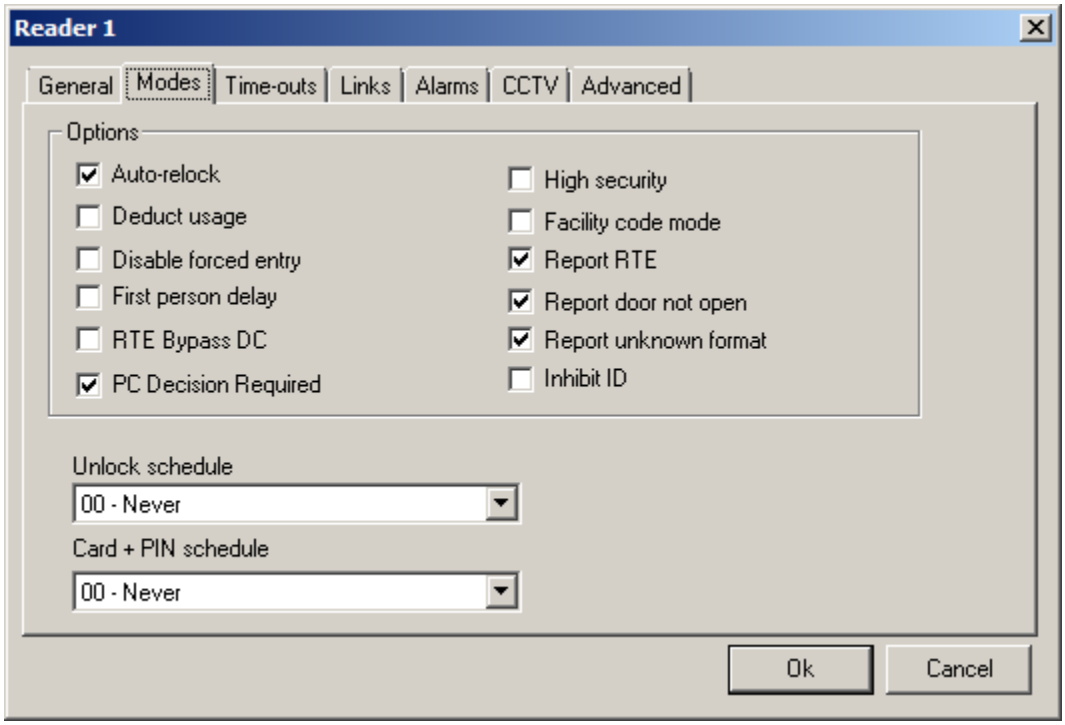


Figure 48: Reader 1 Properties Window - Modes

PC Decision Required needs to be checked for global antipassback, do this for each reader then download to all applicable panels.

3.4 Global Antipassback with Exit Reader Module

Step 1

Draw an area and reader layout.

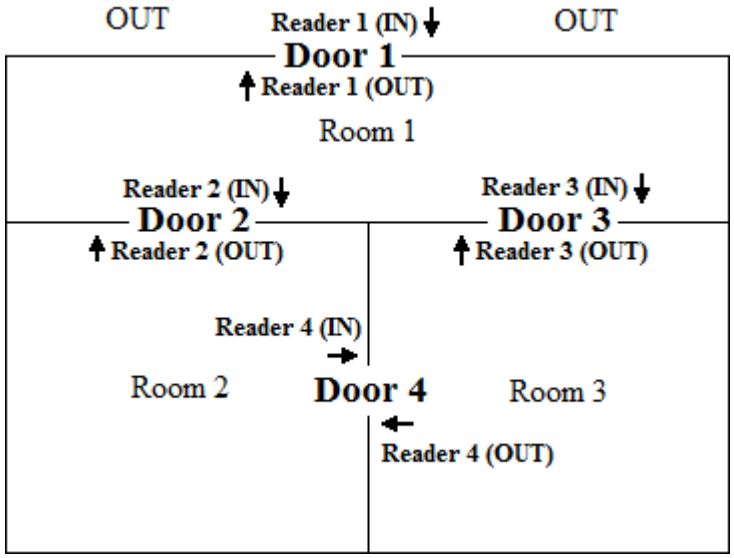


Figure 49: Layout for Global Antipassback

Figure 49: shows that Reader 1 can be used to enter from Area OUT to Room 1. Reader 2 is the entrance from Room 1 to Room 2. Similarly, Reader 3 can be used to enter Room 3 from Room 1. Reader 4 allows access from Room 2 to Room 3.

Hardware Setup

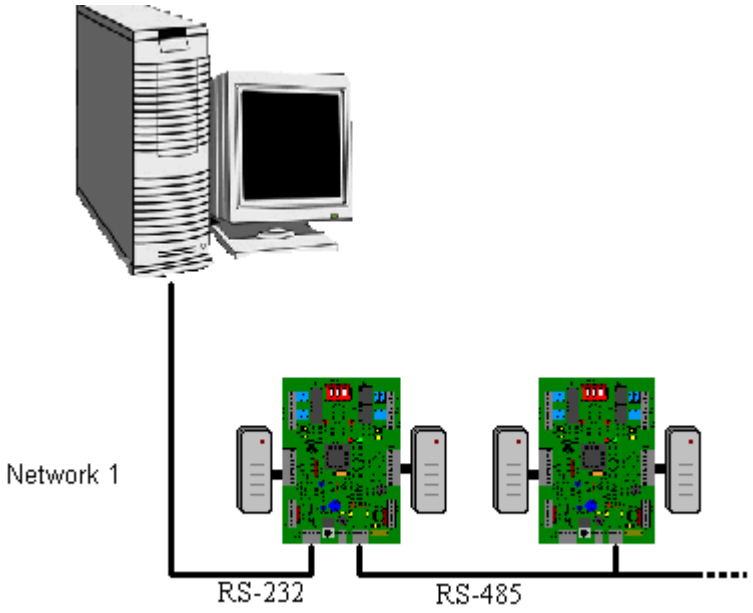


Figure 50: Global Antipassback Requires Normal Hardware Settings for Panels

Software Setup

Step 1

Create Areas OUT, Room 1, Room 2, and Room 3.

Use the same procedure as shown in Step 1 of software setup for global antipassback.

Step 2

Assign the antipassback on the readers. Use the same procedure as shown in Step 2 of software setup for global antipassback.

Set Reader 1
- ✓ Entering Area – Room 1
- ✓ Exiting Area – OUT

Set Reader 2
- ✓ Entering Area – Room 2
- ✓ Exiting Area – Room 1

Set Reader 3
- ✓ Entering Area – Room 3
- ✓ Exiting Area – Room 1

Set Reader 4
- ✓ Entering Area – Room 3
- ✓ Exiting Area – Room 2

PC Decision Required needs to be checked for global antipassback, do this for each reader then download to all applicable panels.

✎ **The IN and out reader is assigned by the hardware. That is, the reader that is connected to the panel is IN reader, and the other reader is OUT reader.**

Test Procedure

1. Present the card on Door 1 IN reader.
2. Present the card on Door 2 IN reader.
3. Present the card on Door 4 IN reader.
4. Present the card on Door 3 OUT reader.
5. Present the card on Door 1 IN reader.
6. Present the card on Door 2 IN reader.
7. Present the card on Door 3 IN reader.
8. Present the card on Door 4 IN reader.
9. Present the card on Door 1 IN reader.

Discussion

When the user presents the card on Reader 1 (IN), the system grants the access and the user enters Room 1 and exits area OUT. To go out the user exits Room 1 via Reader 2 (IN) and enters Room 2. Then the user enters Room 3 via Reader 4 (IN). He goes out of Room 3 using Reader 3 (OUT) thereby entering Room 1. He then leaves through Reader 1 (OUT) into area OUT. However, if the user were somehow to present his card at Reader 2 (IN), Reader 3 (IN), or Reader 4 (IN) he would be denied access. In fact the only reader his card would work at is Reader 1 (IN).

3.5 Timed Antipassback

Set timed antipassback

Open the reader properties and select the *Times-outs* tab. Set the amount of time for *Timed Antipassback*[3] here.

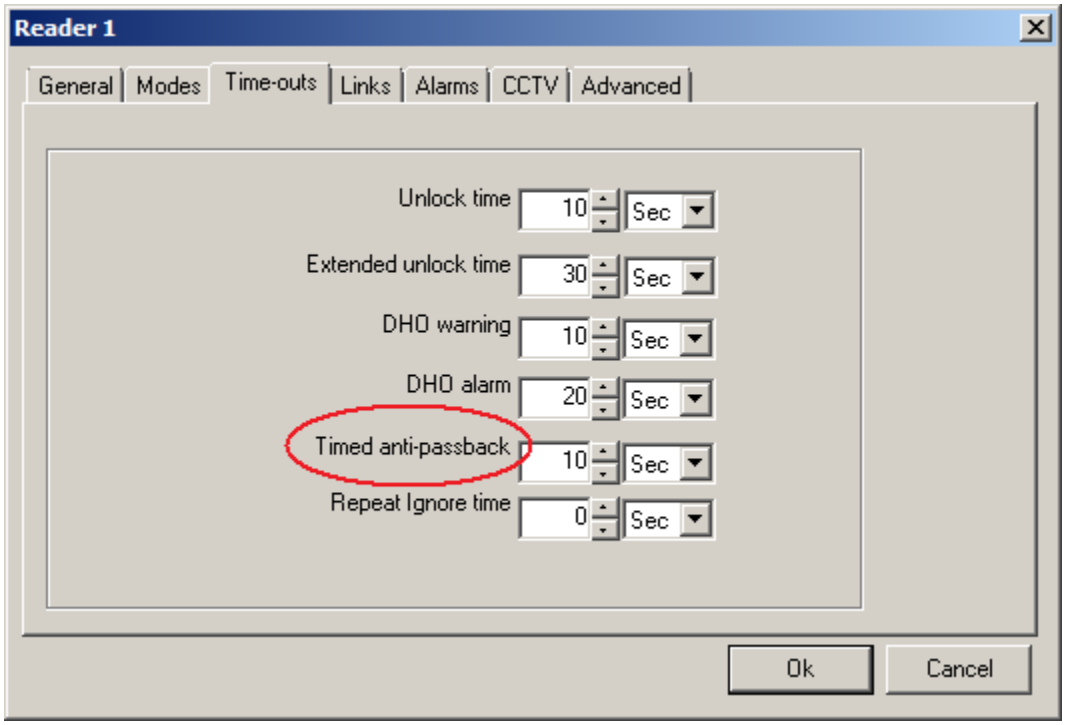


Figure 51: Reader Properties *Times-Outs* Tab

Timed Anitpassback is the lowest level of antipassback. Hardware and software are setup the same as for local antipassback.

[3] Timed Antipassback will reset at the end of the programmed time allowing the cardholder to be granted access into an area they are already logged into. If a cardholder tries to re-enter an area before the timer expires they will cause an antipassback violation.

Table of Figures

Index