

Centralized Opening

AxiomV™

Integration Setup

USER MANUAL

**New generation
building security**



Table of Contents

CONFIGURING THE SYSTEM	3
CONFIGURING THE ACCESS POINTS	9
ALARM MONITORINGPROCEDURE.....	16
LICENSE & WARRANTY.....	21

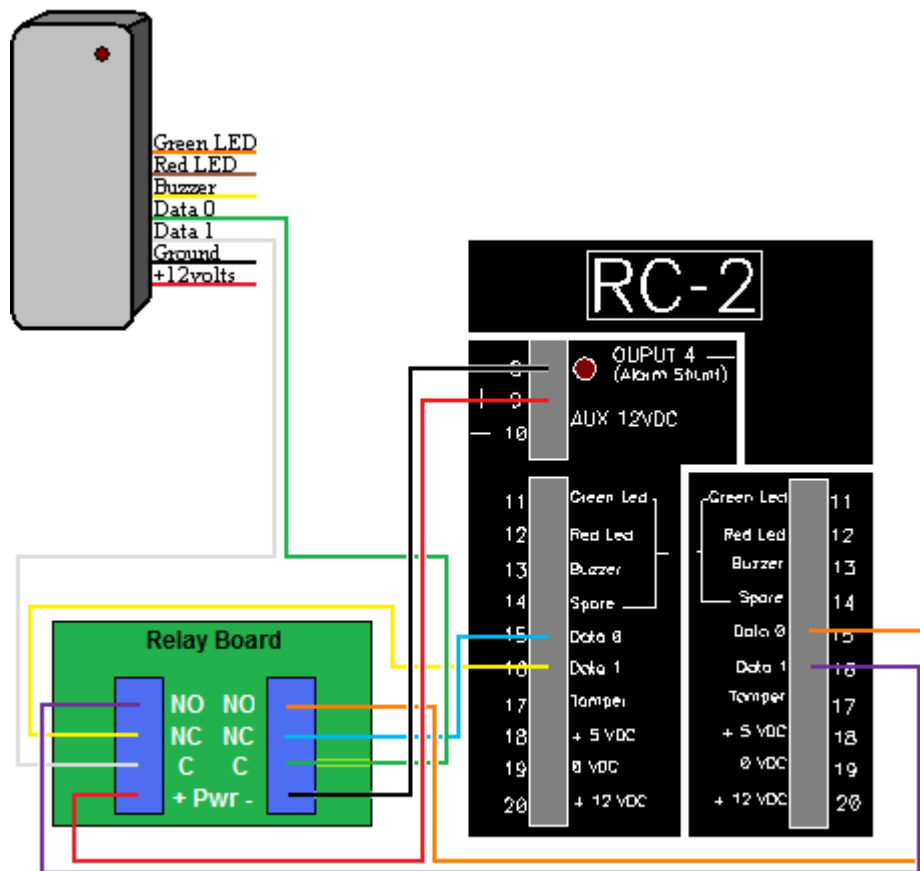
Configuring the System

Centralized Opening is a system option where operator controls the access as per cardholder requests after verifying the person at door requesting to access.

Currently, it is implemented for two people to present the cards one after another requesting access, the operator verifies the information of the cardholders as per the video they see on the screen and if all the information matches, allows access through *Remote Opening*, otherwise *Deny Access* with their comments for denying access in *Alarm detail window*.

Some modifications in hardware is required to implement *Remote Opening*

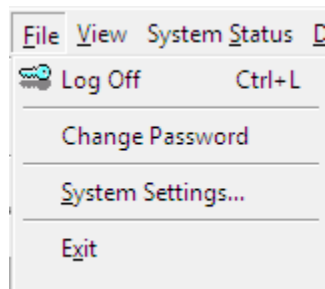
- One RC per door is required so that the picture of both the cardholders can be seen at the same time on the screen.
- The reader needs to be connected only at the A side of the RC.
- One of the Output on side A of the RC is configured as General Purpose Output (any output which is not in use as default output)
- This general purpose output is connected to a Relay board, which also connects to D0 and D1 of side A as well as D0 and D1 of side B, as shown in the diagram below:



- Relay board connection helps to switch the second cardholder swipe on the reader connected to side A to show as a swipe on side B, so that the pictures of both the cardholders can be seen on the video screen at the same time. This is achieved with global command explained later.

To configure the AxiomV system.

- In the main form click on *File*.



- Then click on *System Settings*....

System Settings

General | Display | Badge | **System** | AP Activity | Email Config

☐ Multiple Credentials
 ☐ Send cleared alarms to message port
☐ Restrict Duplicate Card PIN
 ☐ Autogenerate Card number
☐ Multiple Access Levels
 ☐ Do not Initialize the panels
☐ Print area muster report on this client
 ☐ Show Cardholder PIN Code
☐ Use Cardholder Initial Field as numeric data

Use Cardholder Initial Field as:
 Min Data:
 Auto void cards after: Days

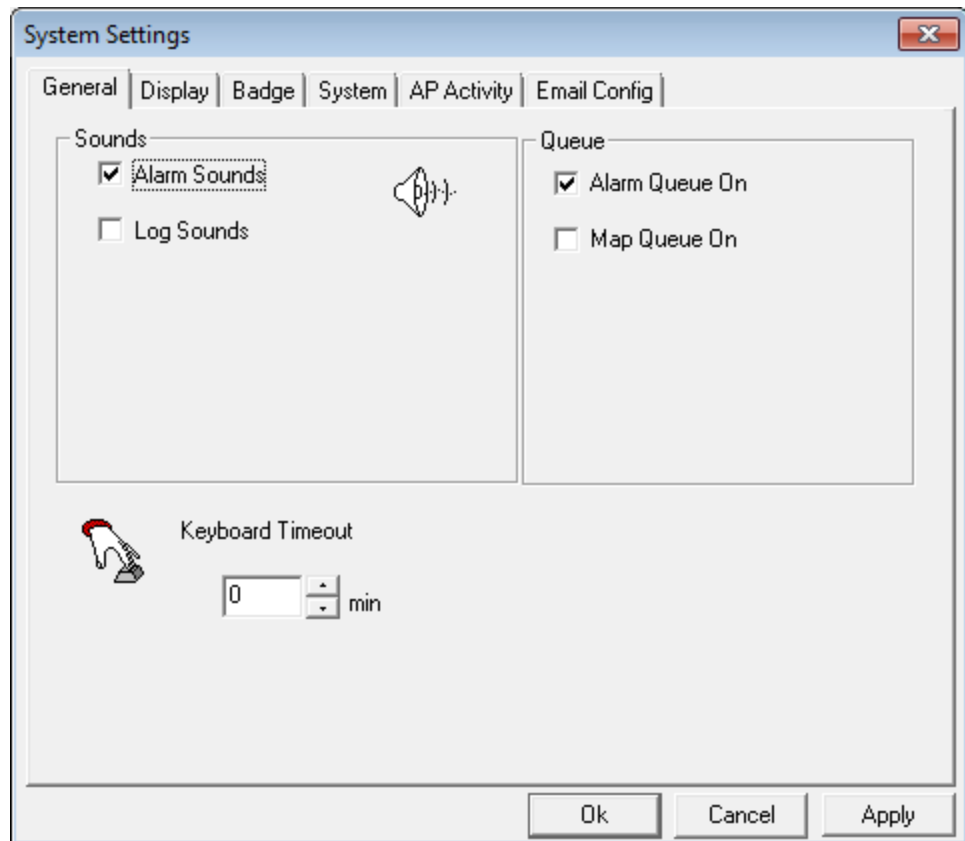
Card Holder Picture Size (Millimeters)
 Height: Width:
 Operator password expires after: Days

Area status check Interval: Seconds (min recommended 60)
 Alarm sound delay: Sec

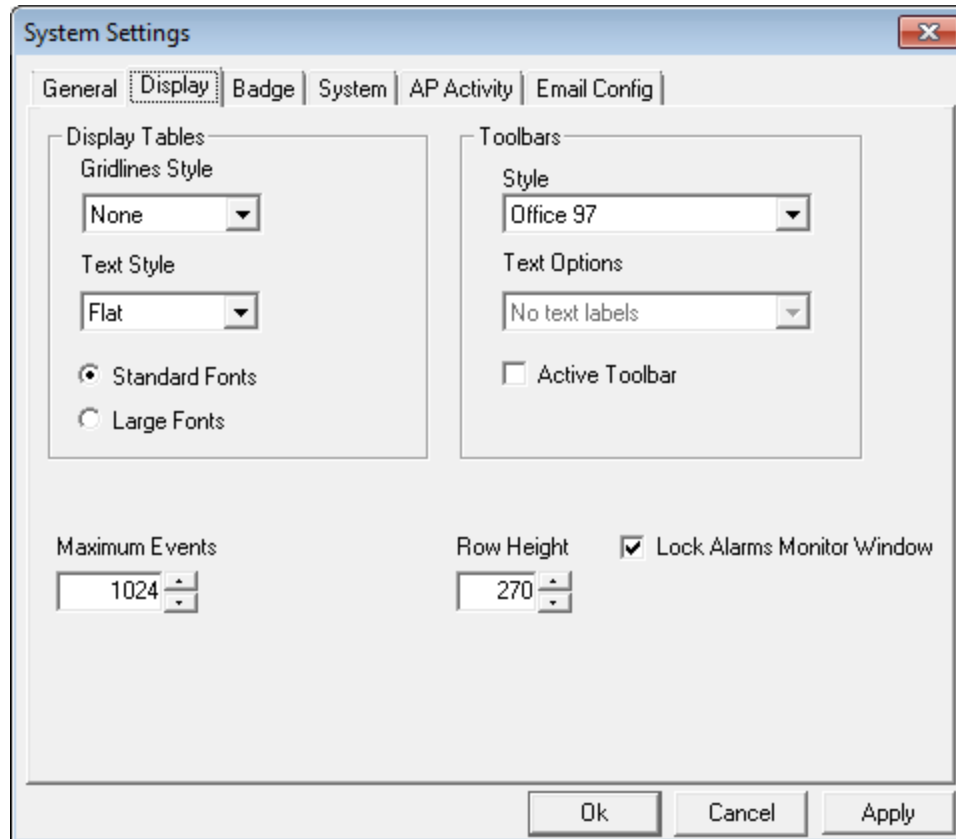
☒ Centralized opening

Ok Cancel Apply

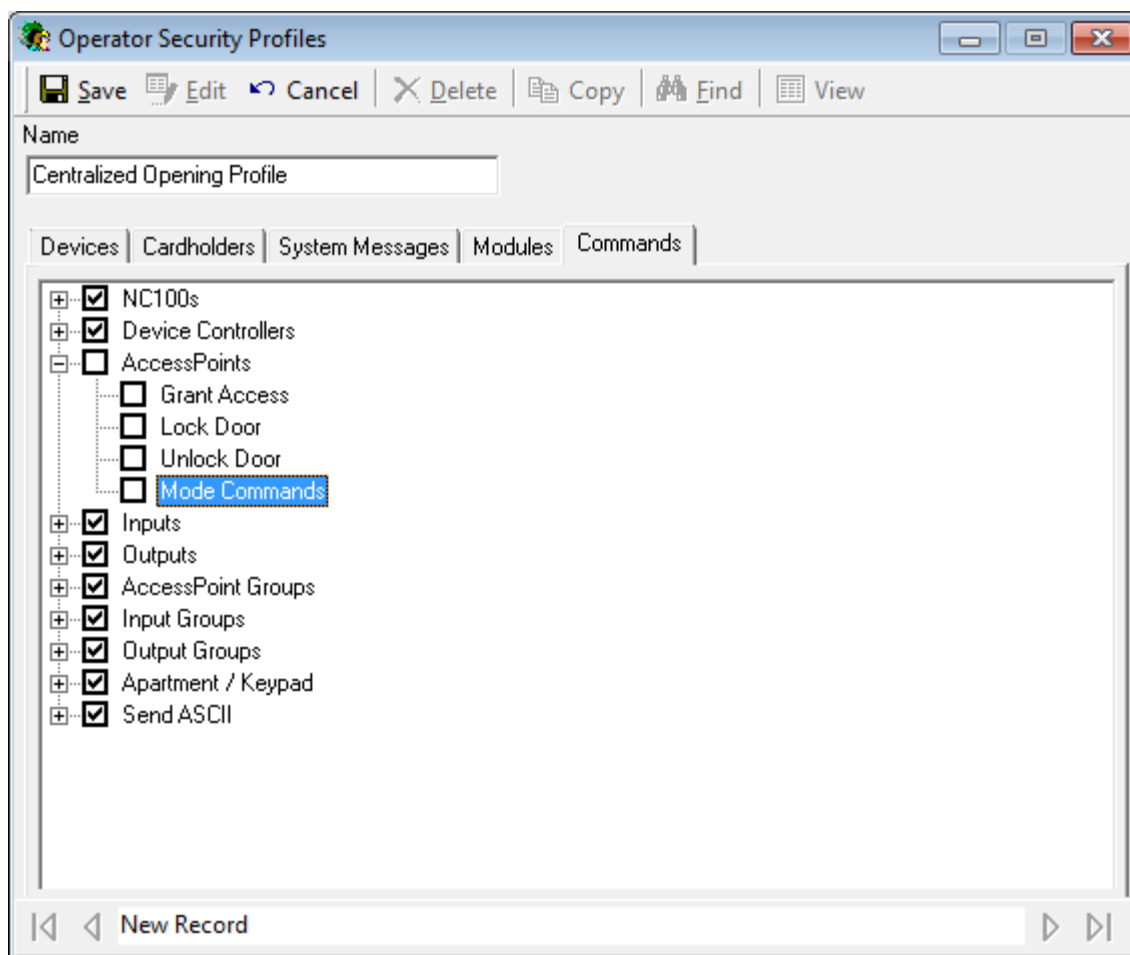
- Click on the *System Tab* and check *Centralized opening*. (**Centralized Opening cannot be combined with the regular video pop ups on events and alarms**)
- Click on *General tab* and check *Alarm Queue on*.



- Next click on the *Display Tab*.



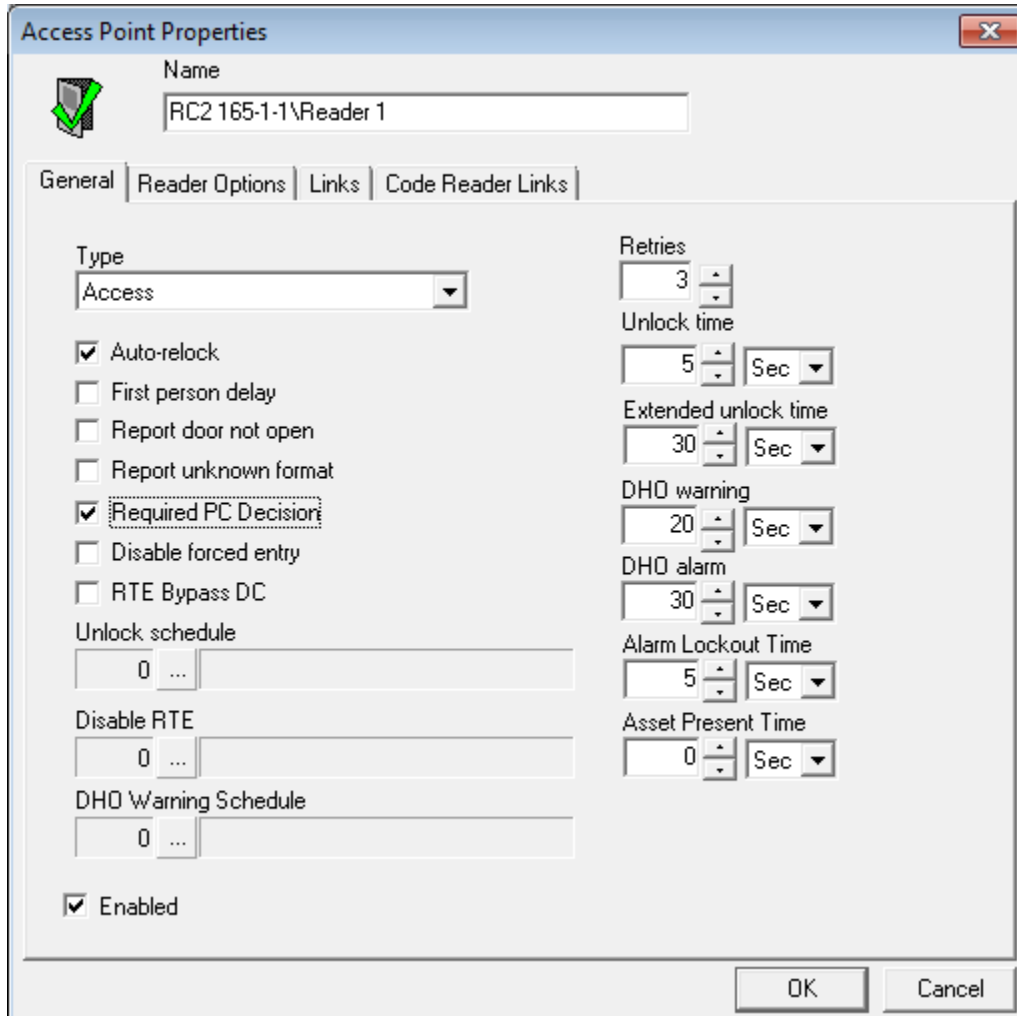
- Check the *Lock Alarms Monitor Window* to lock the Alarm window.
- The operators shouldn't have access to any commands related to Access points which can be set in the *Operator Profile* assigned to these operators by removing the access to these commands from *Commands* tab as shown below.



Configuring the Access Points


Now the access points need to be configured.

- Right click on the desired access point and select *Configuration.....*

The image shows a Windows-style dialog box titled "Access Point Properties". It has a standard Windows icon in the top-left corner and a close button (X) in the top-right. Below the title bar, there is a "Name" field containing the text "RC2 165-1-1\Reader 1". Below the name field are four tabs: "General", "Reader Options", "Links", and "Code Reader Links". The "General" tab is currently selected. Inside the "General" tab, there are several settings. On the left side, there is a "Type" dropdown menu set to "Access". Below it are several checkboxes: "Auto-relock" (checked), "First person delay" (unchecked), "Report door not open" (unchecked), "Report unknown format" (unchecked), "Required PC Decision" (checked), "Disable forced entry" (unchecked), "RTE Bypass DC" (unchecked), "Unlock schedule" (a field with "0" and an ellipsis), "Disable RTE" (a field with "0" and an ellipsis), and "DHO Warning Schedule" (a field with "0" and an ellipsis). At the bottom left of the tab is a checked "Enabled" checkbox. On the right side of the tab, there are several numeric input fields with up/down arrows and unit dropdowns: "Retries" (3), "Unlock time" (5 Sec), "Extended unlock time" (30 Sec), "DHO warning" (20 Sec), "DHO alarm" (30 Sec), "Alarm Lockout Time" (5 Sec), and "Asset Present Time" (0 Sec). At the bottom right of the dialog are "OK" and "Cancel" buttons.

- Check the *Required PC Decision* to allow the operator to grant access.
- Configure the desired output as *General purpose* output.(In our example, we are changing Alarm Shunt, output 4 on side A, as *General Purpose* output.

Output Properties

 Name: RC2 165-1-1\Reader 1 Alarm Shunt

General | Links

☒ OutputType Defaulted

Alarm Shunt


On State: Energized

Counter Value: 0

☒ Enabled

OK Cancel

Output Properties

 Name: Relay Switch

General | Links

☐ OutputType Defaulted

General Purpose

On State: Energized

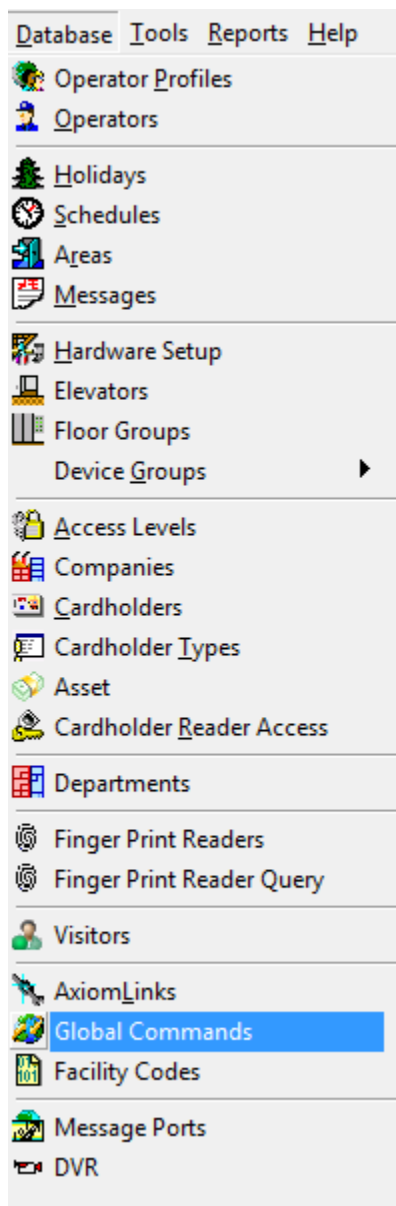
Counter Value: 0

ON Schedule: 0 ...

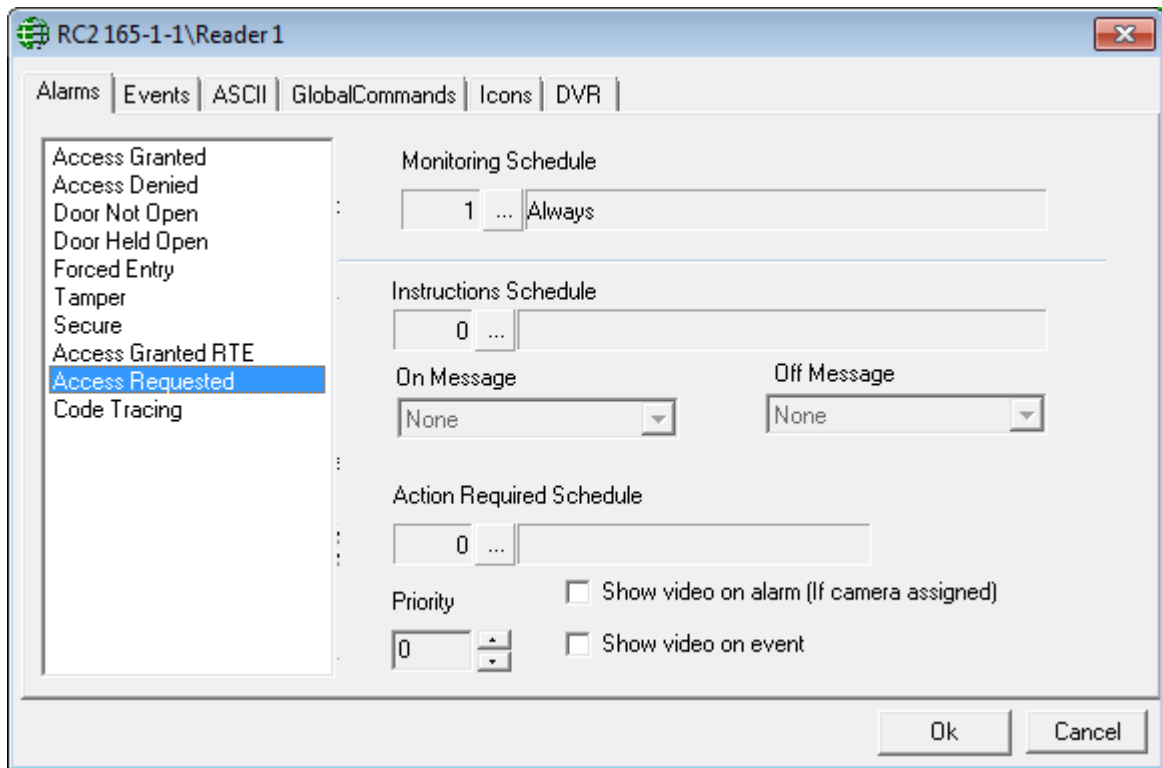
☒ Enabled

OK Cancel

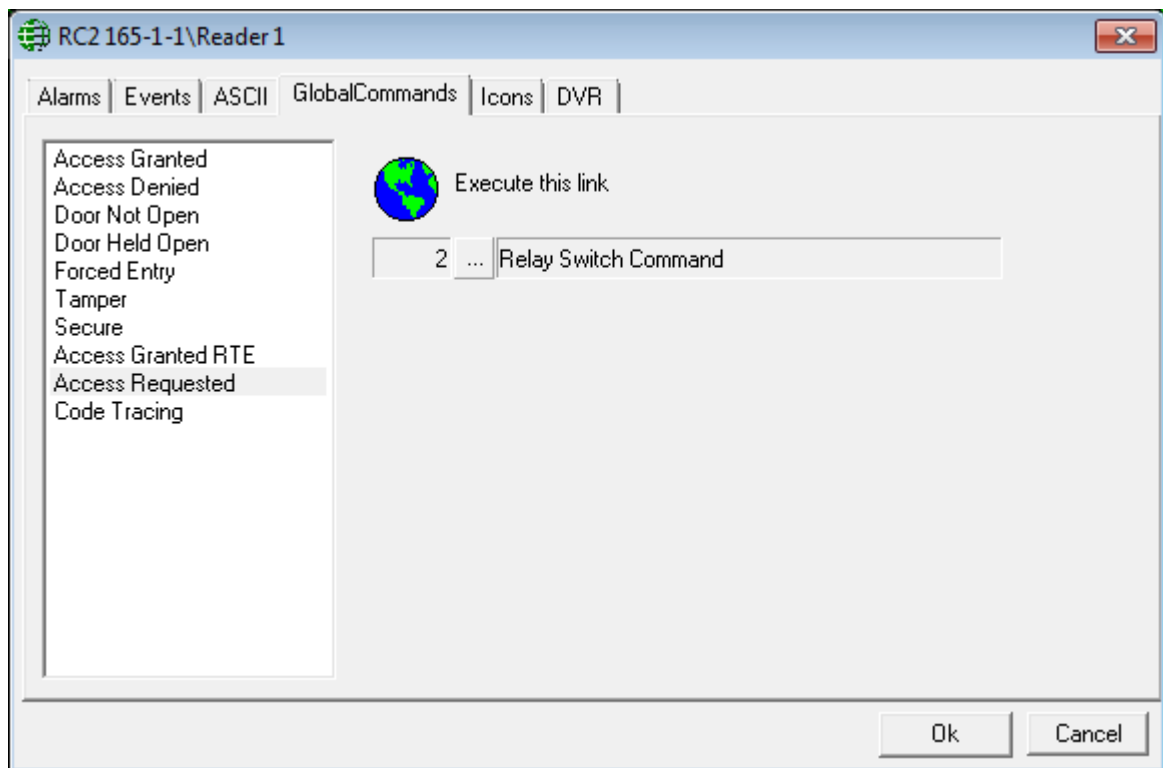
- Click on *Database* and select *Global Commands* .



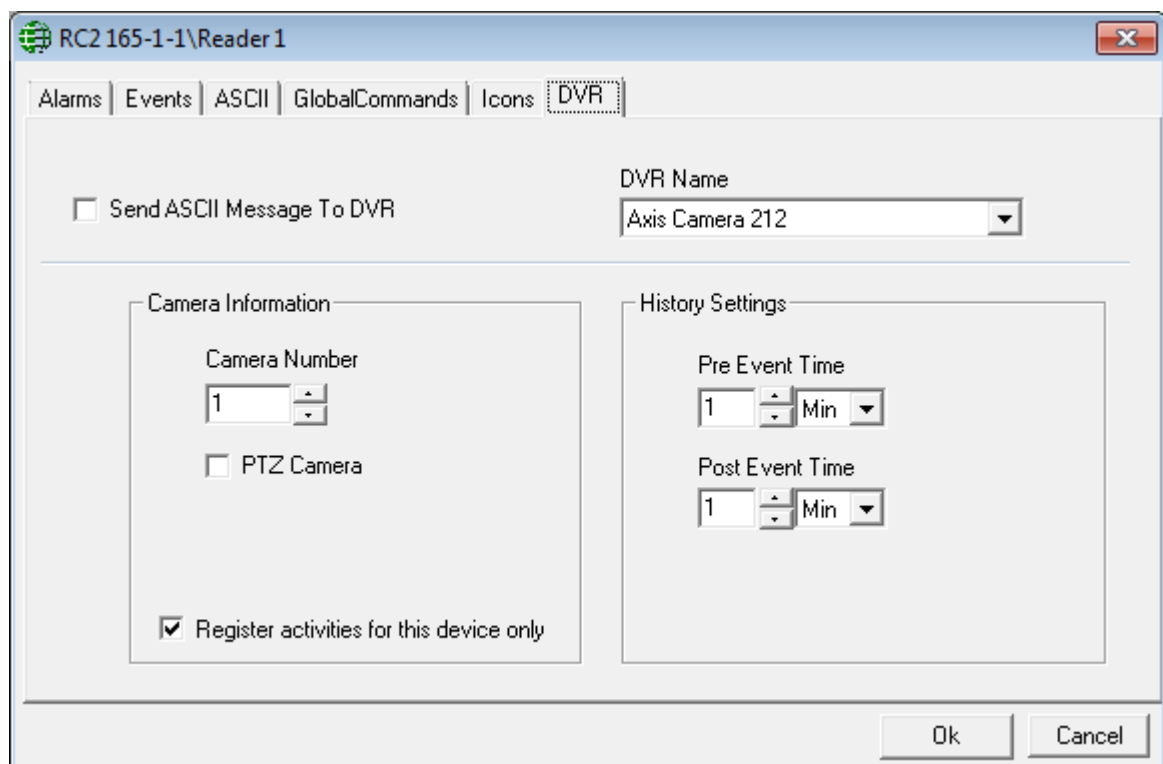
- Configure the *Global Command* as shown below.



- Click on the *Alarms Tab* and select *Access Requested*. In the *Monitoring Schedule* select *Always*.
- Assign the *Global Command* configured to the *Access Requested* event.



- Click on the *DVR Tab*.



- Select the desired DVR from the *DVR Name* drop down box and select the desired camera number from the *Camera Number* text box.
- Check the *Register activities for this device only* (**This option is available only for Access points and not for inputs and output monitoring**) and click *Ok*.
- Click on *Monitoring* for side B reader of the same RC2, and configure the same DVR information in the DVR tab of this reader.

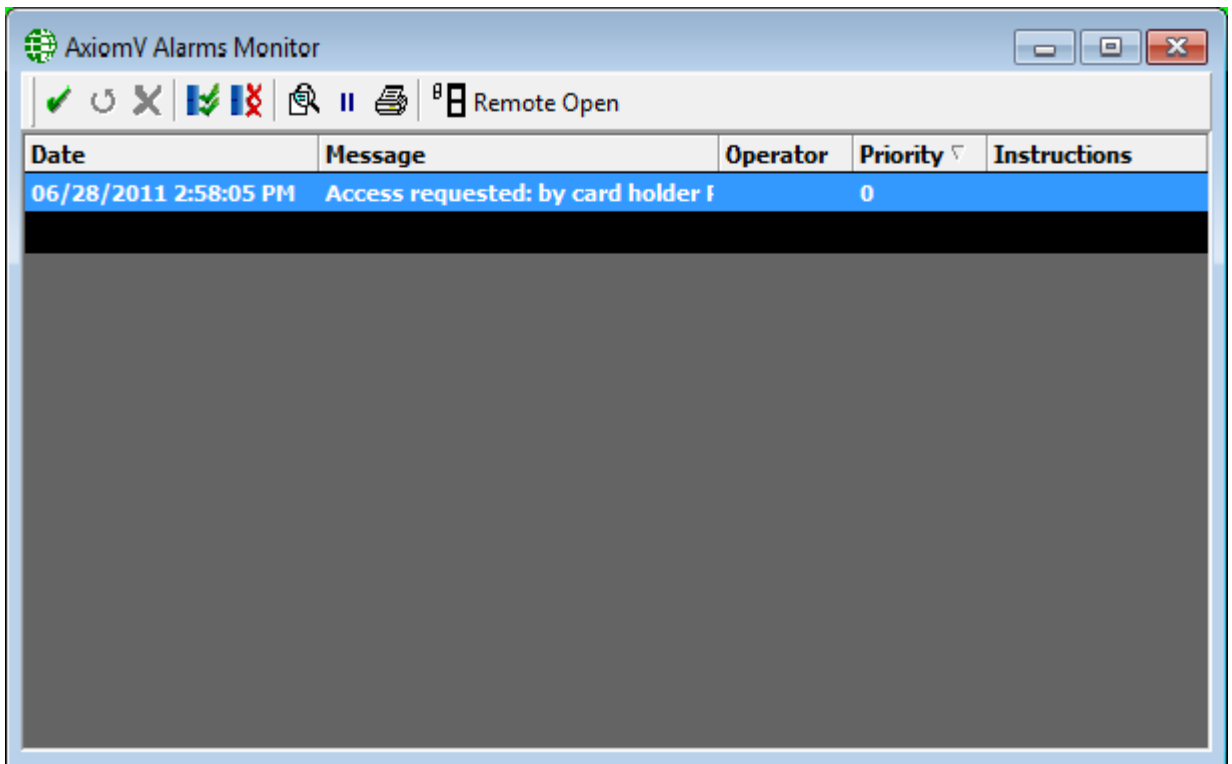
The screenshot shows a software window titled "RC2 165-1-1\Reader 2" with a tabbed interface. The "DVR" tab is selected. The window contains the following elements:

- Alarms | Events | ASCII | GlobalCommands | Icons | DVR** (tabbed menu)
- ☐ Send ASCII Message To DVR
- DVR Name: **Axis Camera 212** (dropdown menu)
- Camera Information** (group box):
 - Camera Number: **1** (spin box)
 - ☐ PTZ Camera
 - ☒ Register activities for this device only
- History Settings** (group box):
 - Pre Event Time: **1** (spin box) **Min** (dropdown)
 - Post Event Time: **1** (spin box) **Min** (dropdown)
- Ok** and **Cancel** buttons at the bottom right.

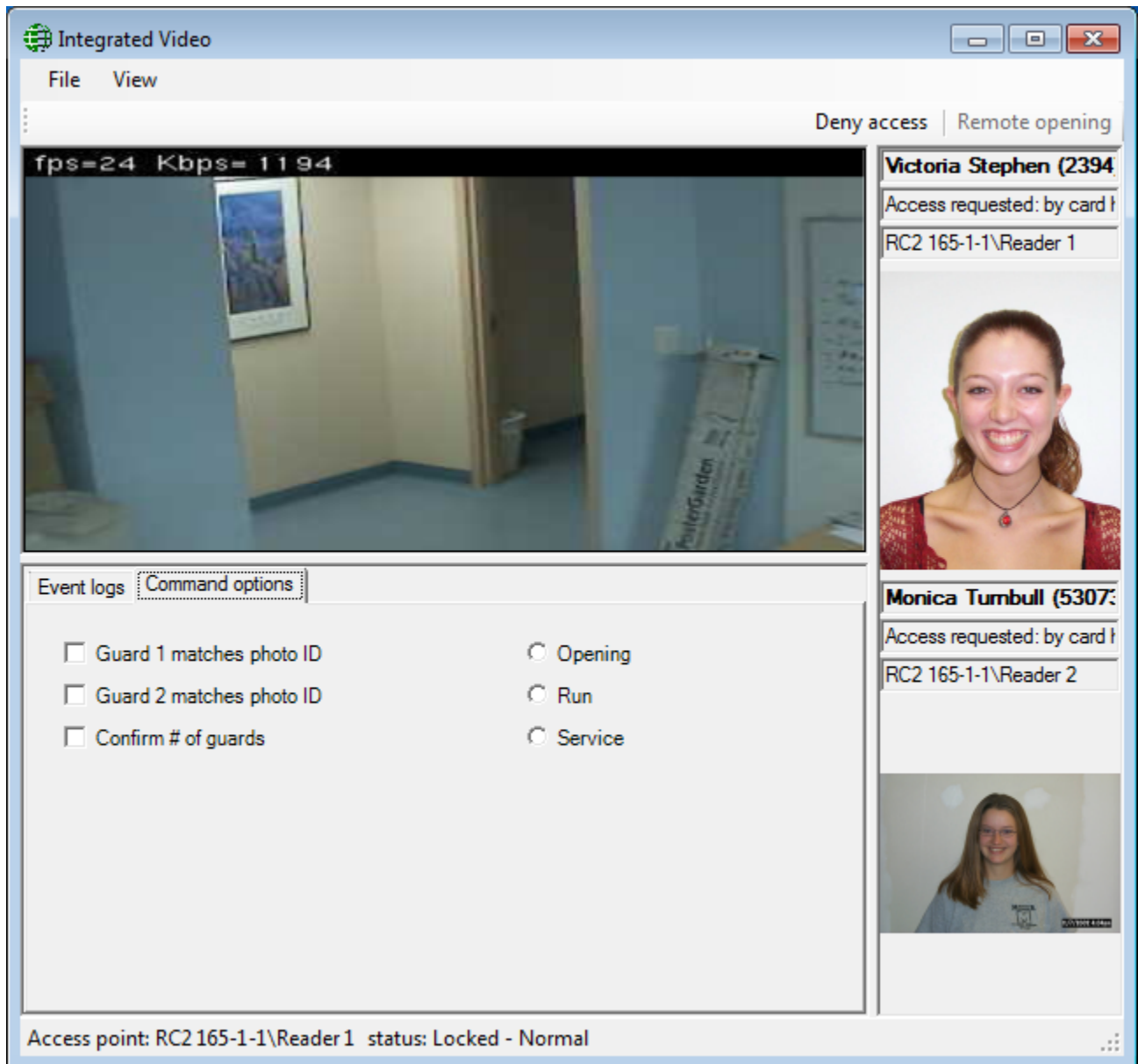
Alarm Monitoring Procedure

The Alarm Monitoring Procedures are as follows.

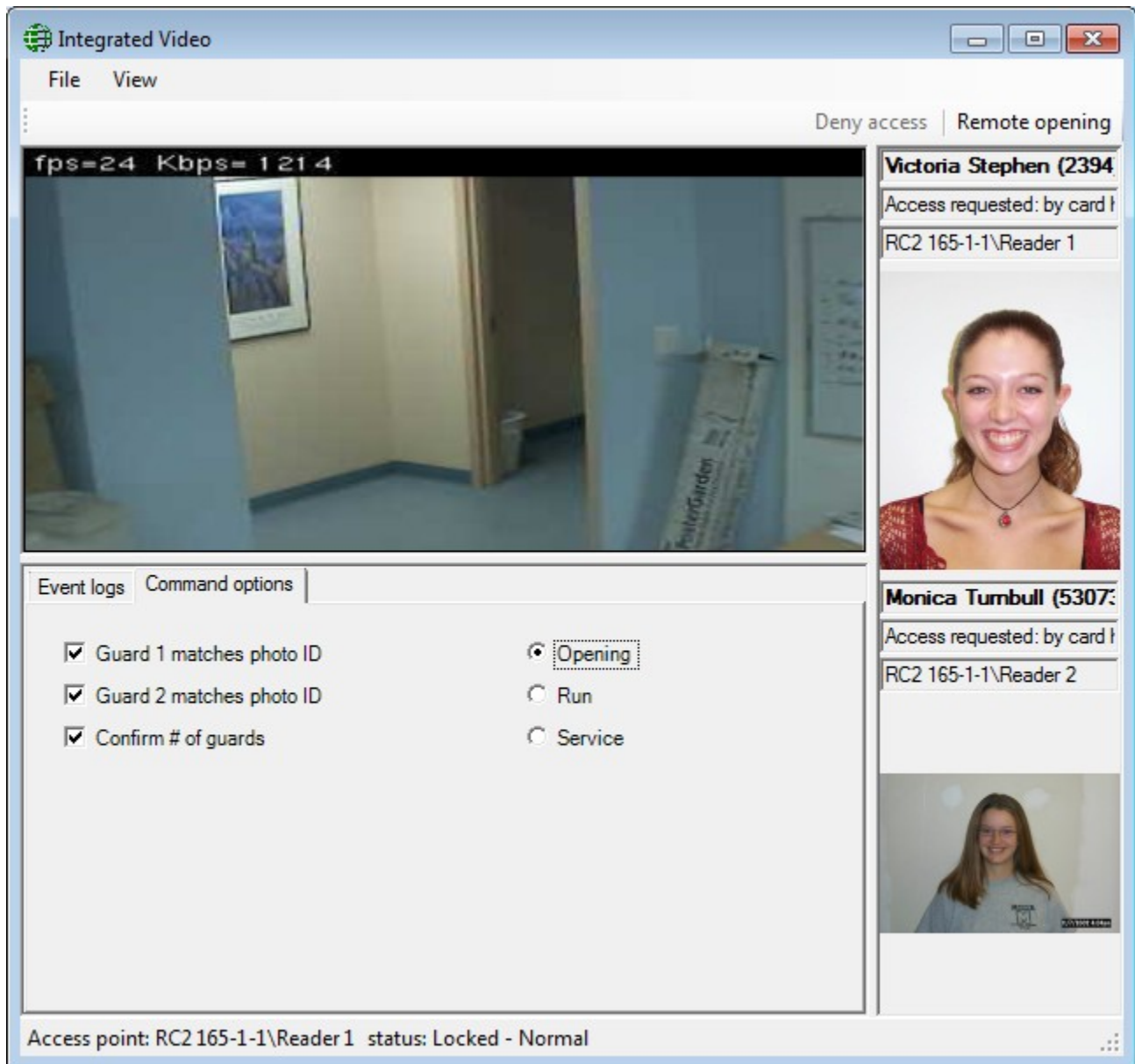
- Both cardholders swipe the same card reader (side A) that brings up the alarm in the *Alarm Monitor window* and an alarm sounds.



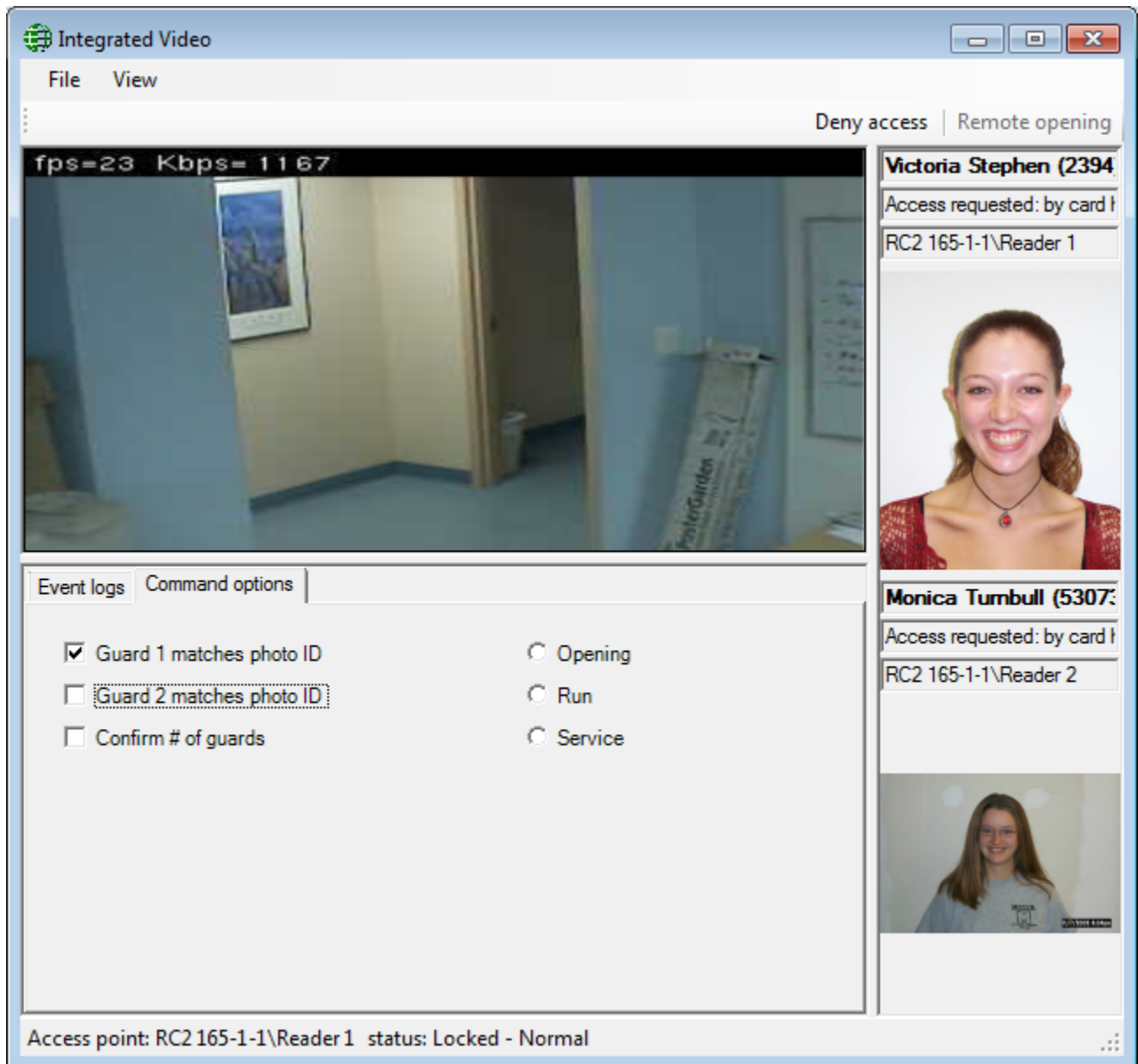
- The operator clicks on the *Remote Open* button on toolbar or Right click on Alarm and select *Remote Open* option (**Right click option on Alarm is available only for Access requested messages if Centralized option is enabled in system settings**) which brings up the *Integrated Video* form and **acknowledges alarm** in alarm monitor.



- The video is displayed and both pictures of the cardholders are displayed as well.
- The operator checks the video and accordingly selects *Guard 1 matches photo ID* and *Guard 2 matches photo ID* and *Confirm # of guards* in *Command Option* tab of *Integrated Video* form



- The operator checks one of the settings on right hand side *Opening/Run/Service* and the *Remote opening* option is enabled.
- The operator clicks on the *Remote opening* button to grants access to the cardholders and open the door requested. This command also closes the *Integrated video form* and *clears* that alarm from Alarm Monitor
- If the Operator doesn't select all the required options in *Command Option* tab, since the operator is not satisfied with what they sees on video, they'll click on *Deny access*, which would bring up alarm detail window to write remarks about why the operator needed to *Deny access*.



Copyright Notice

Copyright © 1995 - 2011 by RBH Access Technologies Inc.

All rights reserved Worldwide. Printed in Canada. This publication has been provided pursuant to an agreement containing restrictions on its use. No part of this book may be copied or distributed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, manual, or otherwise, or disclosed to third parties without the express written consent of RBH Access Technologies Inc., Mississauga, Ontario, Canada.

Trademark

AxiomV™ is a trademark of RBH Access Technologies Inc. Windows is a trademark of Microsoft Corporation. All other product names mentioned herein are the property of their respective owners. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Disclaimer

This book is provided *as is*, without warranty of any kind, either express or implied, including but not limited to performance, merchantability, or fitness for any particular purpose. Neither RBH Access Technologies Inc. nor its dealers or distributors shall be liable to any person or entity with respect to any liability, loss, or damage, caused, or alleged to have been caused directly or indirectly by this information. Further RBH Access Technologies Inc. reserves the right to revise this publication, and to make changes to the content hereof from time to time, without the obligation of RBH Access Technologies Inc. to notify any person or organization of such revision or changes.

RBH ACCESS TECHNOLOGIES INC.

2 Automatic Road, Suite 108
Brampton, Ontario
CANADA
L6S 6K8

Printing Date 28 October, 2011

License & Warranty

Notice 1.01

This Software is licensed (*not sold*). It is licensed to sublicensees, including end-users, without either express or implied warranties of any kind on an “as is” basis. RBH Access Technologies Inc. makes no express or implied warranties to sublicensees, including end-users, with regard to this software, including merchantability, fitness for any purpose or non-infringement of patents, copyrights, or any other proprietary rights of others. RBH Access Technologies Inc. shall not have any liability or responsibility to sublicensees, including end-users for damages of any kind, including special, indirect or consequential damages arising out of or resulting from any program, services or materials made available hereunder or the or the modification thereof.

Notice 1.02

RBH Access Technologies Inc. makes no claim or warranty with respect to the fitness of any product or software for a specific application and assumes no responsibility for installation. This warranty is in lieu of all other warranties expressed or implied. No representative or agent of RBH Access Technologies Inc. may make any other claims to the fitness of any product for any application.