

Continental Access

A Napco Security Group Company



CA3000 V2.7.x FUNCTIONAL TECH NOTES

FEATURE EXPLAINED:

Threat Level Management

Doc # FTN0004

REVISION A

DATE: 3/26/2010

CardAccess® 3000 



CA3000 Functional Tech Notes

Continental Access and CardAccess3000 are registered trademarks of Napco Security Technologies
Microsoft® is a registered trademark of Microsoft Corporation.
Windows® is a registered trademark of Microsoft Corporation.
CardAccess® is a registered trademark of Napco Security Technologies

Document Title: CA3000 V2.7.x Functional Tech Notes (FTN0004)

This document contains proprietary information of Continental Access. Unauthorized reproduction of any portion of this manual without the written authorization of Continental Access is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. Continental Access assumes no responsibility for incorrect information this manual may contain.

Continental Access
355 Bayview Avenue
Amityville, NY 11701
Phone (631) 842-9400
Fax (631) 842-9135

Web: <http://www.cicaccess.com>

Important Information - Must be read before programming software.

- 1) This functional Tech Note will provide you with a basic summary of the advanced feature noted on the cover page. In some cases, you must customize the feature for your specific application.
- 2) Before programming any advanced features, verify all the basic components of CA3000 are programmed. Verify the CardAccess 3000 software is functioning properly (refer to the V2.7 Quick Start Programming Guide).
- 3) If possible, always refer to the Continental Access website (www.cicaccess.com click Support/click Document Library) for the latest documentation. The released CD may not have the most recent documentation.
- 4) Panels must be running firmware version 3.x or higher for the ability to use advanced features.
- 5) The document is written for V2.7.x. Do not reference this document for V2.6.x. The functionality of threat level management has changed from V2.6 to V2.7.

Threat Level Management

This feature provides you with five states of threat level management. It enables managers to more quickly react to present threats, by instantly deactivating access privileges via a mouse click.

Configuring threat level management

Follow the steps below:

- 1) On the main menu, click System/System Settings. Refer to figure 1.



Figure 1.

2) Click the Badges tab. Enable Category Counters. Refer to figure 2.

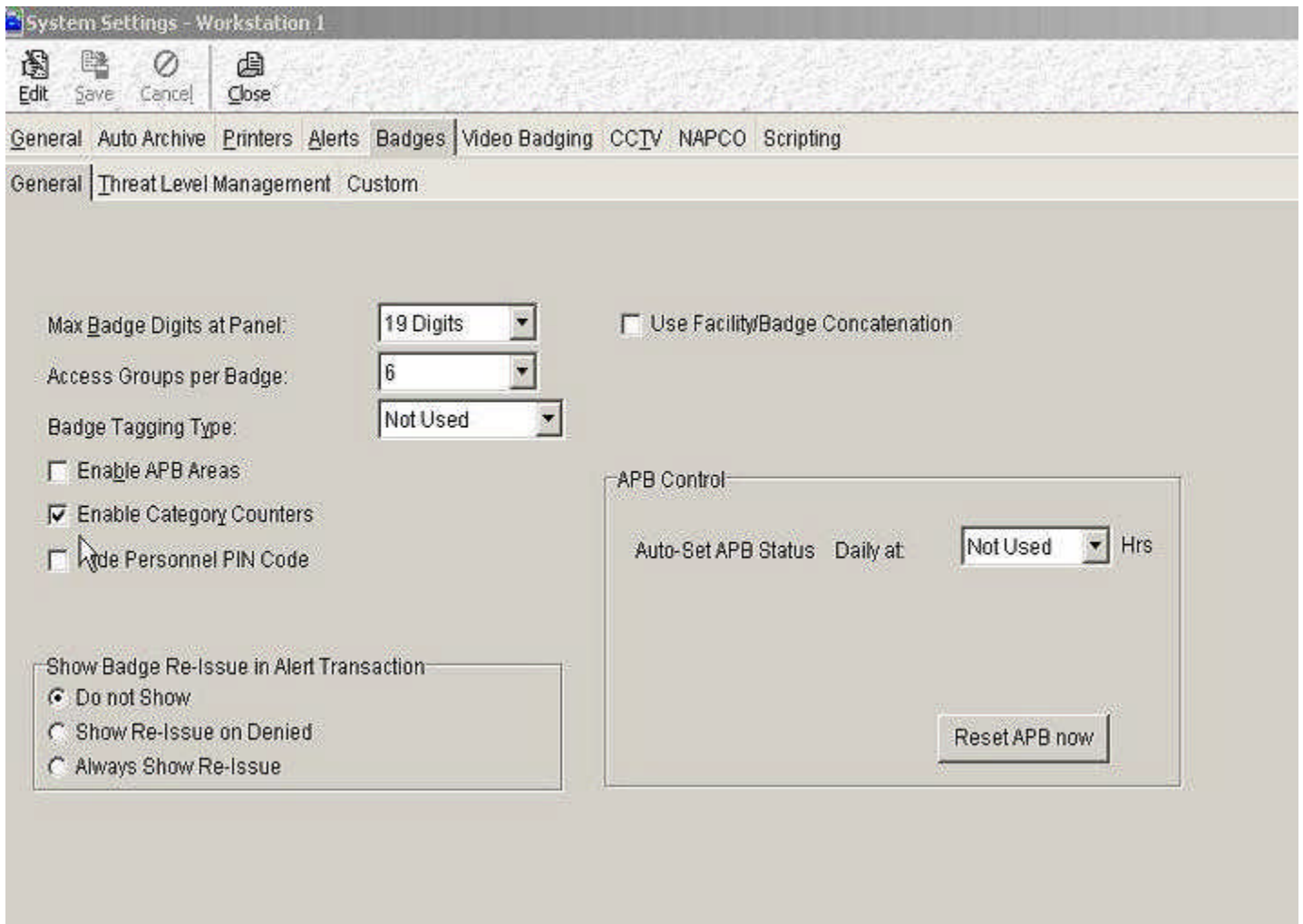


Figure 2.

3) Click the Threat Level Management tab. Refer to figure 3.

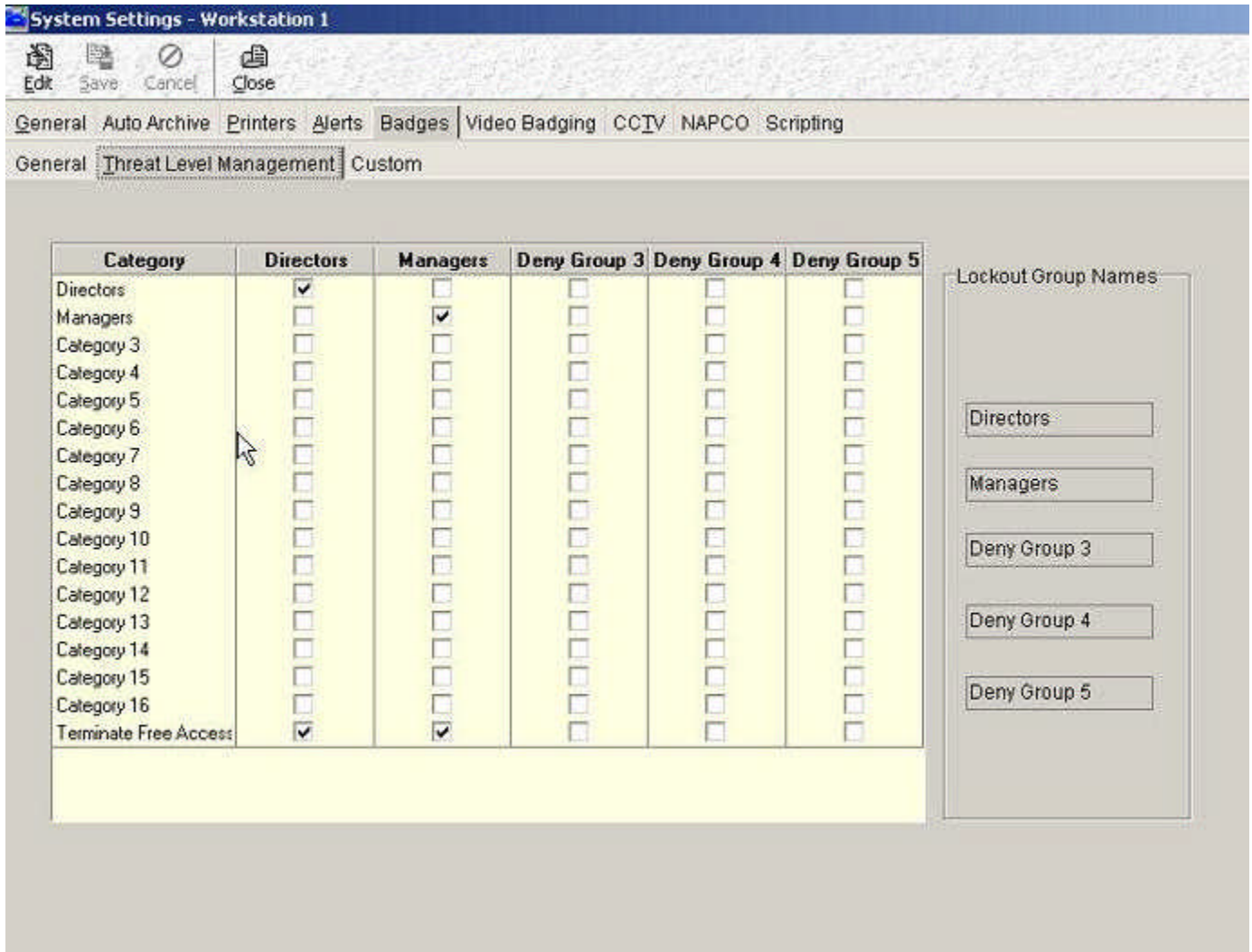


Figure 3.

4) Configure the Threat Level Management screen as per figure 3. As previously noted, you have five states of threat level management. We will only use two levels for our example. Click Edit and change the Lockout Group Names. Change Deny Group 1 to Directors. Change Deny Group 2 to Managers. Under the Category column, rename Category 1 to Directors and Category 2 to Managers. Select Terminate Free Access for both groups. After all the changes are made, click Save and Close.

CREATING BADGES AND CONFIGURING CATEGORY COUNTER ASSIGNMENTS (refer to step 5)

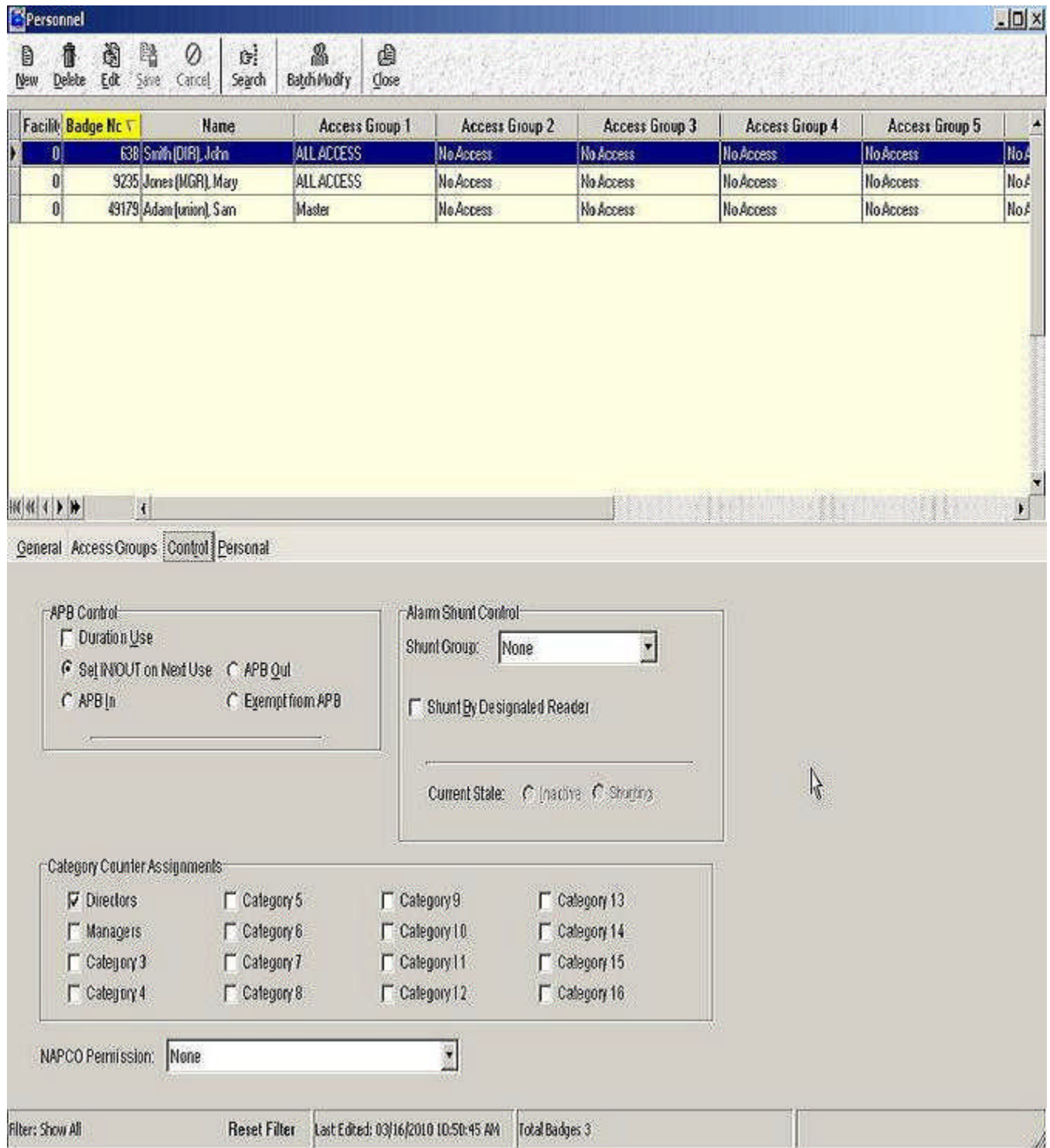


Figure 4.

Personnel

New Delete Edit Save Cancel Search Batch Modify Close

Facility	Badge No	Name	Access Group 1	Access Group 2	Access Group 3	Access Group 4	Access Group 5
0	638	Smith (DIR), John	ALL ACCESS	No Access	No Access	No Access	No Access
0	9235	Jones (MGR), Mary	ALL ACCESS	No Access	No Access	No Access	No Access
0	49179	Adams (Senior), Sam	Master	No Access	No Access	No Access	No Access

General Access Groups Control Personal

APB Control

Duration Use

Set IN/OUT on Next Use APB Out

APB In Exempt from APB

Alarm Shunt Control

Shunt Group:

Shunt By Designated Reader

Current State: Inactive Shunting

Category Counter Assignments

Directors Category 5 Category 9 Category 13

Managers Category 6 Category 10 Category 14

Category 3 Category 7 Category 11 Category 15

Category 4 Category 8 Category 12 Category 16

NAPCO Permission:

Filter: Show All Reset Filter Last Edited: 03/16/2010 11:11:37 AM Total Badges 3

Figure 5.

- 5) For this example, configure a total of three badges. Configure the first badge with a category of Directors (refer to figure 4). Create the second badge with a category of Managers (refer to figure 5). Create one badge without category assignments.

TESTING BADGES PRIOR TO ACTIVATING THREAT LEVEL LOCKOUT

- 6) Swipe the three badges at a reader and verify all three badges display Badge Valid (refer to figure 6). Swipe the badge with the Directors category first. Swipe the badge with the Managers category second and then the badge with no categories third.

BADGE VALID	Smith (DIR), John	1-1 Panel1 Reader 1	3/23/2010 8:39:11 AM	Auto-Acked	3/23/2010 8:39:11 AM
BADGE VALID	Jones (MGR), May	1-1 Panel1 Reader 1	3/23/2010 8:39:19 AM	Auto-Acked	3/23/2010 8:39:18 AM
BADGE VALID	Adam (unior), Sam	1-1 Panel1 Reader 1	3/23/2010 8:39:23 AM	Auto-Acked	3/23/2010 8:39:23 AM

Figure 6.

ACTIVATING THREAT LEVEL MANAGEMENT

VERY IMPORTANT: Only one threat level can be activated at any time. If you activate a threat level, any other threat level that is activated, will be deactivated.



- Padlock represents threat level is not activated.



- Key represents threat level is activated.

7) Click Lockdown Control/Threat Level Control. Before activating, verify the Directors group is currently not activated (padlock displayed). Refer to figure 7. Click Activate: Directors.



Figure 7.

8) A confirmation screen will display. Refer to figure 8. Click OK.



Figure 8.

Verify the Directors group was successfully activated (Key displayed). Refer to figure 9.

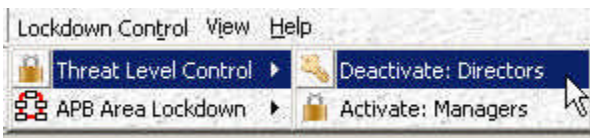


Figure 9.

After the Threat Level is activated, a system alert will display. Refer to figure 10.

SYSTEM	Threat level Activated	Threat Level 1	3/16/2010 11:27:00 AM	Admin	3/16/2010 11:27:11 AM
--------	------------------------	----------------	-----------------------	-------	-----------------------

Figure 10.

VERY IMPORTANT: If Free Access is active on any readers, Free Access will End.

TESTING THREAT LEVEL LOCKOUT

- 9) Swipe the badges again in the order noted above. Verify the Directors badge displays Badge Valid. Verify the other two badges display Badge Violate Lockout. Refer to figure 11.

BADGE VALID	Smith (DIR), John	1-1 Panel 1 Reader 1	3/23/2010 8:44:47 AM	Auto-Acked	3/23/2010 8:44:47 AM
BADGE VIOLATE LOCKOUT	Jones (MGR), Mary	1-1 Panel 1 Reader 1	3/23/2010 8:45:03 AM	Un-Acked	3/23/2010 8:45:15 AM
BADGE VIOLATE LOCKOUT	Adam (union), Sam	1-1 Panel 1 Reader 1	3/23/2010 8:45:17 AM	Un-Acked	3/23/2010 8:45:29 AM

Figure 11.

Note: The only badges that will gain access is the badge with the Directors category assigned to it.

DEACTIVATING AN ACTIVATED THREAT LEVEL

10) Click Lockdown Control/Threat level Control. Click Deactivate: Directors. Refer to figure 12.



Figure 12.

A confirmation screen will display. Refer to figure 13. Click OK.



Figure 13.

After the Lockdown is deactivated, a system alert will display. Refer to figure 14.



Figure 14.

VERY IMPORTANT: If Free Access was previously ended by activating a threat level, Free Access will start again.

11) After the threat level is deactivated, swipe all three badges in the same order again. All three badges should gain access again and display Badge Valid.

This completes the Threat Level Lockdown function.