CCM/CCMx Version 7.6.01 Release Notes

 Updated on April 6, 2018.

Overview

This document describes the changes in the CCM and CCMx firmware since version 7.5.70. To make it easier for you to find information about the things that apply to your system, this document has the following structure:

Like previous versions numbered 7.5.X, version 7.6.01 of the CCM/CCMx firmware works on the traditional CCM7 module used in controllers such as the M2 and the M8, and on the newer CCMx-2, CCMx-4, and CCMx-8 modules used in the Mx controller. It also works on the CCMx components built into the main board of the Mx-1 single-door controller.

This firmware package includes both a CCM BIOS component (for all controllers) and a STM-RTC component (for Mx controllers). The version numbers of these software components (for some recent releases) are shown in the following table:

CCM\CCMx version	CCM BIOS version	STM-RTC version
7.6.01.13	**7.5.75**	**6.0**
7.5.70.12	7.5.66	5.5
7.5.64.95	7.5.65	4.6
7.5.61	7.5.28	4.4
7.5.37	7.5.28	4.0
7.5.36	7.5.28	4.0
7.5.28	7.5.28	4.0
7.5.08	7.5.08	3.0

CAUTION: If you have an Mx controller running a CCMx firmware version earlier than 7.5.08, you must first upgrade to version 7.5.08 before you download version 7.6.01 to that controller. Downloading version 7.6.01 to an Mx controller running CCMx firmware version earlier than 7.5.08 will lock up that controller.

NOTE: Version 7.5.X or later of the CCM firmware is only supported by the Velocity security management system, or version 3.0 (or later) of the Identiv Connected Physical Access Manager (ICPAM). It is not supported by previous software products such as MOMENTUM or SAM.

New Features

This section lists the new features and enhancements introduced in this release.

New Features related to TS Readers (in general)

This section lists the new features and enhancements which are related to Identiv's TS readers, regardless of which communications interface they use. (For information about the new features which are related to readers that use the RS-485/OSDP interface, see the next section.)

DT-409: Support for Code Tamper on TS, via J-record 35 subtype 11

DT-451: Defining and Implementing J records for "Green/Red/Yellow LED Always ON" Feature

FAL-1003: Support for annunciator function in TS through SNIB3

FAL-1009: Support for sending the silent mode option to the TS SP

New Features related to RS-485/OSDP Readers

This section lists the new features and enhancements which are related to readers that use the RS-485/OSDP interface, such as Identiv's uTrust TS Government readers or Veridt's Stealth Bio or Stealth Dual readers. (For information about the new features which are related to Identiv's TS readers regardless of which communications interface they use, see the previous section.)

DT-327: Use Keypad numeric LEDs as annunciator on the TS-SP

DT-328: Support for the TS SP's LEDs over OSDP
DT-372: Support Numeric indications on OSDP Keypads/Readers
PAC-164: DT shall report all reader/keypad-related events and changes to FAL via J-records

DT-381: OSDP reader in programming mode has display scrambled.

FAL-1007: Support for the TS ScramblePad's LEDs over OSDP

PAC-144: Support Granted/Denied indications on OSDP TS Keypads/Readers
PAC-220: Support Numeric Programming indications on OSDP TS Keypads/Readers

PAC-179: Support Annunciator indications on OSDP Keypads/Readers

PAC-180: Accept programming codes from the TS-SP and other Wiegand Keypads

New Features related to the Mx-1 Controller

This section lists the new features and enhancements which are related to Identiv's single-door Mx-1 controller.

Detailed information about that controller is provided in the **Mx-1 Controller** chapter in Revision AG (dated January 17, 2018) or later of the ***DIGI*TRAC Systems Design & Installation Guide***. An overview is provided in the "DIGI*TRAC Hardware Configuration > Controllers > **Mx-1 Controller**" topic of Velocity's online help system.

DT-257: Support for Mx-1
VEL-4004: Support Mx-1

DT-361: Support Mx-1 col. 5 Alarm Status LEDs

DT-362: Support Mx-1 col. 4 Relay Status LEDs

MX-67: Support for Wiegand2 port in Mx-1

MX-126: Alarm relay was NOT turned ON for general, duress, tamper, and trouble alarms
MX-127: On Mx-1, Relay 2 is one of the alarm relays

PAC-90: Feature to detect memory battery absence

PAC-391: Mx-1: On powering the controller by PoE+, message stating 'AC power fail at controller' was displayed in Velocity's Event Viewer

New Features related to LED Behavior (during POST)

This section lists the new features and enhancements which are related to the behavior of a controller's LEDs during the Power On System Test (POST).

DT-290: Support Mx-1 status LEDs
MX-68: Support for new LED behaviour in Mx-1

DT-368: Fine-tune the "Xmas Tree" LEDs for multi-door controllers
DT-374: Rewrite FLASH BIOS POST LED Patterns

As previously documented in the CCM 7.5.70 Release Notes, for a controller equipped with a SNIB2 or a SNIB3, the behavior of its **SYS** and **NET** status LEDs was enhanced in the CCM 7.5.64 firmware release to show when a download is in progress or when there is network activity. In the 7.5.70 release, some additional changes to the behavior of some status LEDs were made. In particular, note that the "Controller is OK" state is now indicated by a **blinking** green SYS LED, instead of the previous solid green SYS LED.

The new meanings of all the controller status LEDs are explained in the following table.

Name and Purpose of row of status LEDs	Meaning of First LED	Meaning of Second LED
BOX TAMPER = Enclosure Tamper or Reader Tamper	ON = Enclosure Tamper	ON = Reader Tamper
AC = AC Power	ON = AC Power is OK	ON = AC Power Failure
	Both LEDs BLINKING = AC Power is Low (or Mx-1 controller is using Power over Ethernet+)	
BAT = Standby Battery	ON = Battery is OK (at 24V – 28V)	ON = Battery Failure (less than 21V)
	Both LEDs BLINKING = Battery is Low (at 21V – 23V); if AC Power is available, the Battery is Charging	
SYS = Controller's Status	**BLINKING** (and second LED is OFF) = Controller is OK	ON (and first LED is OFF) = Controller Failure
KPD = Controller's communication with all of its connected readers	Flash = Controller is sending data to one of its connected readers	Flash = Controller is receiving data from one of its connected readers
NET = Controller's communication with the Velocity Server	ON = Transmitting an event to the Velocity Server Flash = Transmitting some other message to the Velocity Server	ON = Receiving credentials Flash = Receiving configuration or other commands
TEST = Door Alarm or Controller's Power-On Self Test	ON = A door is in an alarm state SLOW BLINKING = A door is held open too long FAST BLINKING = Controller is running its Power-On Self Test	(no second LED on this row)
ALARM = Line Fault Alarm	ON = A fault condition (Out Of Spec, Open, Short, or Noisy) exists on the supervised line input for a door	(no second LED on this row)

PAC-145: Cleanup and document the POST light patterns

Other New Features

This section lists all of the other new features and enhancements which are not covered in one of the previous sections.

DT-92: Disable State Change Reporting when input is masked
PAC-155: Disable State Change Reporting when input is masked

In Velocity 3.6 SP3, the "**Disable state change reporting when masked as default for new controllers**" option was added in the Miscellaneous group on the General page of the Velocity Preferences dialog. Check this box to specify that when new controllers are added to your Velocity system, by default the state change reporting is disabled when their inputs and expansion inputs are masked. (This option can significantly reduce the message traffic at large sites with many controllers and doors.).

For more information, see the "Velocity Basics > Velocity Preferences > **Preferences dialog - General page**" topic in Velocity's online help system.

DT-405: Inhibit reporting of expired credentials

DT-417: Support disabling readers

In Velocity 3.6 SP3, the **Setup** page of the properties dialog for a door's reader includes a new **Disabled** value for the Reader Interface option. This value means there is no reader attached at this address. For more information, see the "DIGI*TRAC Hardware Configuration > Readers and Keypads > **Reader Properties - Setup (or General) page**" topic in Velocity's online help system.

DT-458: Display SNIB3 vn. on ***2 status request.

For a controller with a SNIB3 communications expansion board (or an Mx-1 controller with the SNIB3 functionality built onto the main board), the status request ***2 displays the version of the SNIB3 firmware.

MX-122: Feature to detect STM reset and resend reader configuration

PAC-269: Write up key for '9022' Database Correction Performed messages.

Messages related to the Database Maintenance feature appear in Velocity's Event Viewer window with an Event ID value of 9022. The following table provides information about those messages.

Message category	Event message text	Notes
12, 12XX	PZ Occupancy count was incorrect	Could have resulted in incorrect min/max occupancy behavior. Messages 1202-1298 just mean that event 12 happened 2 to 98 times. Message 1299 means that event 12 happened at least 99 times.
13, 13XX, 14, 14XX, 15, 15XX	Credential ID key errors	Could have made a credential impossible to list by credential ID number. Re-downloading the credential would not necessarily have fixed the issue.
16, 16XX, 17, 17XX	PIN key errors	Could have made a good PIN be denied for "Invalid CODE". Re-downloading the credential would not necessarily have fixed the issue.
18, 18XX, 19, 19XX	Card key errors	Could have made a good card be denied for "Invalid CODE". Re-downloading the credential would not necessarily have fixed the issue.
20, 20XX	Credential ID key errors	Could have made a credential impossible to list by credential ID number. Re-downloading the credential would not necessarily have fixed the issue.
21, 21XX	PIN key errors	Could have made a good PIN be denied for "Invalid CODE". Re-downloading the credential would not necessarily have fixed the issue.
22, 22XX	Card key errors	Could have made a good card be denied for "Invalid CODE". Re-downloading the credential would not necessarily have fixed the issue.
23, 23XX	Credential ID key errors (two records with same credential ID number)	Could have made a credential impossible to list by credential ID number. Re-downloading the credential would not necessarily have fixed the issue.
24, 24XX	Corrupted credential record	Could have made a good credential not work. Re-downloading the credential might have fixed it.
25, 25XX	Total Credential Count was incorrect	Could have made the "Total users" report the wrong number. Re-downloading credentials would not necessarily have fixed the issue.

Message category	Event message text	Notes
42, 42XX	Key bucket was marked as “sorted” but was not in sequence	Could have made some credentials unfindable. Re-downloading credentials would not necessarily have fixed the issue.
43, 43XX, 44, 44XX, 46, 46XX	Key bucket header min, max were misidentified	Could have made some credentials unfindable. Re-downloading credentials would not necessarily have fixed the issue.
45, 45XX	Eliminated empty bucket	Could have made downloading credentials impossible even though there was fewer than the maximum credentials in the controller.
46, 46XX	Key bucket header min, max were misidentified	Could have made some credentials unfindable. Re-downloading credentials would not necessarily have fixed the issue.
47, 47XX	Deallocate unused credential page	Could have made downloading credentials impossible even though there was fewer than the maximum credentials in the controller.
80, 80XX	Credential ID bucket defrag	Harmless.
81, 81XX	PIN key bucket defrag	Harmless.
82, 82XX	Card key bucket defrag	Harmless.
83, 83XX	Deleted/available record chain defrag	Harmless.
84, 84XX	Deleting expired records	Harmless.
85, 85XX, 86, 86XX	Key bucket was sorted, but not marked as such	Harmless. (Marking the in-sequence key buckets enables slightly faster lookups.)
87, 87XX, 88 88XX	Deallocating unused credential page	Harmless. (Although it's possible that a not-full database reported errors when trying to add credentials.)

Enhanced Control of Escorted Visitors

DT-373: Support for Visitor Mode Indications on OSDP Keypads/Readers

DT-385: Visitor/Escort Rule using Vn.7 CCM

DT-443: End Escort mode j record is not sent within 1 minute after start of Escort mode

DT-444: On starting an escort mode, the visitors expected count and reader number are incorrect

DT-448: Escort mode is entered though “Escort First” option is disabled

DT-452: For an unescorted visitor, Error message states as unknown credential ID, instead of User Name

DT-453: On entering PIN of an escort, when “Escort Toggle Mode” is enabled, 0 is displayed as visitor count expected

DT-454: On disabling “Escort Required” option and entering PIN of escort with visitor count, Invalid extension message is not displayed in Velocity

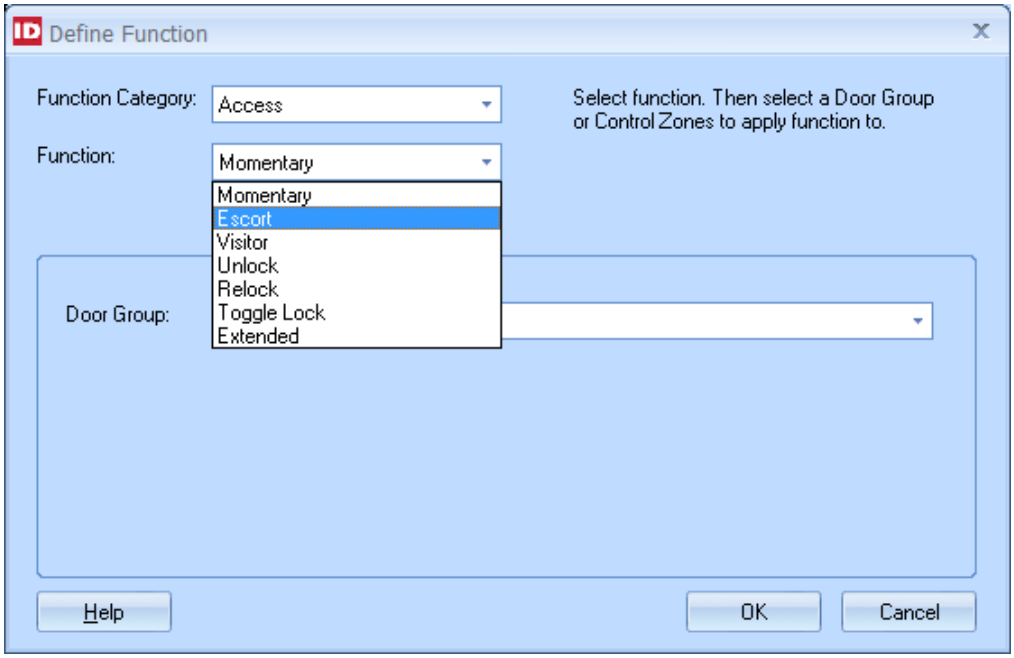
DT-455: On disabling "Escort Toggle” mode and entering the escort PIN with number of visitors, countdown of visitors does not start.

DT-457: On entering PIN of an Visitor, who waits for an Escort, Access Denied LED and Buzzer is seen

PAC-142: Falcon Application restarts on visitor access, followed by a momentary door access.

PAC-174: Visitor Mode LED Indications is not happening for On Board Wiegand Interface with TS Keypad reader

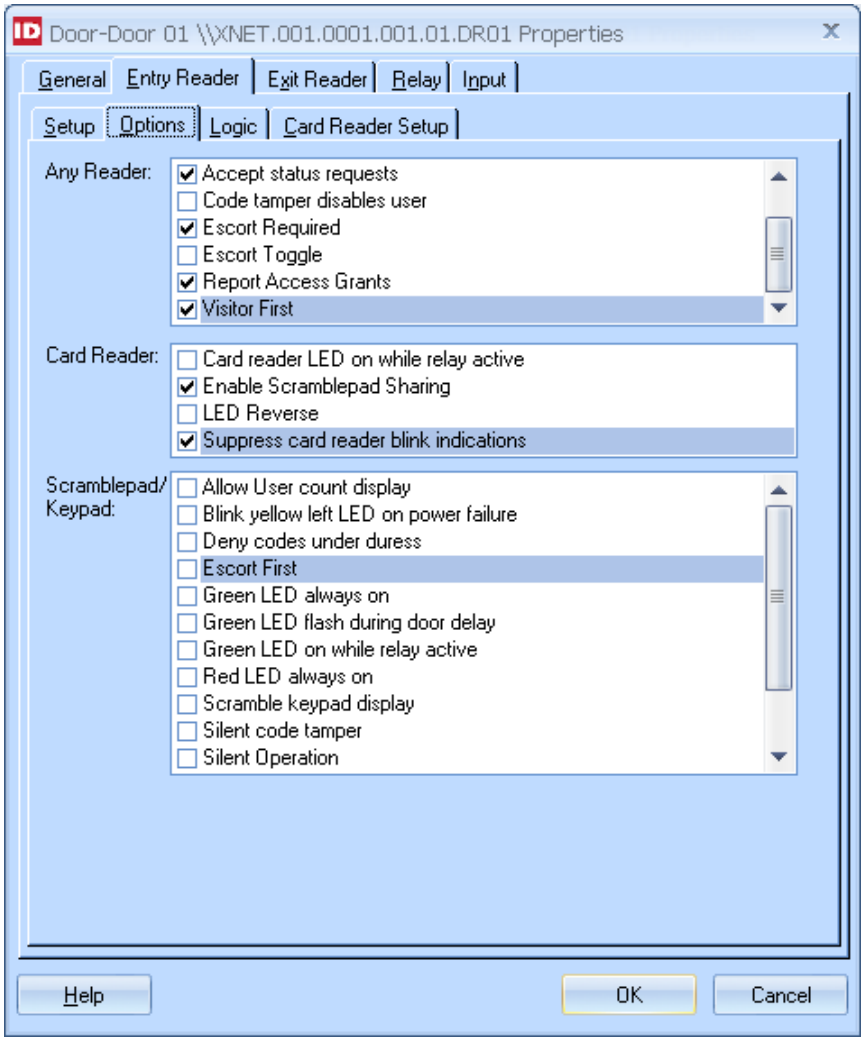
To help you better manage access control for escorted visitors, Velocity 3.6 SP3 includes the Access functions of **Escort** and **Visitor**, which enable you to create specialized credentials such as Tour Guide and Visitor badges. (If none of the three Escorted Visitors modes is in effect, the Escort and Visitor access functions are equivalent to Momentary access.)



The priority of these new Access functions is shown in the Relay Priority Scheme diagram that appears in the "DIGI*TRAC Hardware Configuration > Functions > Control Functions > **Control Function Priority Levels**" topic in Velocity's online help system.

The properties dialog for a reader now includes four additional checkbox options relating to escorted visitors: **Escort Required**, **Escort Toggle**, **Visitor First**, and **Escort First**.

- **Escort Required**. This option determines whether a Visitor credential can be granted access on its own, or if an Escort credential must also be presented to authorize access.
- **Escort Toggle**. This option determines whether the Escort Toggle mode is in effect. This mode enables an Escort to authorize multiple Visitors at a reader which does not include a keypad.
- **Visitor First**. This option determines whether the Visitor First mode is in effect. (This mode is similar to a 2-Person Executive Rule.)
- **Escort First**. This option determines whether the Escort First mode is in effect. This mode requires an Escort credential with a PIN and a reader with a keypad, because the Escort must type the PIN and the number of Visitors in the group. (A countdown timer on the reader's display helps the Escort determine whether any Visitors have wandered away from the group.)



For more information, see the "DIGI*TRAC Hardware Configuration > Functions > Access Functions > **Access Functions - Escorting Visitors**" topic in Velocity's online help system.

Bug Fixes

This section lists the bug fixes included in this release.

Bug Fixes related to TS Readers (in general)

This section lists the bug fixes which are related to Identiv's TS readers, regardless of which communications interface they use. (For information about the bug fixes which are related to readers that use the RS-485/OSDP interface, see the next section.)

FAL-1177: On enabling the Silent Code Tamper feature, Code Tamper LED blink is not seen in the reader

FAL-1192: On entering into Programming mode, the Yellow LED does not blink in the TS SP reader

PAC-60: TS SP: On removing the default LED colour, the Blue colour LED is not turned ON.

PAC-62: On rebooting the OSDP TS readers, default LED colour selected is lost.

PAC-105: TS SP: On issuing extended access from Exit door, 5 Buzzer beep for end of extended access is not heard.

PAC-146: Extended Access Warning Buzzer is not heard in TS SP readers
FAL-1193: Implement J record handling for extended access warning

PAC-149: Send active V bytes J records to SNIB3 when a reader comes online

Bug Fixes related to RS-485/OSDP Readers

This section lists the bug fixes which are related to readers that use the RS-485/OSDP interface, such as Identiv's uTrust TS Government readers or Veridt's Stealth Bio or Stealth Dual readers. (For information about the bug fixes which are related to Identiv's TS readers regardless of which communications interface they use, see the previous section.)

PAC-173: Numeric program command causes controller to go offline

PAC-228: OSDP Mode: Odd behavior seen when a user opts out of entering a PIN by pressing # for a dual credential

Bug Fixes related to the Mx-1 Controller

This section lists the bug fixes which are related to Identiv's single-door Mx-1 controller. (Detailed information about that controller is provided in the **Mx-1 Controller** chapter in Revision AG (dated January 17, 2018) or later of the ***DIGI*TRAC Systems Design & Installation Guide***.)

DT-392: P7 Amber LED does not remain steady ON when there is a reader tamper

DT-395: Line input Out of Spec, Line Input Noisy conditions are not detected

DT-397: System Information report of Mx-1

DT-400: Mx-1: Transmission errors since midnight report

DT-403: Mx-1: P8 Amber LED does not blink while charging the external battery

DT-404: Mx-1: Battery Charging circuit is always ON

DT-408: Mx-1: System power status report does not show the correct readings for UPS Battery under charge

DT-410: STM ADC configuration should be Mx1-dependent.

DT-428: Mx-1: On connecting DTLM in sense1 port, message stating 'Input 2 is secured' is displayed.

DT-463: Mx-1: On placing an unenrolled card in TS Wiegand reader, feedback LED blink is not seen in the reader

MX-123: After a blue button reset, on configuring OSDP entry and exit readers, Exit reader is reported as Door 5 Reader 13

MX-125: On downloading configurations, Wiegand exit reader is reported as Door 5 reader 5

MX-134: Mx-1 Production CCM not entering programming mode

PAC-79: On downloading configuration from Velocity, OSDP readers 1 to 16 come online

Other Bug Fixes

This section lists all of the other bug fixes which are not covered in one of the previous sections.

DT-9: Mask on an expansion input takes 30 seconds to unmask with an RQE

DT-258: Support clearing out XDAT memory during "Clear Credential Database" Command
DT-376: Support full credential database initialization including XDAT records
ICPAM-1385: Issue with using the "Clear Timezone and User Credentials" command from ICPAM

DT-264: Effective/Expiration date is not working

DT-277: On boot-up or reset, transmit current timestamp to SNIB3.
FAL-956: Falcon does not enter into degraded mode, on rebooting the controller when not connected with Velocity

DT-317: Suppress "Maintenance Event" messages by default

DT-348: XDATERR - storing credential

DT-365: Alarm Cancel is sending garbage "Alarm X'ed" messages

DT-382: On changing the door configuration from 'Entry and Exit reader' to 'Entry reader only', data is received from Exit reader.

DT-383: Access is granted to Door, but Door relay is not activated

DT-387: CCM does not send CCOTZ settings to Falcon, after a Falcon watch dog reboot when not connected with Velocity.

DT-396: Case 71818 - 32-digit Credential Problem

The new firmware has a memory map defrag scheme. New "Maintenance Events" in the range of 20100-27999 have been added.

The 20100s tell you that the defrag finished, and how many changes it made. If you only see, say, Maintenance Event 20104, that's harmless.

If you see maintenance event numbers in the range 21000-27999, you should re-download your credentials. We found some kind of corruption in the memory map and corrected it, but you may have lost data from the "XDAT" records in the process. This can affect multiple-door-group and 32-digit match code credentials.

For related information, see the table for issue PAC-269 earlier in this document.

DT-407: Input from a Wiegand or MATCH reader should not be processed, if a door is configured for an RS 485 reader.

DT-414: Report XDAT OVERFLOW condition for credential downloads

DT-416: Access Denied: Incomplete Dual had out of range PZ zone, causing a Who's Inside error

DT-419: MSP AC and BAT monitoring was incorrect

DT-423: On downloading users and issuing 88*1 command, total user count was displayed as 0. Access was not granted for downloaded users.

DT-434: Passback Minimum Occupancy settings didn't work for PZ 4 and up

DT-436: Card Reader LED Blink-Through feature was not working.

In Velocity, the properties for a reader now includes an additional checkbox option to "**Suppress card reader blink indications**". When this option is checked, it suppresses the card reader's normal blinking indications in response to an Access Granted or an Access Denied.

Note that the results of this option are affected by the settings of the **Card Reader LED on while relay active** and the **LED Reverse** options. For details, see the table at the end of the "DIGI*TRAC Hardware Configuration > Readers and Keypads > **Reader Properties - Options (formerly ScramblePad Options) page**" topic in Velocity's online help system.

DT-438: Controller fails to come online with SNIB1
DT-439: Controller fails to come online with SNIB1

DT-348: XDATERR - storing credential

DT-440: Incomplete Dual is reported with incorrect reader, after a status request

FAL-1135: On disabling a reader, the download of properties completes with errors

PAC-172: On triggering a standard Control zone or Master control zone from Command set, Door number is displayed as 8, with no reader number.

Known Limitations

These are known limitations since CCM 7.4.00.

CCMx firmware download to Mx causes lock-up

Downloading CCMx firmware to the Mx from Vn. 7.5.04 (or from a controller that was originally shipped as Vn. 7.5.04) will lock up the controller. Identiv only supports re-flashing CCMx firmware from Vn. 7.5.08, or from Vn. 7.5.12 or later.

If you have an Mx controller running a CCMx firmware version earlier than 7.5.08, you must first upgrade to version 7.5.08 before you download version 7.5.61 or later to that controller. Downloading version 7.5.61 or later to an Mx controller running a CCMx firmware version earlier than 7.5.08 will lock up that controller.

Features that reduce memory capacity

- There are several places in the **DIGI*TRAC Systems Design & Installation Guide** which list the capacity of the various controllers and memory expansion boards to support user records or alarms and events. These capacities assume that your Velocity is configured to use that standard features with data structures of a certain size. Your system's capacity could be reduced by up to 50% when using any or all of the following features (which require larger data structures):

Feature	Initially Released in
timed anti-passback	CCM firmware 7.4.25 and Velocity 3.1
multiple access zones	CCM firmware 7.5.28 and Velocity 3.6
verified anti-passback	CCM firmware 7.5.37 and Velocity 3.6 SP1
FICAM	CCM firmware 7.5.64 and Velocity 3.6 SP2

- If you have 2048 or more credentials and you haven't already installed a memory expansion board, you will need to add one in order to use any of these features. Users with the MEB/CB128 might need to special order an MEB/CE64 to augment their capacity.

- **Special notice for upgrades where a site has already had credentials downloaded to the controller:** If the controller has ever had more than 50% of its user capacity used since its last cold-start (regardless of whether the credentials were deleted later), it may be necessary to cold-start the controller's user database. Cold-starting the user's database can be done via **CMD 98*27*0*0*0*0#**, or by pressing the controller's blue Reset button for 30 seconds. A cold-start may be necessary because the new CMD 98*41*9*8*1*0# feature changes how that database is allocated, but only to the extent that space has not already been allocated.

After removing a memory board, you should cold-start the controller (or at least download all credentials)

If you remove a memory expansion board from a controller, you should download the credentials to that controller again (because it is not done automatically), or you can cold-start the controller.

Controller does not properly detect memory battery

The status of a controller's memory backup battery is not being correctly detected and reported. (The range of acceptable voltages is so narrow that a good battery might be reported as bad.)