CCM/CCMx Version 7.5.70 Release Notes

Overview

This document describes the changes in the CCM and CCMx firmware since version 7.5.64. These changes include several FICAM-related new features, several other new features (for a non-FICAM Velocity system or an ICPAM system), and several Bug Fixes. This document also summarizes the Known Limitations in this release.

Like previous versions numbered 7.5.X, version 7.5.70 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 upcoming 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
7.5.70.12	**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 7.5.70 to that controller. Downloading version 7.5.70 to an Mx controller running CCMx firmware version earlier than 7.5.08 will lock up that controller.

NOTE: Version 7.5.X 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.

FICAM-related New Features and Enhancements

This section describes the new features and enhancements introduced in this release (coinciding with the Velocity 3.6 SP2.1 release) for systems which include Identiv's FICAM Solution. For more information about Identiv's FICAM Solution, see the **FICAM Solution** section of topics in the Velocity online help system.

Be sure to also see the section of this document which describes the other new features in this release (for either a non-FICAM Velocity system or an ICPAM system).

Add transaction dispositions for when a PIV card fails the challenge/response (DT-244)

In support of Identiv's FICAM Solution, the following transaction dispositions have been added for situations when a PIV card fails the challenge/response. (This type of failure indicates a mismatched private key and public key from the certificate downloaded from the card.)

- Denied: Card challenge response failed, known user (FICAM)
- Denied: Card challenge response failed, FASC-N: xxxxx (FICAM)
- Denied: Card challenge response failed, UUID: xxxxx (FICAM)

Add transaction dispositions for Biometric failures or errors (DT-318)

In support of Identiv's FICAM Solution, the following transaction dispositions have been added for situations when biometric (fingerprint) verification fails or times out.

- (alarm 92) Denied: Bio mismatch failure (ACB 374)
- (alarm 99) Denied: Bio tamper detected (ACB 375); formerly "Bio scan timeout error"

Support non-PIV cards at a reader connected by RS-485/OSDP (DT-326)

For Velocity systems that are transitioning to FICAM, a reader connected via OSDP and with the appropriate firmware can now support both PIV cards and traditional non-PIV cards (such as MIFARE or low-frequency cards).

Support the "Scramble keypad display" option of a TS ScramblePad reader (DT-329)

For a TS ScramblePad reader connected via OSDP and with the appropriate firmware, support the option to display its keypad digits either in the standard arrangement or in a randomly scrambled arrangement. This feature appears in Velocity as the **Scramble keypad display** option in the Scramblepad/Keypad category on the Options sub-page of the Entry Reader or Exit Reader page of the Door Properties dialog.

Other New Features and Enhancements

This section describes the new features and enhancements in this release (coinciding with the Velocity 3.6 SP2.1 release) for either a non-FICAM Velocity system or an ICPAM system (not just those Velocity systems running Identiv's FICAM Solution).

Support Wiegand Exit Readers on Mx-2 and Mx-4 Controllers (DT-245)

The Mx controller provides only one Wiegand terminal per door. Previously if you wanted to have a door with a Wiegand exit reader, you had to connect that reader through a MATCH board. Now on an Mx-2 or Mx-4 controller where Wiegand terminals are available from unused doors, some of those available terminals can easily be used for exit readers.

For more information, see "**Unused Wiegand Terminals On Mx-2 and Mx-4 Controllers Are Available for Exit Readers**" in the Velocity 3.6 SP2.1 Release Notes.

NOTE: The upcoming Mx-1 single-door controller provides dedicated terminals for both a Wiegand entry reader and a Wiegand exit reader.

Threat level changes override CCOTZ ASAP (instead of waiting until the start of the next minute) (DT-266)

Previously when a change in the threat level overrode the normal Card or Code Only during Time Zone (CCOTZ) operation defined for specific readers on the system, the override did not take place until the start of the next minute. Now the override takes place as soon as possible.

Add lower-than-access relay control functions (Operate by Time Zone, Suppress Operate, and Suppress Operate Release) (DT-280)

New low-priority relay control functions have been added, which enable standard credentials to access a door when its typical operation by time zone has been temporarily overridden.

The **Operate by Time Zone** relay control function is useful for unlocking a door to the general public during regularly scheduled hours. Typically a receptionist or security guard is present during those hours to oversee the area. The **Suppress Operate** relay control function temporarily overrides (suppresses) only the Operate by Time Zone function, so that you can prevent access to the general public during unusual situations such as the receptionist or security guard not being present. (Personnel with the proper credentials can still be granted access through the door.) When the situation has been resolved, you can return the door to its normal Operate by Time Zone mode using the **Suppress Operate Release** relay control function.

For more information, see "**New low-priority control functions (Suppress Operate and Suppress Operate Release) for relays**" in the Velocity 3.6 SP2.1 Release Notes.

CCM firmware version numbering extended to support a 3-digit build number (x.xx.xx.XXX) (DT-315)

The CCM firmware's version numbering scheme has been extended to support a 3-digit build number (x.xx.xx.XXX).

Show the status of the CCM7/CCMx's write-protection jumper in the results of the 88*1 command (DT-325)

The CCM7/CCMx module includes a write-protection jumper, which can be used to prevent an operator from downloading a different version of the CCM firmware. To remotely determine the status of this jumper, you can execute the 88*1 command or the 288*56 command in the Diagnostic Window. The status is indicated by the phrase of either "CCM DFU Enabled" or "CCM DFU Disabled" in the results.

Support the upcoming Mx-1 single-door controller

This release includes some support for the upcoming Mx-1 single-door controller. For example:

- Define the operation of the Mx-1's status LEDs (in column 8) for AC / POE / BAT power (DT-358)
- Define the operation of the Mx-1's status LEDs (in column 7) for box or reader tampers (DT-359)
- Define the operation of the Mx-1's status LEDs (in column 6) for Event Tx / Credential Rx (DT-360)
- Define the operation of the Mx-1's status LEDs (in column 5) for door or line fault alarms (DT-361)
- Define the operation of the Mx-1's status LEDs (in column 4) for door or auxiliary relays (DT-362)
- Define the operation of the Mx-1's status LEDs (in column 3) for Reader Tx / Rx (DT-363)

The Mx-1 controller will be documented in a new chapter of the next version of the **DIGI*TRAC Systems Design and Installation Guide**.

Fine tune the behavior of the status LEDs on multi-door controllers (DT-368)

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 this 7.5.70 release, some additional changes to the behavior of some status LEDs have been 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)

Defects Fixed

Effective Date and Expire Date were not working for the Mx controller in ICPAM (DT-264)

The Effective Date and Expire Date were not working for the Mx controller in ICPAM. If you added effective and expire dates to a badge, the changes were not downloaded to the controller. This issue has been fixed.

Reader's LED indication of Access Granted was delayed (DT-304)

Version 7.5.64.91 of the CCM firmware caused the reader's LED indication of Access Granted to be noticeably delayed. This issue has been fixed.

After entering an invalid PIN, the Event Viewer displayed all zeros (instead of the entered PIN) in the Access Denied message (DT-307, DT-309, and DT-314)

For a Wiegand keypad reader connected to an onboard Wiegand terminal of an Mx controller, when an invalid PIN was entered, the Event Viewer showed all zeros in the event message (such as "Access Denied: PIN 0000") instead of the PIN that had been entered. This issue has been fixed.

Card data was sometimes read incorrectly by a TS reader (DT-366)

For a TS reader connected to an onboard Wiegand terminal of an Mx controller, the card data was sometimes read incorrectly. This issue has been fixed.

LED behavior was different for an entry reader versus an exit reader (DT-377)

The LED behavior was different for an entry reader versus an exit reader. (The problem was caused by a Velocity bug involving the "LED Reverse" option on exit readers.) This issue has been fixed.

Reader stopped working after an Mx controller's power was cycled (and its expansion boards were physically installed but had not been configured in ICPAM) (ICPAM-1061)

A reader connected to the onboard Wiegand terminal of an Mx controller running ICPAM stopped working after the controller's power was cycled. This happened when the controller was initially added without installing and configuring its expansion boards, and then the expansion boards were installed later but were not configured in ICPAM. This issue has been fixed.

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.