CCM/CCMx Version 7.5.64 Release Notes

Updated on April 26, 2017.

Overview

This document describes the changes in the CCM and CCMx firmware since version 7.5.61. This document also summarizes the Known Limitations in this release.

Like previous versions numbered 7.5.X, version 7.5.64 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.

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
7.5.64.95	**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 7.5.64 to that controller. Downloading version 7.5.64 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.

New Features and Enhancements

Download Activity Shown by Status LEDs of a Controller (with a SNIB2 or SNIB3) (DT-108)

The following downloads to a controller can take a significant amount of time to complete:

- credential downloads
- configuration downloads
- CCM firmware downloads
- SNIB2 or SNIB3 firmware downloads

Now for a controller equipped with a SNIB2 or a SNIB3, the behavior of its **SYS** and **NET** status LEDs has been enhanced to show when a download is in progress or when there is network activity. The 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	ON = Enclosure Tamper	ON = Multiple Enclosure Tampers
AC = AC Power	ON = AC Power is OK	ON = AC Power Failure
BAT = Standby Battery	ON = Battery is OK (at 24V – 28V)	ON = Battery Failure (less than 21V)
	Both LEDs OFF = Battery is Low (at 21V – 23V)	
SYS = Controller's Status	ON (and second LED is OFF) = Controller is OK	ON (and first LED is OFF) = Controller Failure
	Green LED ON and Red LED Flashing = Download in progress (and controller is OK)	
KPD = Controller's Polling of its MATCH boards and ScramblePads	Flash = MATCH board or ScramblePad response to polling by Controller	Flash = Controller is polling its MATCH boards and ScramblePads
NET = Network Polling of all Controllers	Flash = Controller response to polling by Velocity Server ON (and second LED is OFF) = Connected to network (without activity)	Flash = Network activity (such as sending messages to the Velocity Server)
	Green LED ON and Red LED Flashing = Connected to network, with activity	
TEST = Controller's Self Test Mode	ON = Controller is in Self Test Mode	(no second LED on this row)
ALARM = Alarms in Buffer	ON = Alarm Events in the Buffer	(no second LED on this row)

Support for Identiv's FICAM Solution

This release includes the underlying support for numerous features in Identiv's FICAM Solution. For example:

- (DT-243) Report Status of RS-485 Readers
- (DT-250) Define the Behavior of each RS-485 Reader when a Controller Enters FICAM Degraded Mode
- (DT-267) Add messages about unsupported nonce decryption algorithm (for FICAM)
- (DT-289) Support Card + PIN Credential for FICAM on RS-485 Readers

For more information about Identiv's FICAM Solution, see the **FICAM Solution** section of topics in the Velocity 3.6 SP2 main help system.

Defects Fixed

Automatically repair corruption of a controller's credentials database (DT-212)

In certain situations, a controller's credentials database can become corrupted. Now a recovery process (which runs every night or whenever a 148 command is issued) checks the credentials database and repairs many kinds of corruption. It also reclaims XDAT memory which is no longer being used, so it can be reassigned.

Executive Override of 2-Person Rule Takes Precedence Over Occupancy Rule Enforcement (DT-221)

Previously in certain situations (such as a facility where a two-person rule applies to all doors and there are nested anti-passback zones), the enforcement of occupancy rules for an odd number of persons was incorrectly preventing access to an empty room even for a credential with Executive Override. This issue has been fixed, so that a credential with the **Executive Override** option of the **2-Person Rule** section (on the **Limits** page of the **Credential Properties** dialog) is always granted access to an empty room.

Add messages for interim status and possible outcomes of Verified Anti-Passback with 2-Person Rule (DT-228)

When the **Verified Anti-Passback** feature was implemented in the Velocity 3.6 SP1 release, it did not report sufficient information about the interim status and possible outcomes of an attempted access at a door with a 2-person rule. Now the following types of messages will be displayed in the **Event Viewer** for this situation:

- Event ID 2013: Entry Access partial grant [two-person rule or visitor rule]
- Event ID 3905: Entry 2-man access Pending Verified Access
- Event ID 3122: Entry 2-man access granted OR
- Event ID 3914: Entry 2-man access Denied Incomplete Passback Verification

Automatically correct inaccurate occupancy counts for anti-passback zones (DT-229)

In certain situations, an incorrect occupancy count is reported for an anti-passback zone. Now a recovery process (which runs every night or whenever a 148 command is issued) checks for and automatically repairs this problem.

Make LED behavior of card reader on Mx controller's Wiegand interface similar to MATCH2 interface (DT-239) and Behavior of a Card Reader's LED (DT-310)

Previously, the LED behavior of a card reader was significantly different depending on whether it was connected to a MATCH2 interface or an Mx controller's Wiegand interface. Now the LED behavior is very similar, regardless of whether the card reader is connected to a MATCH2 interface or an Mx controller's Wiegand interface.

The behavior of a card reader's LED is affected by some options on the **ScramblePad Options** page of the Door Properties dialog, such as the "**Card reader LED on while relay active**" option (which is unchecked by default). The following table explains the behavior of a card reader's LED in the most common situations. Note that the behavior is distinctly different for Access Granted versus Access Denied.

Card Reader LED Behavior Options	**LED Behavior for Access Granted**	**LED Behavior for Access Denied**	**LED Behavior after Card Accepted and Waiting for PIN**
Default behavior	LED lights up for one long pulse.	LED lights for 8 short blinks.	LED blinks (at a different rate than Access Denied) until a PIN is entered or the time limit has expired.
"Card reader LED on while relay active" and blinking is enabled	LED lights up for the duration of the relay mode time.	LED lights for 8 short blinks.	LED blinks (at a different rate than Access Denied) until a PIN is entered or the time limit has expired.
"Card reader LED on while relay active" and blinking is suppressed	LED lights up for the duration of the relay mode time.	(LED does not light up.)	(LED does not light up.)

On some card readers, it is possible to have the card reader's LED line operate the card reader's beeper.

The last row of the table describes the special situation where the card reader's LED line is used to notify another system that the credential has been granted access.

"Clear Credential Database" command should also clear any XDAT memory (DT-258)

Previously, the "Clear Credential Database" command (98*27*0*0*0*0#) for a controller was not properly clearing any XDAT memory that had been allocated. This issue has been fixed.

The blue button reset of an Mx-8 controller was not deleting the entry for Port 8 Reader 16 (DT-270)

When an Mx-8 controller was reset using the blue button, the entry for Port 8 Reader 16 was not being deleted from the memory for the controller's onboard Wiegand interface. This issue has been fixed.

Readers wired to an Mx controller's onboard Wiegand connectors were not being configured or reconfigured properly (DT-299)

When an Mx controller was started, or when Velocity downloaded updated reader configurations to an Mx controller, the CCM was sending the Onboard Wiegand Reader settings to the STM-RTC chip. As a result, any readers wired to the Mx controller's onboard Wiegand connectors were not being configured properly. 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.