CCM/CCMx Version 7.5.61 Release Notes

Overview

This document describes the changes in the CCM and CCMx firmware since version 7.5.37. This document also summarizes the Known Limitations in this release.

Like previous versions numbered 7.5.X, version 7.5.61 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
7.5.61	**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 7.5.61 to that controller. Downloading version 7.5.61 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. It is not supported by older software such as MOMENTUM or SAM.

New Features and Enhancements

Enhance the Verified Anti-Passback feature to work with the Two-Person Rule feature (DT-206)

When the Verified Anti-Passback feature was initially made available (in version 7.5.37 of the CCM firmware and in Velocity 3.6 SP1), the existing Two-Person Rule feature could not be used at the same time. Now the Verified Anti-Passback feature and the Two-Person Rule feature can be used at the same time.

Disable Verified Anti-Passback when the door's state cannot be verified (DT-211)

When the Verified Anti-Passback feature is enabled for a door that has a supervised door contact, the system only logs someone as having moved to the next location if the door is opened and closed within the specified amount of time. But that approach does not work when the door's state cannot be verified, such as when the input is masked or disabled. In this situation, the system will automatically downgrade from Verified anti-passback to standard anti-passback, and log someone as having moved to the next location after access has been granted.

Simplify the timing settings for the Two-Person Rule feature (DT-214)

The Two-Person Rule timer settings of **Time increment for each valid read** and **Threshold time** (on the Passback page of the Controller Properties dialog) are essentially redundant. We plan to replace these two setting by a single timer In the upcoming Velocity 3.6 SP2 release. Until then, the **Threshold time** setting in Velocity will be ignored by version 7.5.61 of the CCM firmware.

Defects Fixed

A "Door Open Too Long" alarm was not generated when the DOTL time was set to 4140 seconds or greater (DT-175)

If the value for the **DOTL time** option (on the Input **>** Setup page of the Door Properties dialog) was set to 4140 seconds or greater, the alarm would not be generated after the door was open that long.

Keypad Programming sometimes showed scrambled (DT-196)

Occasionally, ScramblePad keypad programming slipped out of Scramble-Normal mode then back again. Also, there was not always a blinking yellow LED to indicate that keypad programming mode was active.

The “User N Added/Updated” message did not show the correct Credential ID (DT-201)

For various DIGI*TRAC commands that add or update credentials, the “User N Added/Updated” message showed User 0 instead of the correct Credential ID. This was typically seen in response to a “Forgive All Credentials” command.

CCOTZ feature was not working for a dual-technology reader on a 6-pin Wiegand port of an Mx controller (DT-202)

The **Card or Code Only Time Zone** (CCOTZ) feature was not working for a card reader with a keypad when it was connected to a 6-pin Wiegand port on an Mx controller.

Controller sometimes went offline during a midnight update process (DT-203)

During a customer's midnight update process, a controller sometimes went offline (with the Event Viewer indicating "User 0 Expired").

Function Group Access didn't report correctly when Verified Anti-Passback was enabled (DT-205)

When a credential is enrolled in an Access Function Group and the verified anti-passback feature is enabled (by checking the **Verify passback** option on the Input **>** Setup tab of the Door Properties dialog for a door that has a supervised door contact), some messages displayed in Velocity's Event Viewer about that credential's usage were confusing or incorrect. For example, a message would say “Function Group Denied” instead of “Access Denied”.

On an Mx controller (which has an STM chip providing the functionality of a MATCH2 board), ensure that the status of card readers is being monitored (DT-216)

When RPK40 card readers were wired into the 6-pin Wiegand ports on an Mx controller, a reader tamper alarm could be reported for the wrong reader address.

uTrust Keypad readers were not giving a visual indicator for Dual Credentials (DT-217)

When a door was configured to require Dual Credentials (so the user has to present a valid ID card and then enter a valid PIN code), a uTrust Keypad reader (model 8232) was not flashing its LED to indicate when to enter the PIN. (This visual indicator is needed for hearing-impaired persons who might not hear the reader's beeping.) Now any card reader’s LED will blink slowly when it is time to enter the PIN.

Enforce Two-Person Rule occupancy requirements for nested anti-passback zones (DT-218)

Where a customer had an anti-passback zone with a 2-person occupancy requirement which contained another anti-passback zone which also had a 2-person occupancy requirement, it was possible for three people to violate the occupancy requirements by performing the following sequence of actions:

1. With both anti-passback zones unoccupied, the first two people enter the outer zone together.
2. Because two people already occupy the outer zone, the third person is able to enter the outer zone alone.
3. Two of the three people were then allowed to enter the inner zone together. This was incorrect because it left one person alone in the outer zone.

Now in this situation, when two of the three people try to enter the inner zone, a “Denied: Overridden” event is generated and they are not allowed to enter. (To enter the inner zone, a fourth person would first need to enter the outer zone.)

During a Two-Person Rule transaction, disable the "opposite" reader (DT-219)

For a Two-Person Rule transaction to succeed, two valid credentials must be presented at the same reader within a specified time interval. It was possible for the system to mistakenly grant access at a reader in the situation where:

1. At a particular reader configured with a Two-Person Rule, one valid credential was presented, starting the timer.
2. While the timer was running and before a second valid credential was presented at that same reader, some other valid credential was presented at the "opposite" reader (which has an address of N+8 or N-8).

Corporate 1000 cards have a different MATCH number when a reader is on an Mx controller's built-in Wiegand port than when it is on a MATCH2 board with Custom 21 Wiegand pass-through (DT-222)

The MATCH number generated for a 35-bit Corporate 1000 card differs when a reader is connected to a built-in Wiegand port on an Mx controller, instead of to a MATCH2 board with Custom 21 Wiegand pass-through. The MATCH2 board's Custom 21 does not implement the 35-bit Corporate 1000 format, and treats the card data as "Octal pass-through, discard parity bits without checking".

Until this type of option is available for an Mx controller through Velocity, the workaround is to use the following command:

403*readernumber*4097*16#

Indala readers were not working reliably on an Mx controller's built-in Wiegand port (DT-231)

Indala readers were not working reliably when they were connected to a built-in Wiegand port on an Mx controller.

Mx controller sometimes locked up during a CCM/STM reflash or upgrade (DT-240)

Sometimes during a CCM/STM reflash or upgrade, an Mx controller would lock up with a "FAIL 7.2" or "FAIL 9.4" code when it should be upgrading the STM-RTC firmware.

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 STM-RTC 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 to that controller. Downloading version 7.5.61 to an Mx controller running CCMx firmware version earlier than 7.5.08 will lock up that controller.

Timed Anti-Passback

- As mentioned in the CCM 7.4.12 Release Notes, if you are using the Timed Anti-Passback feature for all users, your user capacity will be cut in half. Therefore, if you have 2048 or more credentials and you haven't already installed a memory expansion board, you will need to add one. Users with the MEB/CB128 might need to special order an MEB/CE64 to augment their capacity.
- If your site has more than 2000 credentials and will need Timed Anti-Passback, the **CMD 98*41*9*8*1*0** command should be added to a command set and put into the "Additional command sets to download" feature (on the General page of the Controller Properties dialog in Velocity).
- **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.

Digi*Trac Annunciator (DTA) and Digi*Trac Annunciator with 2-line LCD (DTA2)

- Until Velocity has native support for the new embedded LCD display, it is necessary to add a command **403*READER*65*72#** for each reader that has an LCD unit. We suggest using the Controller Properties "Additional command sets to download" feature.

- As of Vn. 7.4.37, as part of the 2-line embedded LCD project, the output format for the DTA and the DTA2 has been changed to show shorter messages, such as showing **14:20** instead of **08 Oct 2:20 pm.**