

CCM Version 7.4.58 Release Notes



Copyright© 2013, Identive Group. Released June 1, 2013.

Overview

CCM 7.4.58 supports newer PIV cards which use the updated FIPS201 data layout, supports PIV-I cards with a UUID (128-bit GUID), supports facilities using multiple variations of PIV and PIV-I cards, and fixes several bugs.

For more information, see the [New Features](#) and [Enhancements](#) sections of this document. (Additional information is also provided in the “Using PIV and PIV-I Cards” section of the Velocity 3.1 KB640 Release Notes.) This document also summarizes the [Defects Fixed](#) and the [Known Limitations](#) in this release.

CCM 7.4.58 is a **required** upgrade for customers needing support for any of the following functionality:

- newer PIV cards which use the updated FIPS201 data layout (as specified in the NIST Special Publication 800-73-3)
- PIV-I cards with a UUID (128-bit GUID), per the updated FIPS201 data layout
- multiple variations of PIV and PIV-I cards

CCM 7.4.58 is a **recommended** upgrade for customers wanting to install the bug fixes.

New Features

Handle 128-bit GUID (UUID) per NIST SP800-73-3 [DT-79]

CCM 7.4.58 supports multiple variations of PIV and PIV-I cards. PIV cards contain fields such as Agency Code, System Code, and Credential Number which make up portions of the Federal Agency Smart Credential Number (FASCN). For PIV-I cards, these fields are populated with 9s, and the Universally Unique Identifier (UUID) field is used instead of the FASCN.

Both PIV and PIV-I cards have a GUID or UUID field, consisting of 32 hex digits. (On PIV cards, the data in that field is often just a meaningless placeholder such as all 0000 or all 3030, because the FASCN is used instead.) The UUID is 128 bits, and it's always represented as 32 hex digits.

To use this feature, you must be running the following:

- Velocity 3.1 KB640 or later
- MATCH version 130127 or later (see KB640 Release Notes for more information)

Enhancements

Bypass Code Conflicts for long card codes [DT-96]

A PIV card can output either a 64-bit, 75-bit, or 200-bit FASCN, while a PIV-I card will output a 128-bit GUID/UUID. However, a controller's CCM handles data in chunks of 16 hex digits, so card codes greater than 64 bits must be represented in two chunks.

Although unlikely, it is possible that even though an entire 32-digit card code is unique in the Velocity database, its first 16 digits could be the same as other 16-digit or 32-digit card codes. In that case, an error used to be generated when attempting to download the credential to a controller with multiple card readers that support different variations of PIV and PIV-I smart cards. To ensure that unique 32-digit card codes can be downloaded to a controller, the CCM no longer checks for uniqueness of the first 16 digits (starting with CCM 7.4.58).

To use this feature, you must be running the following:

- Velocity 3.1 KB640 or later

Defects Fixed

Controllers on CCM 7.4.51 do not report the “ACC Mskd” Status in Diagnostics [DT-73]

After triggering a door's relay by right-clicking on a door and choosing Functions > Access > Momentary Access, the “9 – Alarm Special Setups and Status” report from the Diagnostics drop-down list (in the Velocity Diagnostic Window) was not reporting the “ACC Maskd” status while the relay was active. This issue has been fixed.

Repeated use of 01 command with same PIN fails when duress is enabled [DT-74]

When the Duress digit was enabled, repeated use of the 01 (Change master keypad programming password) command with the same PIN would fail with a “conflicting code” error message at the end of the download. This issue has been fixed.

DOTL alarm triggers with DOTL Timer set to 0 [DT-77]

The Door Open Too Long (DOTL) alarm was being triggered even when the DOTL time was set to 0 (which should have disabled the alarm). This issue has been fixed.

Extended Access Does Not Mask DOTL Warning Time [DT-98]

The Extended Access feature was not properly masking the Door Open Too Long (DOTL) warning. This issue has been fixed.

Known Limitations (since CCM 7.4.0)

Timed Anti-Passback

- As mentioned in the CCM 7.4.12 Release Notes, if you're 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'll 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)

- As of CCM version 7.4.37, the output format for the DTA has been changed to show shorter messages, such as showing **14:20** instead of **08 Oct 2:20 pm**.
- Until Velocity has native support for the new embedded 2-line LCD display, it is necessary to add a **403*READER*65*72#** command for each reader that has an LCD unit. We recommend using the “Additional command sets to download” feature on the General page of the Controller Properties dialog in Velocity.