Velocity 3.1 KB640 Release Notes

Overview

The Velocity 3.1 KB640 release supports newer PIV cards which use the updated FIPS201 data layout, allows you to use the Windows built-in SYSTEM account to install Velocity updates, supports PIV-I cards with a UUID (128-bit GUID), makes the Velocity database more secure, and fixes several bugs. (The Velocity 3.1 online help system has also been updated.)

To utilize all the features of KB640 requires CCM version 7.4.58 (in production as of 6/1/2013). To utilize the PIV-I/128-bit GUID support also requires MATCH2 version 130127 (available on special order from 6/1/2013 and full production from 8/1/2013). Check with Inside Sales to verify the current production version of MATCH2 or Scramblepad.

For more information, see the tables of New Features and Enhancements and Bug Fixes.

This document also summarizes the Known Issues in this release.

NOTE: This Velocity 3.1 KB640 release includes some bug fixes, enhancements, and new features which are not part of the Velocity 3.5 initial release. If you install 3.1 KB640 and later want to upgrade to 3.5, you should then upgrade to the 3.5 SP1 (or newer) release.

New Features and Enhancements

Reference ID	Feature	Description
VEL-791	Velocity supports an unlimited number of USB Smart Card Readers	Velocity now supports a virtually unlimited number of USB Smart Card Readers. (Previously, if you had more than 4 USB Smart Card Readers attached to your computer, they would not all appear in the drop-down list of the Select Smart Card Reader dialog.)
VEL-2500	Added support for updated FIPS201 data layout	Enrollment Manager can now read the Printed Information Buffer (PIB) from newer PIV cards which use the updated FIPS201 data layout, as specified in the NIST Special Publication 800-73-3. See Using PIV and PIV-I Cards later in this document.
VEL-2856	Added ability to install Velocity updates using the built in SYSTEM account	You can now use the Windows built-in SYSTEM account to install Velocity updates. **NOTE:** After using the SYSTEM account to install KB640, Velocity will generate an Access Denied message dialog when it first tries to start up, because it is using the SYSTEM account which is not a Velocity operator. Click OK to close the message dialog, then restart Velocity, at which point it will use the account you are logged on with.
VEL-2898	Added support for PIV-I cards with a UUID (128-bit GUID)	Velocity now supports the UUID (128-bit GUID) in PIV-I cards which use the updated FIPS201 data layout, as specified in the NIST Special Publication 800-73-3. This feature requires CCM firmware version 7.4.58 or later and MATCH2 firmware version 130127 or later. For more information, see Using PIV and PIV-I Cards later in this document.
VEL-2925	Compliance with DISA's Application Security and Development STIG	Some portions of the Velocity software were updated to validate compliance with the specifications outlined in the "Application Security and Development Security Technical Implementation Guide" by the Defense Information Systems Agency (DISA). (These enhancements did not change the functionality of Velocity.)

Reference ID	Feature	Description
VEL-2948	Controllers - Advanced Options Setups dialog change for Bypass Code conflict checking	To help support facilities using multiple variations of PIV and PIV-I smart cards, the function of the “Bypass CODE conflict checking” option on the Advanced Options Setups dialog (which is reached by clicking the Advanced button on the Setup page of the Controller Properties dialog) has been changed, starting with CCM firmware version 7.4.58. 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 on or more other 16-digit or 32-digit card codes. In prior versions an error would be generated when attempting to download the credential to a controller where this conflict existed. For example when multiple card readers that support different variations of PIV and PIV-I smart cards were used one system. 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. As indicated this change also caused a change in the function of the “Bypass CODE conflict checking” option on the Advanced Options Setups dialog for a controller. Un-checking this option would previously enable the controller to check PIN# or CARD# for conflicts in the user database. In this version un-checking the option checks only the PIN# for apparent conflicts.
VEL-2974	New UDF type “UUID” tor PIV card support	To support the UUID (128-bit GUID) in PIV-I cards, Velocity now includes a new UDF type called UUID, which consists of 32 hexadecimal digits. When entering a UUID, you can include dash characters (“-“), but they will be stripped out when the value is saved. User-Defined Fields with this new field type will show up, along with numeric UDF types, when you press the UDF mapping button for a credential’s Card data. Although ideally a UUID should be unique, Velocity does not check for uniqueness, to support legacy PIV cards (which often have dummy UUID data that is not unique).

Bug Fixes

Reference ID	Bug	Description
VEL-932	Customized tab settings get lost when newer KB’s get applied	Some changes made using Customization Manager could be lost when applying newer updates to Velocity, because some newer components had lower version numbers than before.
VEL-939	Incorrect operator name would sometimes appear when downloads would take place	When an operator changed the credentials for a user, Velocity sometimes incorrectly reported that the downloading of the information to the controllers was started by a different operator.
VEL-1095	Stopping and starting the Digi*Trac Network Service would cause active downloads to disappear from the spooler directory	A mismatch between the Velocity database and a controller's information could occur if a download did not complete. Now downloads are monitored to make sure they resume and complete after any of the following problems occur during the download: • The Velocity services are restarted • The Velocity Server is restarted • A controller is powered off • A controller is disconnected from the network • A controller's CCM is replaced

Reference ID	Bug	Description
VEL-1788	An error would occur when accessing the door properties after applying KB620 or KB630	Velocity would sometimes generate an error message when trying to access the properties of a door. The error generated is as follows: The following unexpected application error occurred… Function Name: LoadReader FunctionSubItem: 32 Number: 3265 Description: Item cannot be found in collection corresponding to the requested name or ordinal
VEL-2011	Long command responses can take controllers and ports offline	Executing a DIGI*TRAC command from the Diagnostics Window that should return a lot of data in a short time (such as ten or fifty credential records in two seconds) sometimes took a long time to respond and caused the port and controller to go offline and then back online.
VEL-2780	Loss of network connection not detected from Velocity clients	Velocity clients failed to detect when they lost connection to the Velocity server on a loss of network connection.
VEL-2811	Deleting identical Standard Time Zones from a Master Time Zone would generate errors on the Input/Relay Logic Tab	Deleting identical Standard Time Zones from a Master Time Zone would generate errors on the Input Logic and Relay Logic page of a door's Properties dialog. The error generated is as follows: Master Time Zone Error occurred in sp_CanSyncMasterTZToController
VEL-2821	Arithmetic overflow error when updating a Door Group	When modifying a Door Group that belonged to a Master Door Group where the Port address of the Controller was greater than 255, Velocity sometimes generated an unexpected application error. The error generated is as follows: Hirsch Electronics The following unexpected application error occurred… Function Name: MMasterDoorGroup:UpdatedUserCredentialsInMDG FunctionSubItem: 17 Number: -2147217833 Description: Arithmetic overflow error for data type tinyint, value = xxx
VEL-2831	CCTV Call Camera to Monitor custom link prompt not working	In the Graphics module, the “CCTV Call Camera to Monitor” custom link’s “Prompt the user for the camera/monitor each time” setting (for the Default Click Behavior option on the Settings page) was not working.
VEL-2833	Graphics generates errors after moving controllers from SNET to XNET Port	The Graphics module was generating errors after a controller's address had changed due to it being moved from an SNET Port to an XNET Port. (Now when a map is opened, the addresses of the plotted VIOs are checked, and automatically updated when necessary.) The error generated is as follows: An error has occurred. Description: Object required Function: Graphics.FMain.InitVIO(160) Error Number: 424 File Version: Velocity Graphics – 3.1.19
VEL-2863	Search error on a UDF with the Unique Number type	While searching in Enrollment Manager on a User-Defined Field with the Unique Number type and a value like 5415840865, a search error message was sometimes displayed. The error generated is as follows: The search criteria was malformed. Please check your criteria.

Reference ID	Bug	Description
VEL-2867	Error occurs after clicking on the Add button in the Search All Groups option within Enrollment Manager	While searching in Enrollment Manager, an error sometimes occurs after clicking the Add button on the Search All Groups dialog. The error generated is as follows: Hirsch Electronics The following unexpected application error occurred… Function Name: frmQueryBuilder.cmdTextAdd_Click FunctionSubItem: 176 Number: 9 Description: Subscript out of range
VEL-2881	Exit reader address is the same as the Entry reader in the Event Viewer	For a door with separate Entry and Exit reader, the Event Viewer was incorrectly showing the Exit reader's address as the Entry reader's address.
VEL-2914	Auto Display Credentials does not function on exit readers	The "Default Display Credential" setting in the badge Template drop-down list (in the "Display Credentials Default" section on the General page of Velocity's Preferences dialog) was not working on exit readers.
VEL-2916	The Velocity update program will unintentionally mark a KB as complete even if any of its scripts fail or are manually cancelled	The Velocity Updater sometimes incorrectly marks an update as completed, even though a script had failed or been cancelled by the user. (Now a script cannot be cancelled by the user, logging of script results during an update has been enhanced, and a subsequent run of a failed update will re-run every script.)
VEL-2918	Database access error after running a "hardening" script	A customer reported a database access error after running a "hardening" SQL script to lock down their database. (This error was caused by the way that the DVR code used the ADO command object to pass parameters to stored procedures by name.) The error generated is as follows: Hirsch Electronics Error in access database <OK>
VEL-2936	Unbundled readers do not display the "Enable Wiegand Hex Pass-through" option	When a reader was unbundled from a door, it did not include the "Enable Wiegand Hex Pass-through" option on the General page of the reader's Properties dialog.
VEL-2961	Changing Central Station Receiver (CSR) point names does not update the name in Point Level Customization	Customization Manager was not automatically updating the name of a point defined in Point Level Customization after you went to the Central Station Receiver (CSR) and changed the name of a defined point. This was causing Customization Manager and the CSR to have different names for that point.
VEL-2962	Deleting Central Station Receiver (CSR) points does not remove them from Point Level Customization	Customization Manager was not automatically deleting a point defined in Point Level Customization after you went to the Central Station Receiver (CSR) and deleted that point. This was causing orphaned points to remain in Point Level Customization, which could not be deleted.

Reference ID	Bug	Description
VEL-2967	FIPS 201 Contact with “Read locked information (required PIN)” enabled will stop responding when scanning PIV cards in the Enrollment Manager	While scanning a PIV-I card, the Accept button in the Verify Scanner Data dialog was not being enabled and Enrollment Manager stopped responding, after clicking the Read PIV Card button while the Type was set to “FIPS 201 Contact” and the “Read locked information (requires PIN)” option was checked.
VEL-2968	When enrolling PIV cards using unique text for GUID causes UDF error as PIV GUIDs are all zeros	Attempting to use the UDF type of “Unique Text” for the GUID field of PIV cards resulted in a UDF Validation error, because the value was not unique. (On PIV cards, the data in the GUID field is often just a meaningless placeholder such as all 0000 or all 3030, because the Federal Agency Smart Credential Number is used instead.) This issue was fixed by adding a new UDF type called UUID, which consists of 32 hexadecimal digits. For more information, see the Description of VEL-2974 in the New Features and Enhancements table.
VEL-2977	Velocity doesn’t check if a Duress digit would cause a code conflict	When you added a duress digit to an existing PIN code, Velocity wasn’t properly checking whether the resulting code conflicted with another existing PIN code that had more digits. (For example, a 4-digit PIN code which was later edited to add a 5th duress digit was not being checked for a conflict with the existing 5-digit PIN codes.) This enabled you to define a conflicting code, which caused errors (such as “command failure 69”) when Velocity tried to download the code to a controller.
VEL-2980	Velocity crashes after disabling all column headers if a status group contains at least one door	If a status group contained at least one door, and you disabled every column of the Status Viewer (by clearing all the checkboxes on the Column Headers page of the Status Viewer Properties dialog and clicking OK), Velocity used to crash and a “Velocity has stopped working” message appeared. Now at least one column must be visible, and you are prevented from disabling every column.
VEL-3001	'Out of Memory' error on Velocity client when using Auto Display Credentials	An “Out of memory” error was generated sometimes when using the Auto Display Credentials feature on multiple doors. The error generated is as follows: Velocity: Display Credential An error has occurred. Description: Out of memory Function: ImageListCtrl.FPPreview.InitToolbar(6) Error Number: 7 A related error is: Velocity: Display Credential An error has occurred. The object invoked has disconnected from its clients. Function: PhotoCallupBT.FPPreview.TempPictureFiles(34) Error Number: -2147417848
VEL-3017	DTServer incorrectly treats some database deadlock as database connection failure and does not recover	The DIGI*TRAC service’s database connection monitoring code incorrectly interpreted a database deadlock as a database connection failure.

Known Issues

Reference ID	Name	Description
VEL-878	Pelco DVR integration does not work on Windows Vista or Windows 7	Velocity crashes (with an “ActiveX component can’t create object” error message) when connecting to the PELCO DX8100 DVR's cameras, using a Velocity Client on Windows Vista or Windows 7. (The integration works as expected when using a Velocity Client on Windows XP Professional.) This issue is caused by Pelco not supporting Windows Vista or Windows 7. There is no workaround.
	DVR/NVR video cannot be viewed on Windows Server 2008	When trying to view DVR video from a Velocity Server running on Windows Server 2008, Velocity crashes. The workaround is to view the video from a Velocity Client (instead of the Velocity Server). As a rule of thumb, the Velocity server should not be used to perform client type functions.
VEL-2859	Installing Velocity clients using a DVD that contains KB630 will unintentionally update the server with the KB630 files	Installing Velocity clients using a Velocity 3.1 DVD that contains KB630 will unintentionally update the Server with the KB630 files. This is a problem when the server has a KB that is newer or older than KB630. For example: If the server has a newer KB (such as KB640) installed, and you install a new client using a DVD that contains KB630, after the installation is complete it will try to automatically run KB630 on the client and it will also apply the KB630 files on the server, overwriting the newer KB640 files. When this happens, the client will generate a message stating the following: Velocity Update This machine is currently up to date. Do you wish to re-copy files? <Yes> <No> **NOTE:** Due to this known issue with KB630, we recommend that you do NOT install Velocity clients using a DVD containing KB630 if the server is running a different KB.
VEL-2908	KB620 or KB630 installs sometimes do not successfully complete	Some customers have reported that sometimes the Velocity 3.1 KB620 or KB630 updates fail to complete. The cause of this issue is unknown. Tech Support has found that the updates will complete if the MSIExec process and SDK.bat are manually ended. However, this can cause an out-of-memory error on Velocity client computers. To solve this problem, you must contact Tech Support to obtain some batch files which register DLL and OCX files in the Velocity installation directory.
VEL-3026	Pelco DVR not functional on KB640	On the Velocity 3.1 KB640 release, you cannot connect to a Pelco DVR.

Using PIV and PIV-I Cards

Software Requirements:

Velocity now supports the UUID (128-bit GUID) in PIV-I cards which use the updated FIPS201 data layout, as specified in the NIST Special Publication 800-73-3. This feature requires CCM firmware version 7.4.58 or later, and MATCH2 firmware version 130127 or later.

An Overview of PIV and PIV-I Cards:

PIV cards are personal identity verification smart cards issued by federal agencies for their employees. **PIV-I** cards are similar non-federal personal identity verification smart cards that can interoperate with federal PIV systems, and are issued in a manner that enables the federal government to trust the card. For example, PIV-I cards require a specific identity verification process and they must include a photograph, fingerprint information, and an Authentication Digital Public Key Infrastructure (PKI) certificate. Examples of PIV-I cards include the First Responder Authentication Credential (FRAC) and the Transportation Worker Identity Credential (TWIC).

PIV-C cards are also non-federal personal identity verification smart cards that can interoperate with federal PIV systems, but they are not issued in a manner that enables the federal government to trust the card. (Velocity does not differentiate between PIV-I and PIV-C cards, so we will only use the terms PIV and PIV-I.)

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.

Configuring Readers for PIV and PIV-I Cards:

Multiple-technology card readers exist, sometimes in "high and low frequency" configurations. Depending on the card reader's hardware and firmware, it could send a:

- FASCN when a PIV card is presented
- UUID when a PIV-I card is presented
- card code (which is usually shorter) when a low-frequency proximity card is presented

For a **FASCN**, a multiple-technology card reader could output either the 64-bit, 75-bit, or 200-bit FASCN format. A particular reader will output only one format for FASCN, as specified in its firmware or other settings.

For this output:	Set each reader's MATCH2 board to:	and in Velocity:
64-bit FASCN format	Custom 24, 25, or 26	On the Setup page of each door's Properties dialog (or the General page of each unbundled reader's Properties dialog), select the "64-bit FASCN bypass" value from the Special Handling drop-down list. For each enrollment station, select the same value (which you selected for each reader) from the Special Handling drop-down list on the Credential Enrollment page of the Enrollment Manager's Device Configuration dialog. (This value is used to automatically select the appropriate card Type on the General page of the Credential Template Properties dialog and the Credential Properties dialog.) If your system does not include any enrollment stations, select the appropriate card Type on the General page of the Credential Template Properties dialog and the Credential Properties dialog.

For this output:	Set each reader's MATCH2 board to:	and in Velocity:
75-bit FASCN format	Custom 18, 20, or 21	On the Setup page of each door's Properties dialog (or the General page of each unbundled reader's Properties dialog), select either the "75-bit (14 digits) FASCN bypass" or the "75-bit (16 digits) FASCN bypass" value from the Special Handling drop-down list. For each enrollment station, select the same value (which you selected for each reader) from the Special Handling drop-down list on the Credential Enrollment page of the Enrollment Manager's Device Configuration dialog. (This value is used to automatically select the appropriate card Type on the General page of the Credential Template Properties dialog and the Credential Properties dialog.) If your system does not include any enrollment stations, select the appropriate card Type on the General page of the Credential Template Properties dialog and the Credential Properties dialog.
200-bit FASCN format	Custom 27, 28, or 29	On the Setup page of each door's Properties dialog (or the General page of each unbundled reader's Properties dialog), select the "200-bit FASCN bypass" value from the Special Handling drop-down list. For each enrollment station, select the same value (which you selected for each reader) from the Special Handling drop-down list on the Credential Enrollment page of the Enrollment Manager's Device Configuration dialog. (This value is used to automatically select the appropriate card Type on the General page of the Credential Template Properties dialog and the Credential Properties dialog.) If your system does not include any enrollment stations, select the "200-bit FASCN" value for the card's Type (on the General page of the Credential Properties dialog and the Credential Template Properties dialog).

For a **UUID**, if your reader outputs the 128-bit GUID/UUID code, then:

- Any of the MATCH2 Wiegand Customs 18, 20-21, or 24-29 will handle it.
- On the Setup page of each door's Properties dialog (or the General page of each unbundled reader's Properties dialog), select one of the "FASCN bypass" values from the Special Handling drop-down list.
- For each enrollment station, select the same value from the Special Handling drop-down list on the Credential Enrollment page of the Enrollment Manager's Device Configuration dialog. (This value is used to automatically select the appropriate card Type on the General page of the Credential Template Properties dialog and the Credential Properties dialog.)
- If your system does not include any enrollment stations, you can use almost any value for the card's Type (on the General page of the Credential Properties dialog and the Credential Template Properties dialog).

If a card with a UUID that is not enrolled in Velocity is presented at a reader, an "Invalid UUID" event is generated. (This is similar to message type 115 for "Invalid FASCN".)

For a low-frequency **proximity card**, you can use the "Standard Wiegand (parity)" format, or the "Octal Pass-through" format (with or without parity), for the card's Type on the General page of the Credential Properties dialog and the Credential Template Properties dialog.

- Customs 18, 24, and 27 take the low-frequency card codes and output them as **Octal Pass-through No Parity**. For example, a 26-bit card would send a 9-digit card code.
- Customs 20, 25, and 28 take the low-frequency card codes and output them as **Standard Wiegand with Parity**. Any bit length card will result in an 8-digit MATCH code, assuming it passes the parity test.
- Customs 21, 26, and 29 take the low-frequency card codes and output them as **Octal Pass-through with Parity**. For example, a 26-bit card would in an 8-digit card code, assuming it passes the parity test.

The "Enable Wiegand Hex Pass-through" option on the Setup page of a door's Properties dialog (or the General page of an unbundled reader's Properties dialog) can be used with any of the Octal Pass-through values, to transform the card code into a 16-digit Hex card code.