IDENTIV uTrust Velocity 3.6 SP2.1 Release Notes

Overview

The Velocity 3.6 SP2.1 release includes:

- several FICAM-related new features,
- several other new features (for any Velocity system), and
- several Bug Fixes.

This document also summarizes the Known Issues in this release.

IMPORTANT INSTALLATION NOTES:

- Due to an issue caused by Microsoft changing the security certificate of its installer for Windows updates including the .NET Framework, the Velocity 3.6 SP2.1 release is not available as a full new installation. It is only available as an update to an existing Velocity 3.6, 3.6 SP1, or 3.6 SP2 system.
- If you are installing Velocity 3.6 SP2.1 on a computer running Windows 10, then you must first install .NET 4.6.2 or higher. You will receive an error message stating "A certificate chain could not be built to a trusted root authority.", if your computing environment is disconnected from the Internet or has a firewall that blocks content from http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en.

  To resolve this issue, you must download and install the latest Microsoft certificates, using one of the methods explained in https://support.microsoft.com/en-us/help/3149737/known-issue-for-security-update-3136000-for-the--net-framework-4-6-1-4.

Firmware Requirements

- To utilize all the features of Velocity 3.6 SP2.1 requires CCM firmware version 7.5.70.12 or later. (Identiv's FICAM Solution requires CCM firmware version 7.5.64.95 or later.)
- To utilize the PIV-I/128-bit GUID support (first provided in CCM firmware version 7.4.58) also requires MATCH2 firmware version 130127 or later. (ScramblePad model numbers starting with DS47L-SSP include a MATCH2 board.)
- If a controller has a SNIB2 board, Velocity 3.6 SP2.1 requires SNIB2 firmware version 5.99 or later. (The most recent version which is available is 6.42.) If a controller has a SNIB3 board, Velocity 3.6 SP2.1 requires SNIB3 firmware version 2.02.0004.

Compatible Versions of Integrations or Optional Components

The following table shows the compatible versions of integrations or optional components for Velocity's recent releases.

Component:	Compatible version for **Velocity 3.5 SP2.1**	Compatible version for **Velocity 3.6**	Compatible version for **Velocity 3.6 SP1**	Compatible version for **Velocity 3.6 SP2**	Compatible version for **Velocity 3.6 SP2.1**
Velocity Web Services Client	3.5.1.67	**3.6.2.10**	**3.6.2.11**	**3.6.5.1**	**3.6.6.515**
Hirsch Video Integration framework					
plug-in for Aventura	1.1.1.12	**1.1.3.1**	1.1.3.1	**1.1.3.9**	1.1.3.9
plug-in for unified American Dynamics	1.1.1.12	**1.1.3.4**	1.1.3.4	**1.1.3.5**	1.1.3.5
Edge EVO Controller Integration	1.0.1.53	**1.0.2.1**	1.0.2.1	**1.0.3.3**	1.0.3.3

FICAM-related New Features and Enhancements

This section describes the new features and enhancements introduced in the Velocity 3.6 SP2.1 release for systems which include Identiv's FICAM Solution. Be sure to also see the section which describes the other new features (for any Velocity system).

The following table shows the compatible versions of the software components in Identiv's FICAM Solution, corresponding with the Velocity 3.6 SP2.1 release.

FICAM Software Component:	Compatible version for Velocity 3.6 SP2.1
CCM firmware	7.5.70.12
SNIB3 firmware	2.02.0004
uTrust TS Government reader firmware (TRN file)	2.1.315
Velocity	03.06.006.1128
Velocity Certificate Checking Service	3.6.6.184

For more information, see the **FICAM Solution** section of topics in the Velocity main help system. Information about the hardware components of Identiv's FICAM Solution is available in the **DIGI*TRAC Systems Design and Installation Guide**.

Support for Veridt's Stealth Bio and Stealth Dual Readers

The Velocity 3.6 SP2.1 release includes support for Veridt's Stealth Bio and Stealth Dual readers, which adds BIO authentication of a fingerprint to Identiv's FICAM solution.

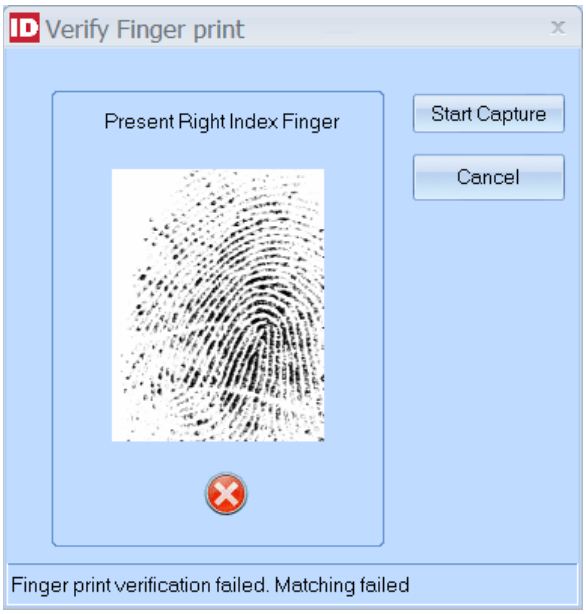
The reader must be connected to a Hirsch controller using OSDP/RS-485, in a Velocity system running in FICAM mode.

To manage the biometric authentication, the following three options have been added to the **FICAM Validation Options** page of the **Velocity Cert Check Service Configuration** dialog:

Option (in group)	**Description**
Fingerprint Required (in Required Data)	When this option is checked, the Fingerprint Object container is required to be present on the card, and fingerprint verification will be performed when the card is enrolled in Velocity (to ensure the person's live fingerprint matches what is stored in the card).
Fingerprint Signature Check (in General Checks)	When this option is checked, verify that the signature found in the Fingerprint object is correct (using the certificate found in the CHUID).
Certificate in Fingerprint (in Certificate PKI Checks)	When this option is checked, the fingerprint container's certificate will be validated (if present).

Fingerprint Authentication During Enrollment

By default, the **Fingerprint Required** option (on the **FICAM Validation Options** page of the **Velocity Cert Check Service Configuration** dialog) is checked, so fingerprint verification will be performed when the card is enrolled in a Velocity system running in FICAM mode. This ensures that the person's live fingerprint matches what is stored in the card. To do this, your enrollment station needs to include a fingerprint scanner.



More Optional Checks During Enrollment

Two more options have been added to the **FICAM Validation Options** page of the **Velocity Cert Check Service Configuration** dialog:

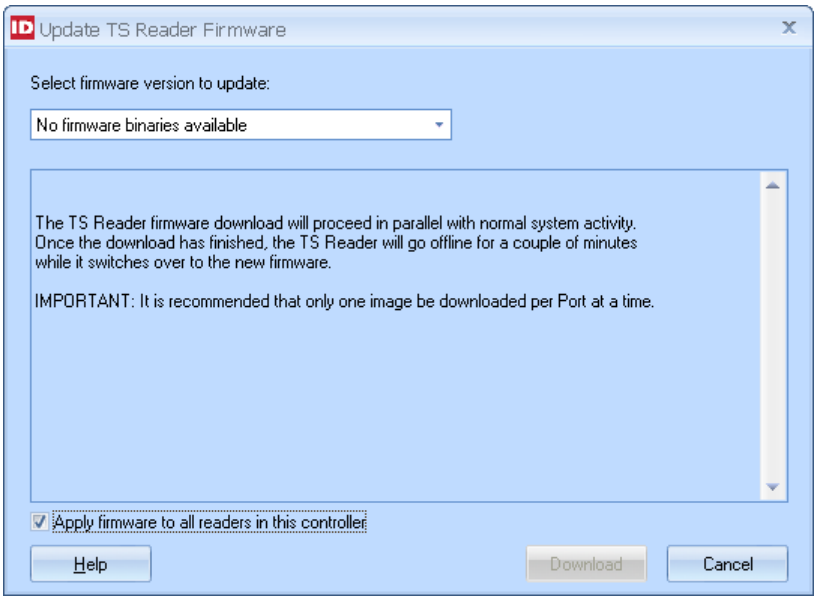
Option (in group)	**Description**
Card Challenge PIV Auth (in General Checks)	When this option is checked, the PIV Authentication certificate must pass a dynamic challenge-response authentication. When this option is unchecked, the card can still be enrolled even if the PIV Auth authentication fails.
Card Challenge Card Auth (in General Checks)	When this option is checked, the Card Authentication certificate must pass a dynamic challenge-response authentication. When this option is unchecked, the card can still be enrolled even if the Card Auth authentication fails.

Downloading Firmware Updates to a TS Reader from Velocity

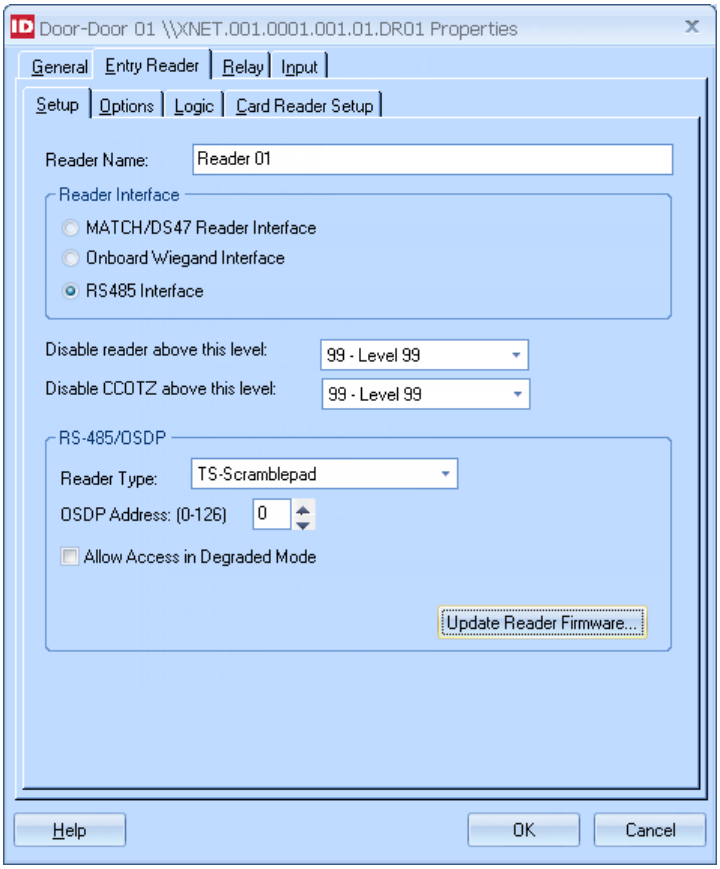
You can now download firmware updates to a TS reader from Velocity, if that reader is connected via OSDP RS-485. The firmware download process for TS readers is very similar to that for the CCM, SNIB2, and SNIB3 firmware.

After you import the correct files into Velocity, the update becomes globally available. Firmware changes can be made either one reader at a time, or for all the TS readers on one controller. uTrust TS Government reader firmware downloads are initiated by either:

- Clicking Velocity's menu button, then choosing **Data Exchange ▸ TS Reader Import**:



- Clicking the **Update Reader Firmware…** button on the **Setup** page of the Door Properties dialog, which is present only when the **RS485 Interface** value is selected for the Reader Interface option and the selected **Reader Type** is one of the available TS readers by Identiv:



CCOTZ Assurance Level

Background Information

Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, dated August 2013 includes a section about **PIV Cardholder Authentication**. That section defines a suite of authentication mechanisms that are supported by PIV cards, and how much assurance each one can provide that the holder of a PIV card is actually the authorized owner. For physical access:

PIV Assurance Level	Applicable PIV Authentication Mechanisms
Little or No confidence	VIS, CHUID
Some confidence	PKI-CAK, SYM-CAK
High confidence	BIO
Very High confidence	BIO-A, OCC-AUTH, PKI-AUTH

Higher levels of assurance require multiple authentication factors (what you have, know, or are). For FICAM:

- What you **have** is a PIV card (with multiple data elements and encryption keys)
- What you **know** is the PIN (for your PIV card)
- What you **are** is a biometric (such as a fingerprint)

The more recent (December 2015) Draft of NIST Special Publication 800-116 Revision 1, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), defines a set of **security areas** (Unrestricted, Controlled, Limited, and Exclusion) that correlate with the FIPS 201-2 PIV Assurance Levels:

Security Area	# of Authentication Factors Required	Applicable PIV Authentication Mechanisms
Unrestricted	0	(none)
Controlled	1	**PKI-CAK**: Authentication with the Card Authentication Certificate Credential. **SYM-CAK**: Authentication with the optional Symmetric Card Authentication Key.
Limited	2	**BIO**: Authentication using Off-Card Biometric Comparison.
Exclusion	3	**BIO-A**: Attended Authentication using Off-Card Biometric Comparison. **OCC-AUTH**: Authentication using the optional On-Card Biometric Comparison. **PKI-AUTH**: Authentication with the PIV Authentication Certificate Credential.

NIST SP 800-116 also proposes a PIV Implementation Maturity Model (PIMM) for measuring the progress of agency and facility implementations towards an ideal state:

- At Maturity Level 1, there is only ad hoc PIV verification for the various security areas.
- At Maturity Level 2, there is systematic PIV verification for the Controlled security areas. Either PIV cards or currently deployed non-PIV cards are accepted for access to the Controlled security areas.
- At Maturity Level 3, there is access to the Exclusion security areas by PIV card or exception only. Non-PIV cards are not accepted for access to the Exclusion security areas.
- At Maturity Level 4, there is access to the Limited security areas by PIV card or exception only. Non-PIV cards are not accepted for access to the Limited or Exclusion security areas.
- At Maturity Level 5, there is access to the Controlled security areas by PIV card or exception only. Non-PIV cards are not accepted for access to the Controlled, Limited, or Exclusion security areas.

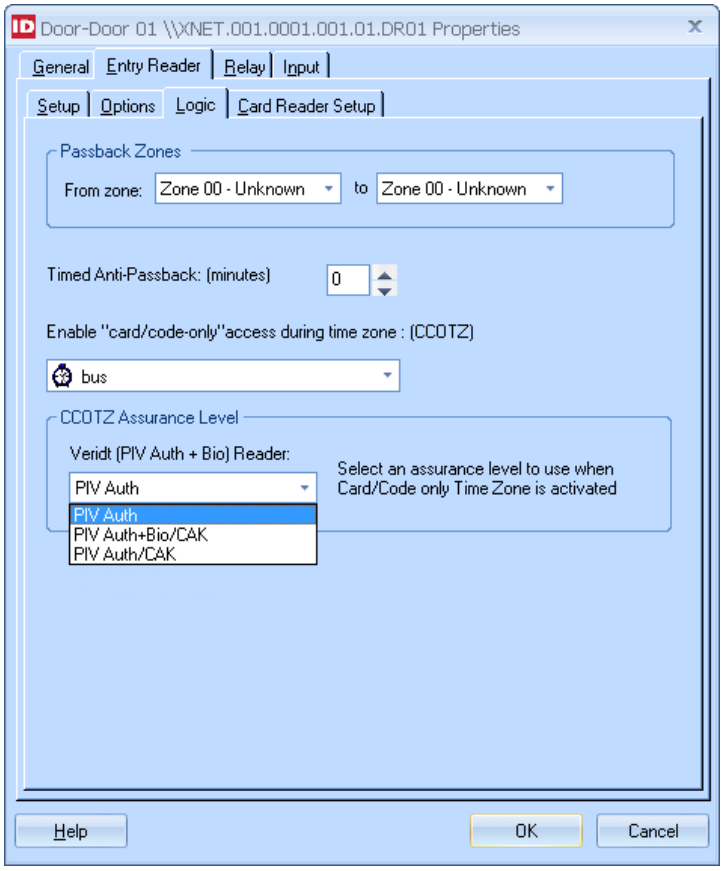
The expectation is that for a variety of practical reasons, you will gradually migrate from a traditional PACS to FICAM.

Specifying which Authentication Methods to use during a Card or Code Only Time Zone

Velocity offers several different ID formats (IDFs), some of which enable multi-factor authentication at a card reader with a keypad. The Card or Code Only Time Zone (CCOTZ) feature enables you to specify that during a particular time zone, at a card reader with a keypad that would normally require a person to both present a valid card and enter the correct PIN, the person can choose to either present the card or enter the PIN in order to be granted access. This can help reduce bottlenecks during times of high traffic volume.

This concept has been extended to help you as you migrate to FICAM, by enabling you to specify which authentication methods can be used at an RS-485/OSDP reader during a particular time zone. For example, you can specify that a uTrust TS government reader at the entrance to a Controlled security area will accept either PIV cards or non-PIV credentials when a security guard is on duty.

When the **RS485 Interface** value is selected for the Reader Interface option on the **Setup** page, the option for setting a lower **CCOTZ Assurance Level** appears on the **Logic** page of the Properties dialog for a door or a reader:



The choices appearing in this drop-down list are determined by the specific **Reader Type** selected on the **Setup** page.

The choices in the **Reader Type** drop-down list are:

- **TS**
- **TS-Scramblepad**
- **TS-Keypad**
- **Veridt (PIV-Auth)**, for the Veridt Stealth Dual reader
- **Veridt (PIV Auth + Bio)**, for the Veridt Stealth Bio reader

Other New Features and Enhancements

This section describes the new features and enhancements introduced in the Velocity 3.6 SP2.1 release for any Velocity system (not just those running Identiv's FICAM Solution).

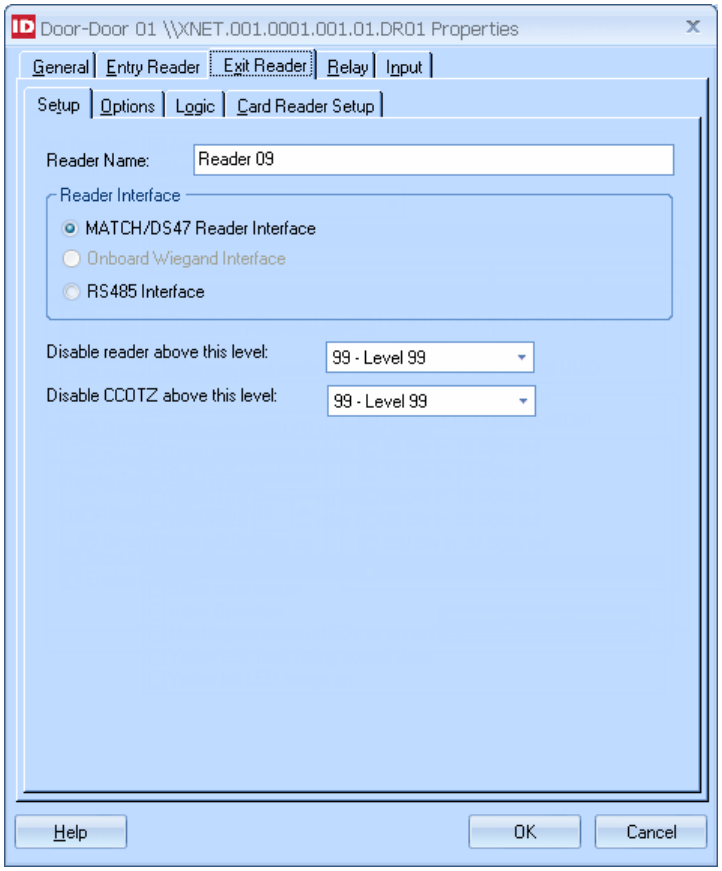
Unused Wiegand Terminals On Mx-2 and Mx-4 Controllers Are Available for Exit Readers

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. The following table shows the mapping of the 8 Wiegand terminals for the Mx-8, Mx-4, and Mx-2 models.

Terminal	Usage on Mx-8	Usage on Mx-4	Usage on Mx-2
Wiegand 1	Entry reader for Door 1	Entry reader for Door 1	Entry reader for Door 1
Wiegand 2	Entry reader for Door 2	Entry reader for Door 2	Entry reader for Door 2
Wiegand 3	Entry reader for Door 3	Entry reader for Door 3	(unavailable)
Wiegand 4	Entry reader for Door 4	Entry reader for Door 4	(unavailable)
Wiegand 5	Entry reader for Door 5	**Exit** reader for Door 1	**Exit** reader for Door 1
Wiegand 6	Entry reader for Door 6	**Exit** reader for Door 2	**Exit** reader for Door 2
Wiegand 7	Entry reader for Door 7	**Exit** reader for Door 3	(unavailable)
Wiegand 8	Entry reader for Door 8	**Exit** reader for Door 4	(unavailable)

NOTE: On an Mx-8 controller, the Wiegand terminals are all dedicated to entry readers. So when you use this feature to add Wiegand exit readers on an Mx-2 or Mx-4 controller, if you later decide to upgrade that controller to an Mx-8 model, you will need to rewire each Wiegand exit reader to use a MATCH board.

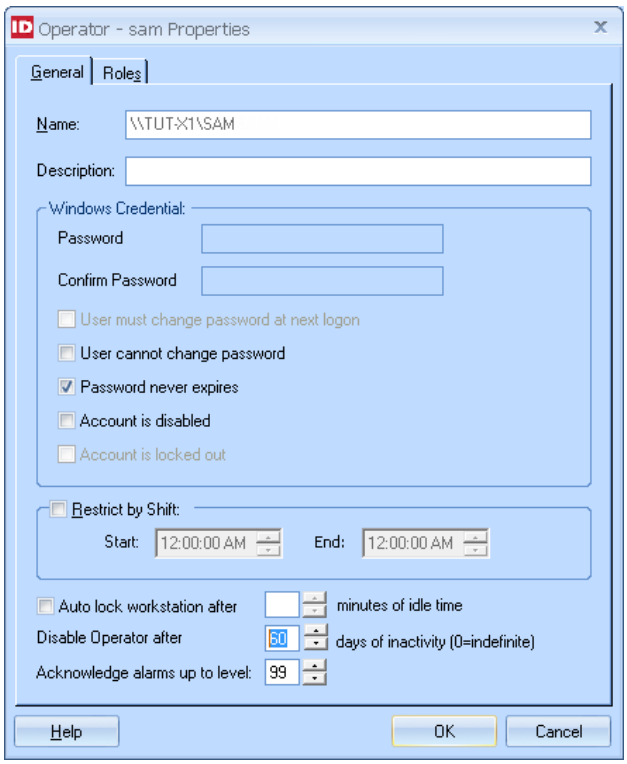
When a Wiegand terminal cannot be used for an exit reader, the **Onboard Wiegand Interface** choice for the Reader Interface option is greyed out:



Option to Automatically Disable Inactive Operators

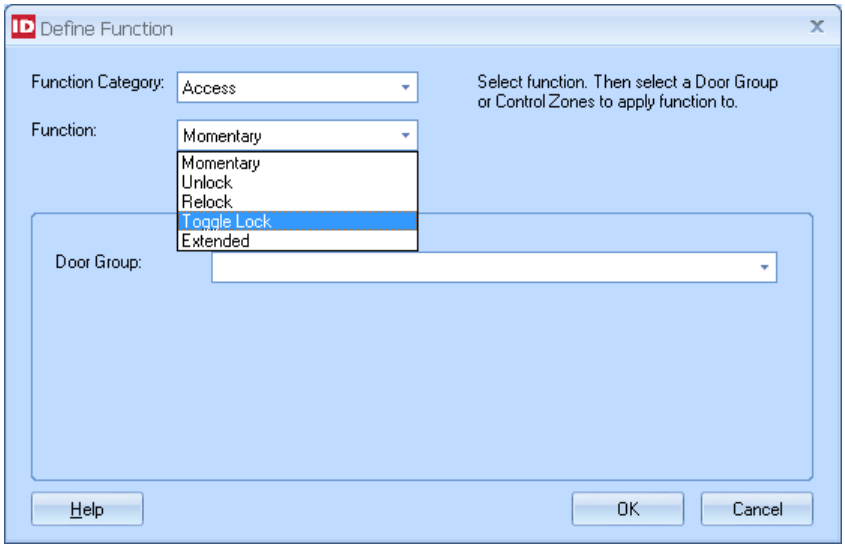
Revision 4 of the NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, includes Appendix F: Security Control Catalog. Security Control AC-2, Account Management, recommends that an information system automatically disables inactive accounts after a period of time which is determined by the organization.

The Velocity 3.6 SP2.1 release provides this security control as the option to "**Disable Operator after N days of inactivity**" on the **General** page of the **Operator Properties** dialog. Note that this option is set individually for each operator, enabling you to specify the period of time which is appropriate for the assigned roles.



New access function to Toggle Lock

Velocity has a new Access function named **Toggle Lock**. When no other relay programming is active, this new function enables a single card, PIN code, extension digit, or other credential format to toggle any relay-controlled device (such as a lobby door or an HVAC system) between its on and off states.



New low-priority control functions (Suppress Operate and Suppress Operate Release) for relays

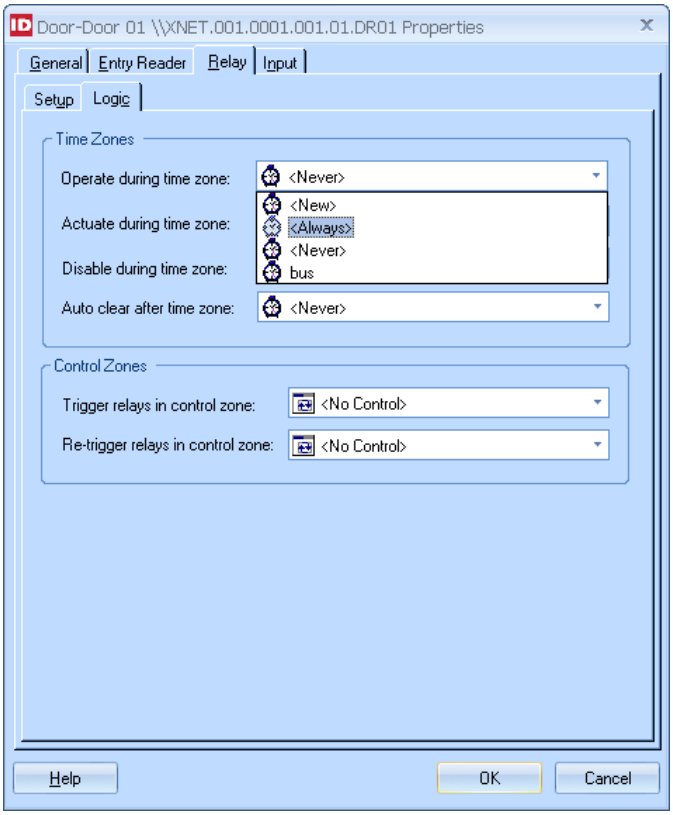
Velocity has added two new relay control functions named **Suppress Operate** and **Suppress Operate Release**. Along with **Operate by Time Zone**, these new functions have the lowest priority.

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.

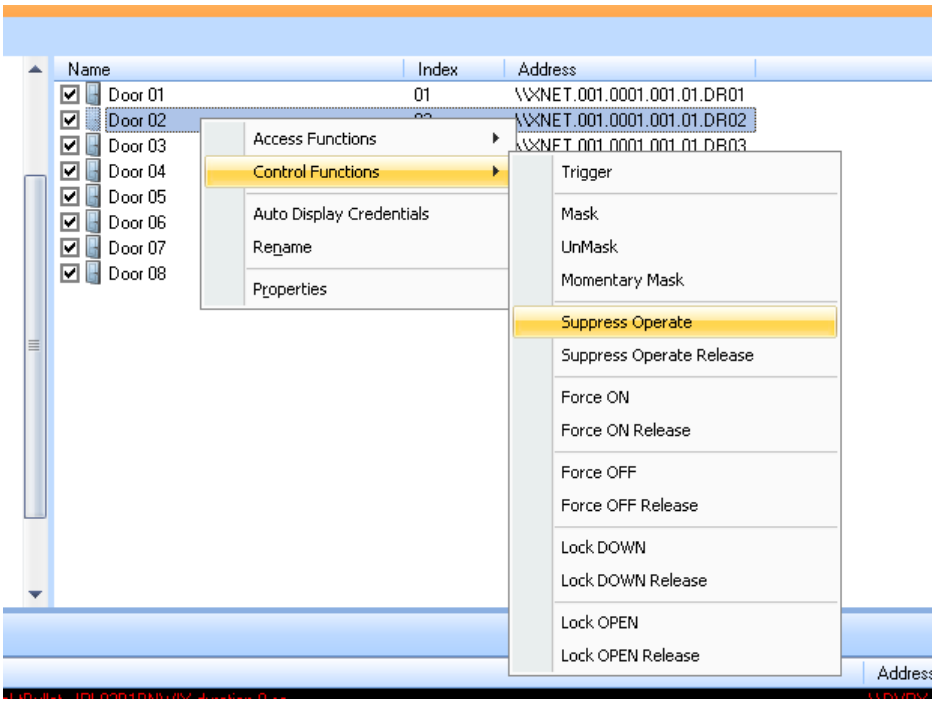
The **Suppress Operate** relay control function temporarily overrides (suppresses) only the **Operate by Time Zone** function, so that you can prevent access to the general public during unusual situations such as the receptionist or security guard not being present. (Personnel with the proper credentials 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.

Relay control functions can be used in several different ways:

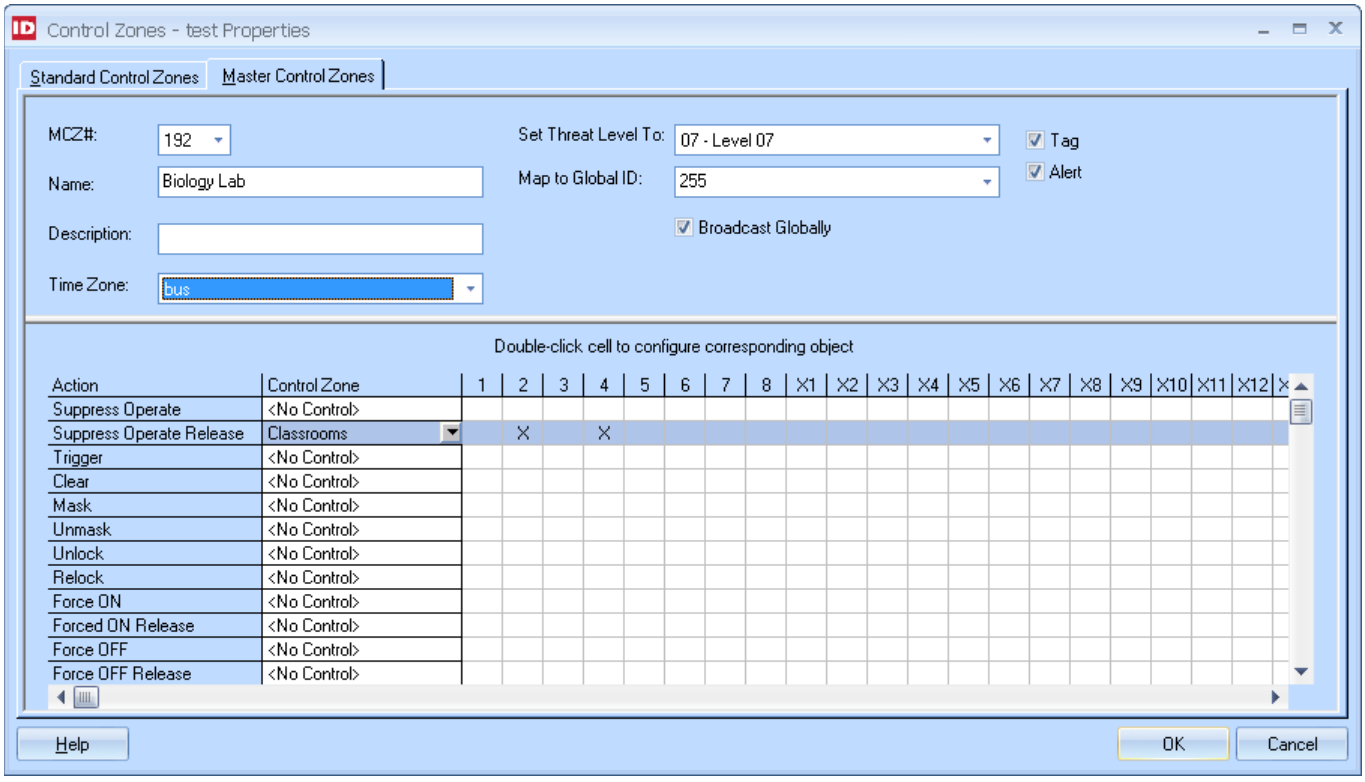
- programming a relay by Time Zones or Control Zones is done on the **Logic** page of the Properties dialog for a door or a relay



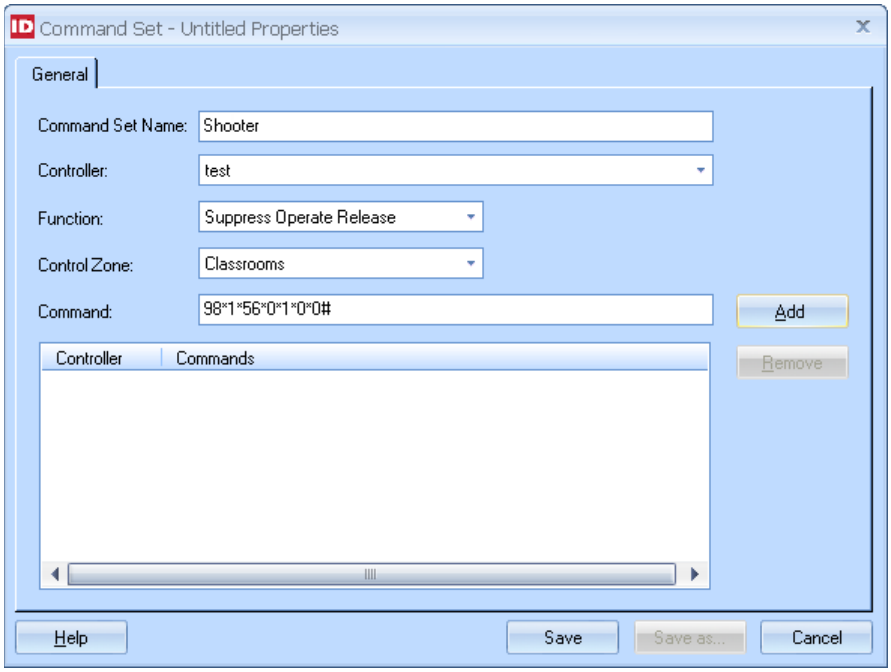
- manually operating a door's relay is done using right-click menu commands (such as **Control Functions ▸ Suppress Operate**)



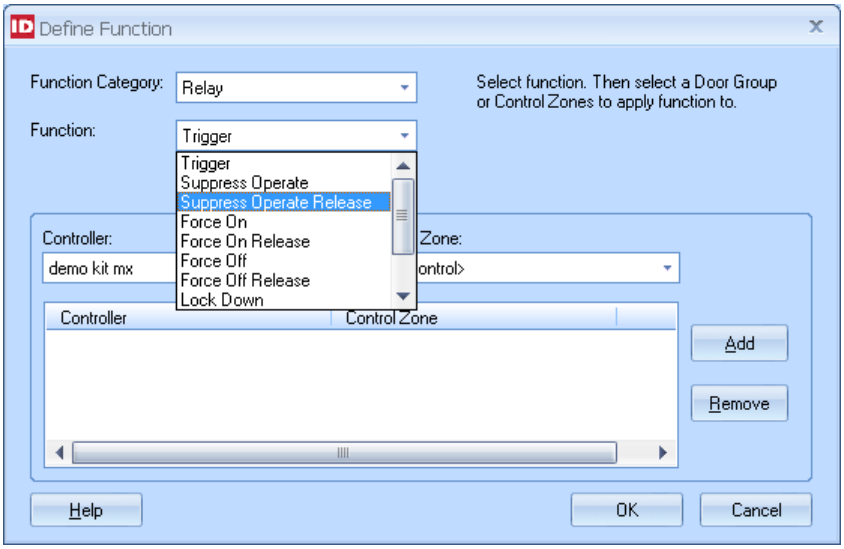
- programming a relay by Master Control Zones is done on the **Master Control Zones** page of the Properties dialog for a Control Zone



- programming a relay can also be done using a **Command Set**



- a relay function can be used to define a **Credential Function**



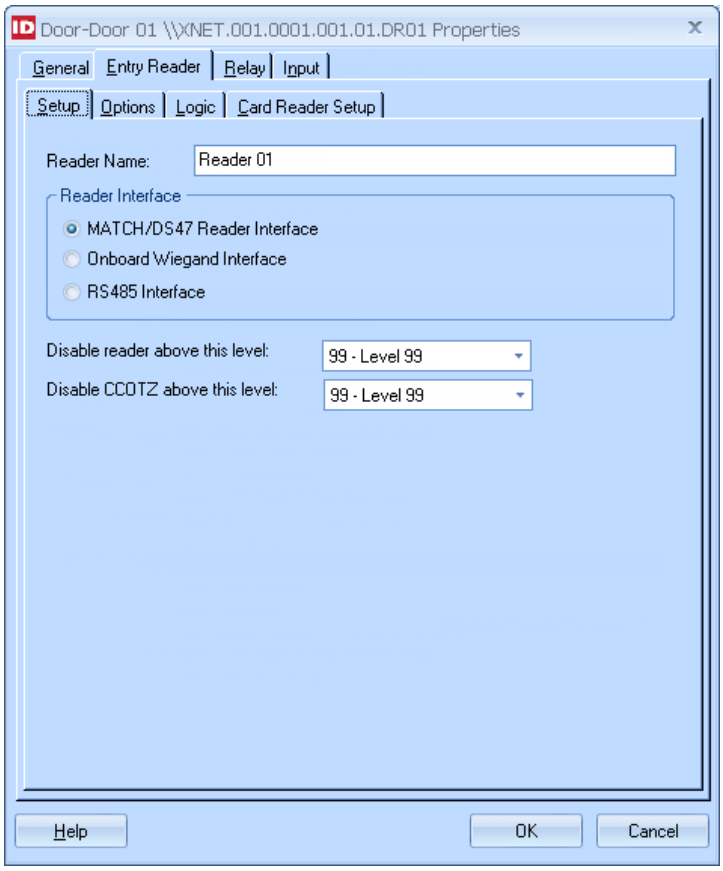
Redesign of Reader Properties and Door Properties Dialogs

With the addition of the RS-485/OSDP type of readers (which are required for FICAM), it became necessary to redesign some pages of the Properties dialogs for a reader or a door. The following changes were made in the Velocity 3.6 SP2.1 release:

- On the **Setup** page, the **Reader Interface** option was moved here (from the Card Reader Setup page), with its radio buttons for choosing between **MATCH/DS47 Reader Interface**, **Onboard Wiegand Interface**, or **RS485 Interface**. When the **RS485 Interface** value is selected for the Reader Interface option, additional options are displayed, including a **Reader Type** drop-down list of specific reader models.
- The specified **Reader Type** determines the content of the **CCOTZ Assurance Level** drop-down list on the **Logic** page. When an Identiv TS reader is specified, the **Setup** page also includes an **Update Reader Firmware…** button. (For information about that new feature, see Downloading Firmware Updates to a TS Reader from Velocity.)

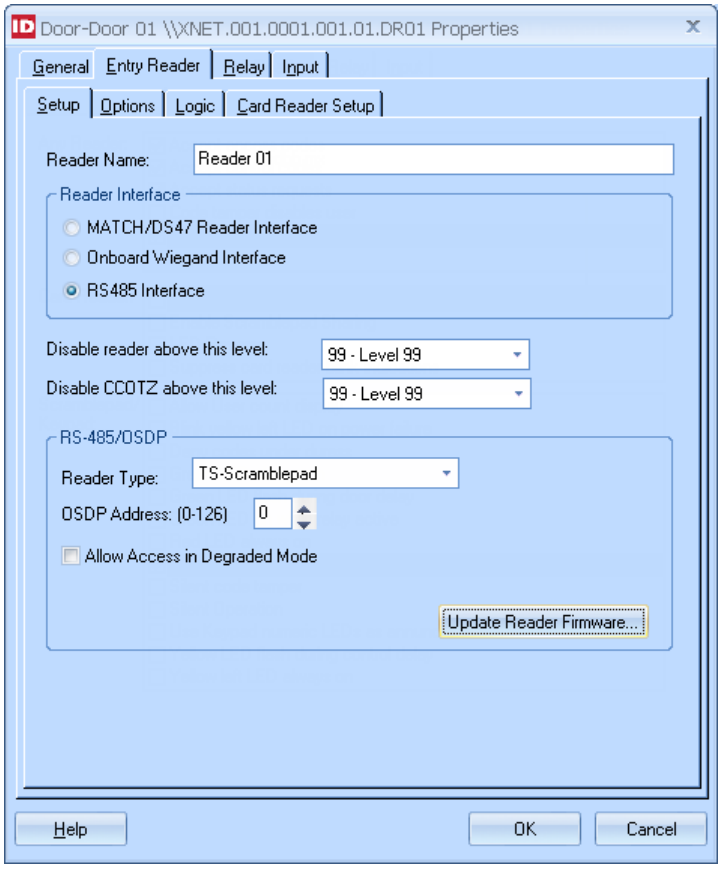
- The previous ScramblePad Options page was renamed to just **Options**, and the numerous options were organized into three categories for **Any Reader**, a **Card Reader**, or a **Scramblepad / Keypad**.
- On the **Logic** page, the **CCOTZ Assurance Level** drop-down list was added for a reader with the **RS485 Interface**.
- On the **Card Reader Setup** page, these changes were made:
  - The selection of the **Reader Interface** type was moved to the **Setup** page. (The value selected determines the set of options that is displayed on the **Setup** page.)
  - The **LED Reverse** and the **Enable ScramblePad Sharing** options were moved to the Card Reader category on the **Options** page.
  - The **OSDP Address** field and the **Allow Access in Degraded Mode** option (for an RS-485/OSDP reader) were moved to the **Setup** page.

The remainder of this topic provides some example pages of the Properties dialog for different types of readers.



- When a reader is connected to the controller through a MATCH board, select the **MATCH/DS47 Reader Interface** value for the Reader Interface option.
- When a Wiegand reader is connected to an Mx controller using the onboard Wiegand terminal for a door, select the **Onboard Wiegand Interface** value for the Reader Interface option. (See Unused Wiegand Terminals on Mx-2 and Mx-4 Controllers are Available for Exit Readers for information about that new feature.)
- When a FICAM-capable reader is connected using OSDP through a port on an RS-485 Readers Expansion Board (RREB), in a controller which also has a SNIB3, select the **RS485 Interface** value for the Reader Interface option. Then select the appropriate reader model from the **Reader Type** drop-down list.

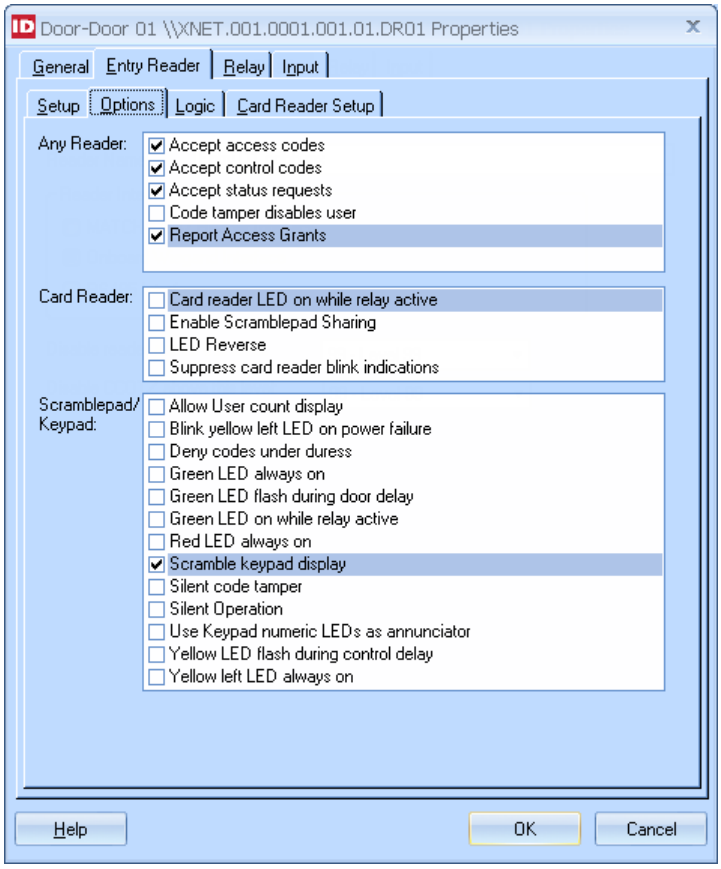
  The choices in the **Reader Type** drop-down list are:
  - TS
  - TS-Scramblepad
  - TS-Keypad
  - Veridt (PIV-Auth), for the Veridt Stealth Dual reader
  - Veridt (PIV Auth + Bio), for the Veridt Stealth Bio reader



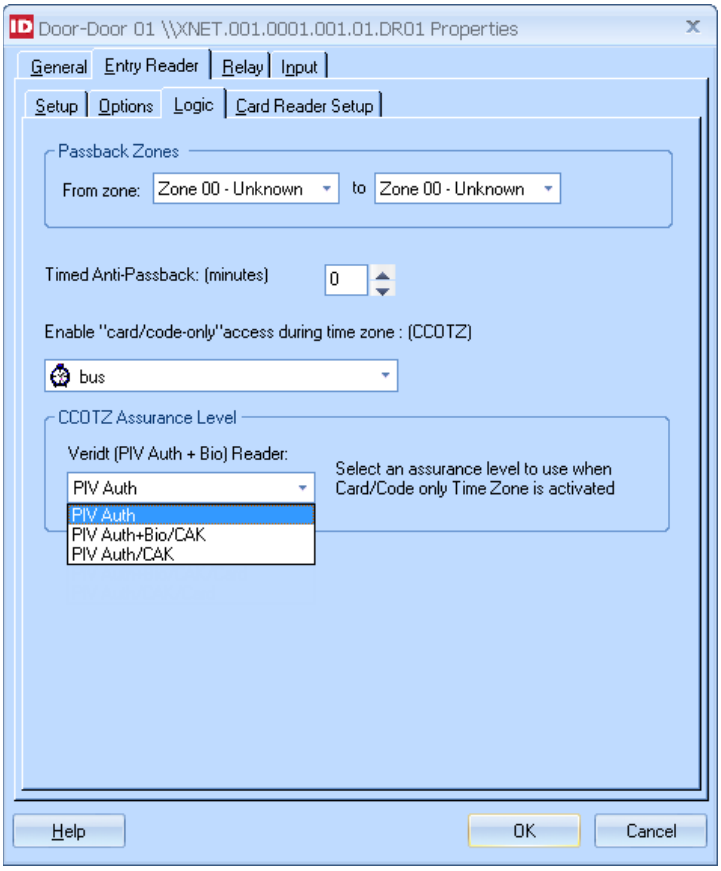
Be aware that:

- The value selected for the **Reader Interface** option also determines the set of options that appear on the **Card Reader Setup** page.
- The value selected in the **Reader Type** drop-down list on this page affects the content of the **CCOTZ Assurance Level** drop-down list on the **Logic** page.
- The **Update Reader Firmware…** button is present only when the **RS485 Interface** value is selected for the Reader Interface option and the selected **Reader Type** is one of the available TS readers by Identiv.

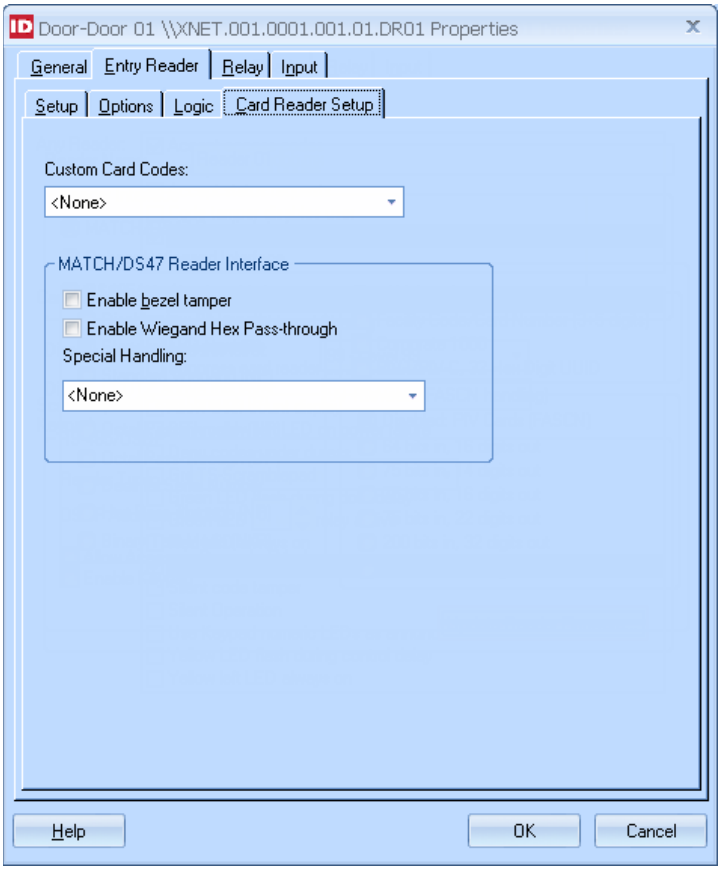
  TIP: In this release, the version information for a TS reader's firmware can be viewed in Velocity's **Diagnostic Window**. (In a future release, some version information will also be displayed on this page.)



Note that the numerous options have been reorganized into three categories for **Any Reader**, a **Card Reader**, or a **Scramblepad / Keypad**. (Within each category, the options appear in alphabetical order.)



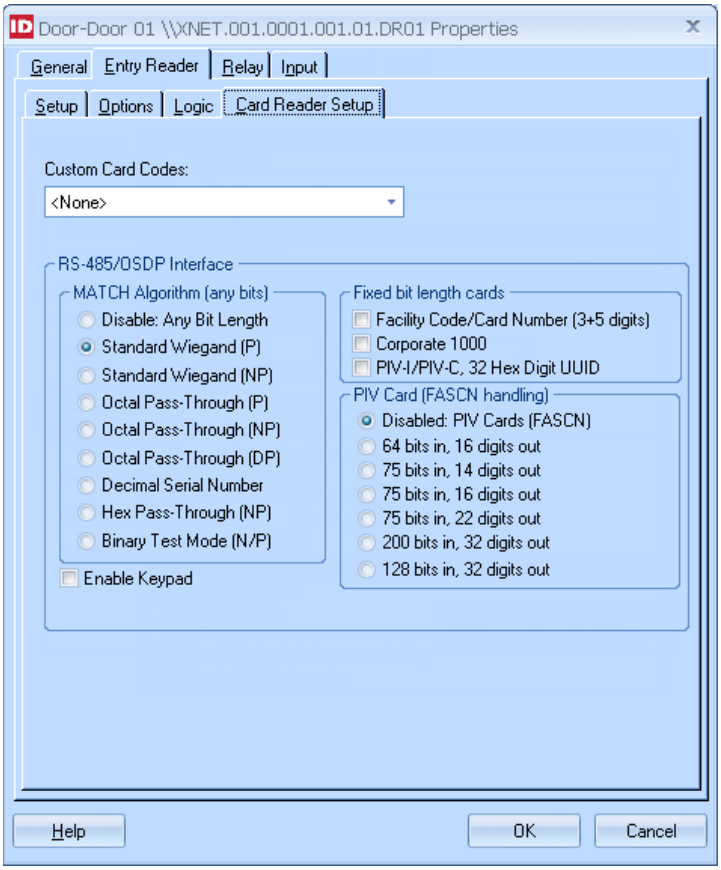
When the **RS485 Interface** value is selected for the Reader Interface option on the **Setup** page, the option for setting a lower **CCOTZ Assurance Level** appears on the **Logic** page. The choices appearing in this drop-down list are determined by the specific **Reader Type** selected on the **Setup** page. (For information about this new feature, see CCOTZ Assurance Level.)



Note that the following changes were made on this page:

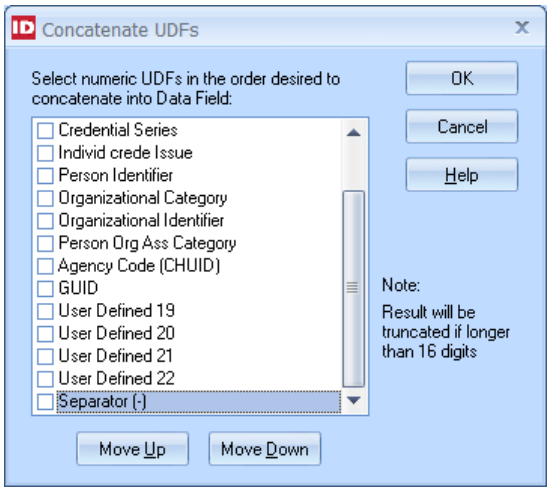
- The selection of the **Reader Interface** type was moved to the **Setup** page. (The value selected there determines the set of options that is displayed on this Card Reader Setup page.)
- The **LED Reverse** and the **Enable ScramblePad Sharing** options were moved to the Card Reader category on the **Options** page.
- The **OSDP Address** field and the **Allow Access in Degraded Mode** option (for an RS-485/OSDP reader) were moved to the **Setup** page.

The following screen capture shows the set of options that is displayed when either **Onboard Wiegand Interface** or **RS485 Interface** is selected for the **Reader Interface** type on the **Setup** page.

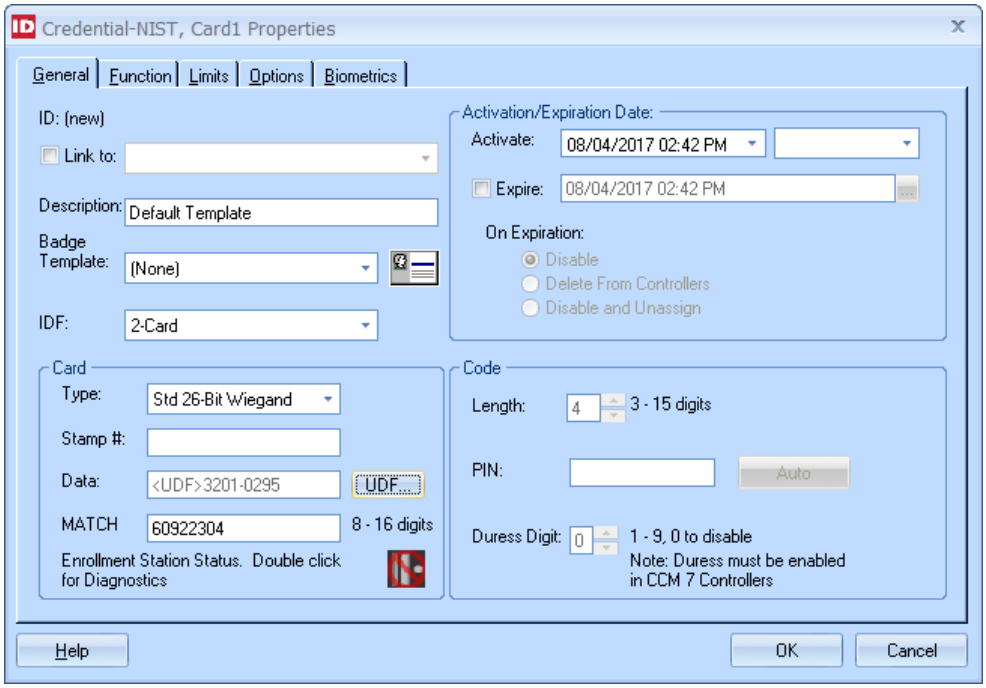


Ability to Use a Separator Character when Concatenating User-Defined Fields

Velocity now enables you to specify that concatenated user-defined fields contain a dash as a separator character. This is helpful when your enrollment process involves importing user data that includes this character, such as <FacilityCode>-<SystemCode>. The new **Separator** item appears at the end of the list on the **Concatenate UDFs** dialog, and when used can be moved up or down to position it within the data:



The concatenated data which includes the separator character is then used to generate a MATCH code or a FASCN.



Miscellaneous Performance Enhancements

This release includes the following performance enhancements:

- (VEL-4104) Removed unnecessary SyncData calls from a Velocity client to all other clients on the system.
- (VEL-4121) Improved the performance of the Polling Engine's message queue, by changing the "high water mark" to allow more room before the queue is full, and only posting a message when the queue transitions from empty or hits the "high water mark".
- (VEL-4126) Disabled DisplayEvent from sending anything to the Velocity Security Domain Service, and stopped sending DisplayEvents to the Velocity Security Domain Service and Velocity clients (because they have no use in Velocity).
- (VEL-4134) Prevented excessive port connection retries by having the Polling Engine use a port connection separation time (in addition to the existing port connection retry time).

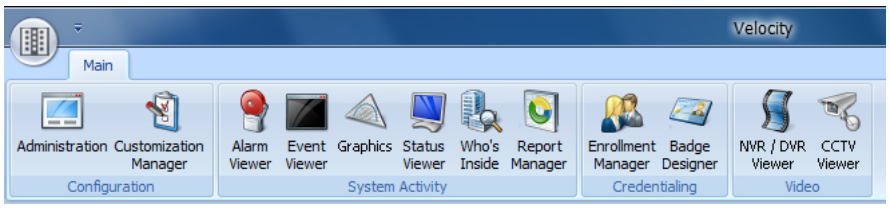
Bug Fixes

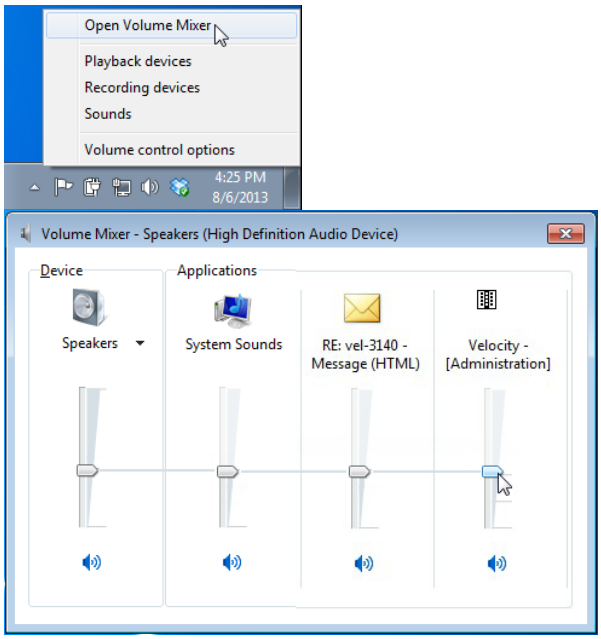
Reference ID	Bug	Description
VEL-3089	After KB640, the Central Station Alarm Receiver's port kept changing to COM0	After applying the KB640 update to Velocity 3.1, the Central Station Alarm Receiver feature stopped working because its COM port setting was mistakenly being changed to the invalid value of "\\MachineName\COM0". (If you tried to change the value to the desired COM port, it kept being changed back to COM0.) The workaround was to temporarily change the port type to TCP/IP and save those settings; stop and restart the Extensions service; and then change the port type to Serial with the desired COM port. This issue has been fixed.
VEL-3250	SCM Settings dialog would not open in a clustered server environment	In a clustered server environment, Velocity's Service Control Manager Settings dialog would not open on either of the server nodes. The only workaround was to manually edit the appropriate tables in Velocity's database. (At customer sites with a rigorous software change management process, this issue made it difficult and time-consuming to turn debugging on and off.) This issue has been fixed.
VEL-3285	NumberOfDaysTo Keep option in VelocityDebug.ini was not working as intended	If a customer restarted the Velocity services multiple times, log files could have been lost because the NumberOfDaysToKeep option in VelocityDebug.ini was not working as intended. This issue has been fixed. Now when Velocity starts up, it will: 1. Rename <logfile>.txt to <logfile>_<DateStamp>.txt, and 2. Remove any file where the name matches <logfile>_<YYYYMMDDhhmmss>.txt and which is older than NumberOfDaysToKeep.
VEL-3607	An unexpected exception could occur if a port was disabled during a download	An unexpected exception could occur if a port was disabled while credentials or configuration was being downloaded. To prevent problems caused by queued messages arriving after a port has been disabled, the port shutdown process was changed to an asynchronous operation. This issue has been fixed.
VEL-4073	Download Monitor could show an active batch as still queued	In certain situations, the Download Monitor would show an active batch as still being queued. This issue has been fixed. NOTE: The Download Monitor was changed to use VelocityDebug.dll; the LogBatchStatus option in VelocityDebug.ini controls the logging of the Download Monitor's BatchStatusUpdate information.
VEL-4077	No event was displayed when manually executing a function on a disabled port	Previously, nothing was displayed in the Event Viewer when you manually executed a function (such as granting momentary access to a door) on a disabled port. Instead, an unexpected exception was recorded in the DTServer's log file. This issue has been fixed, so the Event Viewer displays an event explaining that the attempted function failed because the port is disabled.

Reference ID	Bug	Description
VEL-4105	Velocity was incorrectly limiting the database size to 4GB for SQL Server Express 2008R2 or later	For recent versions of the free Express edition of SQL Server, Velocity's database archiving process was incorrectly limiting the database size to the previous 4GB maximum supported by previous versions. This issue has been fixed. Now Velocity recognizes that the database size limit is 10GB for the following versions of SQL Server Express: • SQL Server Express **2008R2** (10.50.6000.34) • SQL Server Express **2012** (11.0.6020.0) • SQL Server Express **2014** (12.0.5000.0) • SQL Server Express **2016** (13.0.4001.0)
VEL-4128 and VEL-4131	Incorrect door address shown for conditional unmask and pre-arm status	An incorrect door address was shown in the Event Viewer for some events, such as conditional Unmask and pre-arm status. This issue has been fixed.
VEL-4130	Renaming a door's exit reader, input, or relay did not take effect until SDService was restarted	After the exit reader in a door bundle was renamed, the change did not take effect until Velocity's Security Domain service was restarted. The same issue was occurring for the input and the relay in a door bundle. These issues have been fixed.
VEL-4159	Command error events could not be customized	Previously, the Customization Manager did not include command error events. (This prevented a customer from suppressing "user not found" events.) This issue has been fixed. Now the command error events are fully supported by the Customization Manager.
VEL-4169	Installer may stop while trying to get the Current Windows User Name	The Velocity Installer sometimes stopped while trying to obtain the Current Windows User Name. This issue has been fixed, by adding the ByRef keyword to the API call (which previously had not been needed).
VEL-4175	Update some Help IDs for the revised Velocity Scheduling Agent	The role permissions for the Scheduling Agent were significantly redesigned in the Velocity 3.6 SP2 release, and the Scheduling Agent section of the Velocity online help was significantly revised. A couple of issues were discovered: • A Help ID was needed for the Role page of the Scheduler Wizard. • The Help ID being used for the topic about the Email Reports type of scheduled task had to be changed because it was already being used (by the topic about Changing Time Zones for Door Groups). These issues have been fixed.
VEL-4187	Transaction dispositions 35 and 36 were reporting incorrectly	Transaction dispositions 35 and 36 were incorrectly reporting as disposition 21 (Event 2021) in the Event Viewer. Disposition 21 is a related event containing the second half of the card data. This issue has been fixed, by using a temporary object to construct the complete result for a transaction disposition 35, 36, 42, or 43 event and its corresponding transaction disposition 21 event.

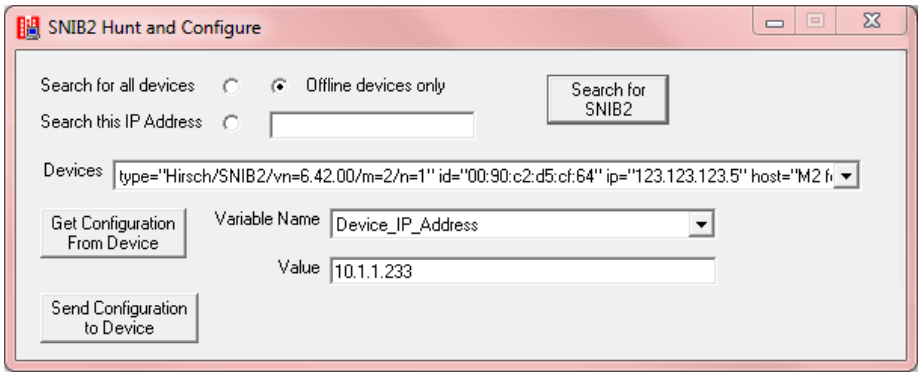
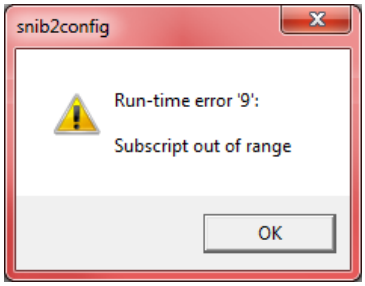
Reference ID	Bug	Description
VEL-4191	Velocity Client might fail to start, if a Velocity Web Services update was installed on the server	If a Velocity Web Services update was installed on the Velocity Server, when the traditional Windows-based Velocity Client started up, the client might think there is an update that needs to be downloaded and run. But the Velocity Client was not aware that this is a server-only update so there is no file to download. (The workaround was to add specific information about this update to your Velocity Client's LocalManifest.ini file, so it thought it had been updated.) This issue has been fixed, so the Velocity Client knows that it does not need to be updated if there is no file to download.
VEL-4225	Upgrading to 3.6 might fail on a Velocity system using custom group names	When a Velocity system which uses Custom Group Names was upgraded to the 3.6 release, the upgrade could fail when trying to apply SQL object permissions using the [Velocity Services] group. (Only the [Velocity Users] app role needs to be applied.) This issue has been fixed, by no longer trying to apply SQL object permissions using the [Velocity Services] group.
VEL-4233	Controller date/time information was missing from reports	While trying to remove the controller date/time information from the Edge EVO controller integration's alarms raised by software, the column name was changed, which broke existing reports (so that the controller date/time information was missing for all events). This issue has been fixed.
VEL-4236	Expansion input's address shown (instead of reader's address) for a manually executed access function	The Event Viewer's Address column was showing an expansion input address (instead of the reader's address) for a manually executed access function such as granting momentary access to a door. This issue has been fixed.
VEL-4240	Unexpected error while trying to add a function group	While adding a new function group, an unexpected error was thrown (instead of opening the Define Function dialog) after clicking the Add button on the Define Extension dialog. This issue has been fixed.
VEL-4241	Expiration Date of PIV card not parsed for FICAM's UDF mapping	For FICAM, an Expiration Date for a credential based on a User-Defined Field was not working properly. This issue has been fixed. Now when you first scan a PIV card during the enrollment process, its expiration date appears in the universal date format of YYYY-MM-DD. After you save the card's data, the date in a user-defined field is displayed according to the regional settings on your computer (for example MM/DD/YYYY).
VEL-4278	Right-clicking on an expansion relay could generate an overflow error	Right-clicking on an expansion relay in the Velocity Administration window could generate an overflow error, if the relay's ID number in the Velocity database is greater than 32767. This issue has been fixed, by having the right-click menu use the Long data type (instead of the Int data type).
VEL-4323	Addressing of exit readers was incorrect in the Graphics module	In the Graphics module, the addressing of the optional exit reader for a door was incorrect. This meant that Graphics was not properly handling the alarms and events for exit readers. This issue has been fixed.

Known Issues

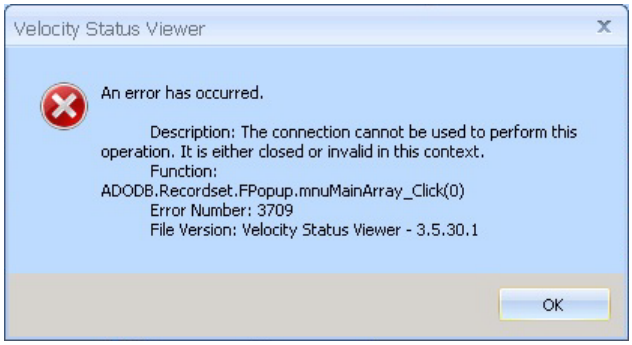
Reference ID	Summary	Description
VEL-2558	DIGI*TRAC Network Service does not always start automatically (after rebooting the Velocity server)	Normally after rebooting the computer that is your Velocity Server, the necessary services are automatically restarted. But on some slower computers, the Velocity DIGI*TRAC Network Service might not automatically start because Windows was killing the process (if it did not complete within 30 seconds). If you experience this issue, the possible workarounds are: • Change the value of the Startup Type property of the Velocity DIGI*TRAC Network Service to Automatic (Delayed Start). Note that doing so can significantly increase the time before the service starts and the Velocity Service Control Manager's icon (in the Windows system tray) turns green. • Add an entry to the Windows Registry that increases the kill timer (for all services) from its default value of 30 seconds; we recommend 180 seconds. For example: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control] "ServicesPipeTimeout"=dword:0002bf20
VEL-2690	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). In general, the Velocity server should not be used to perform client type functions.
VEL-2750	After installing a new version of Velocity, the ribbon toolbar in Velocity's main window sometimes loses its icons (and only displays text)	The ribbon toolbar in Velocity's main window typically looks like this:  But sometimes after installing a new version of Velocity, the toolbar loses its icons and only displays text, so it looks like this:  The workaround is to reset the ribbon toolbar to its default settings, and restart Velocity. **NOTE:** This will undo any customizations you had made to the toolbar.
VEL-3027	Pelco DVR not functional on 3.5 SP1 (or later)	Starting with the Velocity 3.5 SP1 release, you cannot connect to a Pelco DVR.

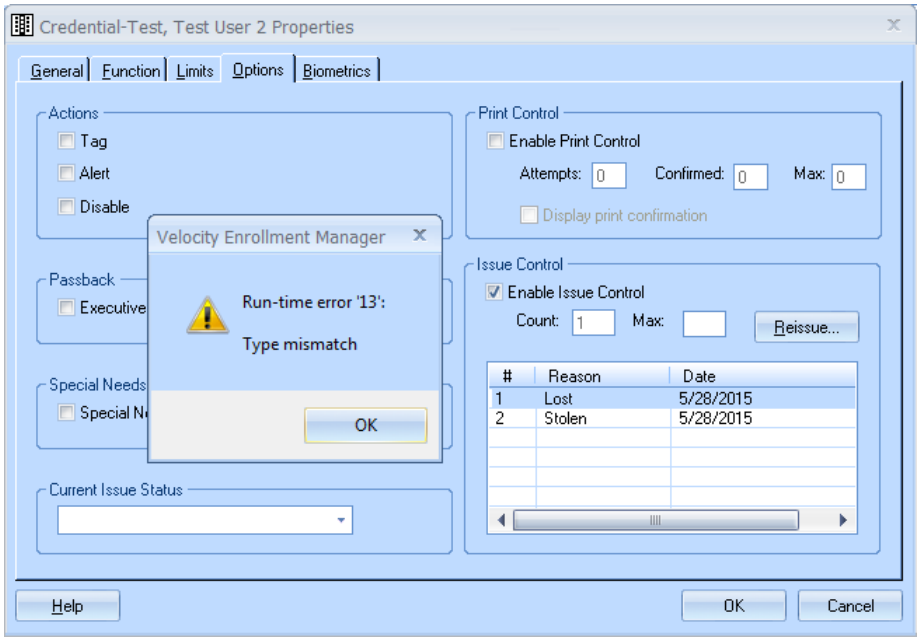
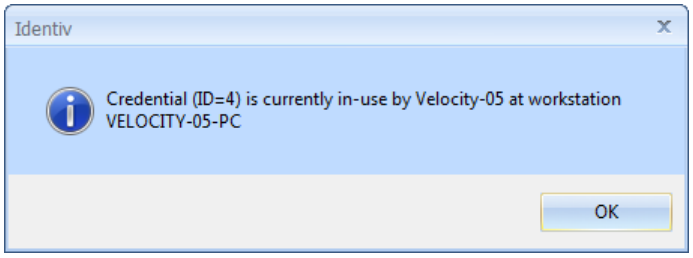
Reference ID	Summary	Description
VEL-3140	Custom alarms do not play on some machines	On some computers running Windows Vista or later, custom alarm sounds are not heard (either in the Customization Manager or in the Alarm Viewer). Although the exact cause of this issue is unknown, the reason that the sounds are not heard is because the Velocity application's volume is set to 0% (mute) in the Windows Volume Mixer. The workaround is to open the Windows Volume Mixer (by right-clicking on the speaker icon in the system tray and choosing the Open Volume Mixer command from the pop-up menu), and increase the volume for the Velocity – [Administration] application (by dragging its slider bar up). 
VEL-3268	The Enrollment Manager's window sometimes opens with a maximized height.	Normally, the Enrollment Manager's window opens at a standard size. But if the window was maximized when it was closed, the next time the Enrollment Manager is opened, its window will have a maximized height (instead of the default height). There is no workaround for this issue.
VEL-3287	If periods are used as separators in a UDF with the Type of Date, the value is changed to a time of 12:00:00 AM.	On an English language system, a user-defined field with the Type of Date expects the date to be entered in the form of MM/DD/YY or MM/DD/YYYY, where forward slashes are used to separate the 2-digit month from the 2-digit day of the month and the 2-digit or 4-digit year. If you try to use periods instead of forward slashes for the separators, the value you enter is automatically converted to a time of 12:00:00 AM. The workaround is to enter the date using the expected forward slashed to separate the month, day, and year.
VEL-3299	If a computer has only one serial port, a serial CCTV port's settings cannot be changed.	On a computer which has only one serial port, if you open the Properties dialog for a serial CCTV port, its Port Settings fields are disabled so you cannot change their values. The only workaround is to delete the existing port, then create a new port with the desired settings.
VEL-3310	An application error occurs if no value is specified for the Port of a serial CCTV port.	When creating a serial CCTV port, an application error will occur if you do not specify a value for the required Port field. The workaround is to try creating the port again, and make sure that you specify a value for the Port (by selecting an entry from the Port drop-down list).

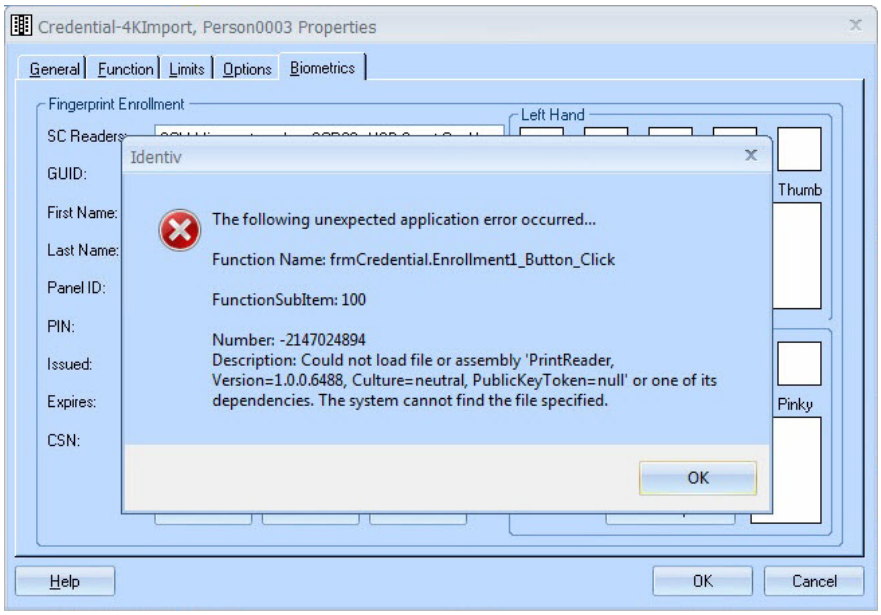
Reference ID	Summary	Description
VEL-3356	Incorrect date/time is shown for an alarm video triggered on an AD VideoEdge NVR (using Velocity's legacy support)	The Recorded Alarm Video window shows an incorrect date/time stamp for an alarm video triggered on an American Dynamics VideoEdge NVR that is using the legacy support provided in Velocity. A possible workaround is to use the new American Dynamics plug-in to the Hirsch Video Integration, which supports either an Intellex DVR or a VideoEdge NVR.
VEL-3365	Titles and column headers are truncated or misplaced when a report is exported to an Excel spreadsheet.	Although a report's titles and column headers are displayed correctly in Report Manager, they can be truncated or misplaced when the report is exported to a Microsoft Excel spreadsheet. The only workaround is to manually correct the report titles and column headers in the Excel spreadsheet.
VEL-3390	Enrollment station sometimes will not read additional cards when finding a credential by MATCH code.	The Enrollment Manager has a **Tools ▸ Find Credential…** command that open the Find Credential dialog, which includes a MATCH Code option. If you use that option and then open a credential from the Search results pane, after closing the credential and returning to the Find Credential dialog, the enrollment station will not read another card. The workaround is to close the existing Find Credential dialog and issue the Tools ▸ Find Credential… command again.
VEL-3391	After changing a door group in the Administration window, the focus switches to the first item in the Components pane.	When the **Velocity Configuration ▸ Door Groups** folder is selected in the system tree pane of Velocity's Administration window, the focus that indicates which item is selected in the Components pane switches to the first item after you make a change to an existing door group. There is no workaround for this issue.
VEL-3397	Update installation fails if Velocity's help system is open.	If Velocity's online help system is open during the installation of a Velocity update, the installation will fail with a "Path/File access error" when it tries to overwrite the Velocity.chm file (which is currently in use). The workaround is to close Velocity's online help system and start the installation again. (If you must keep the help system open, copy the Velocity.chm file to a different folder, and double-click on the copied file to open Velocity's help system.)
VEL-3400	After you install a Velocity update, the Alarm Viewer is sometimes initially blank.	When Velocity's main window is automatically opened after the successful installation of a Velocity update, the Alarm Viewer is sometimes blank (with just a light blue background). The workaround is to close this blank Alarm Viewer window, and then open the Alarm Viewer again.
VEL-3413	The Cogent CSD200i driver is not working for biometric enrollment.	Cogent replaced its model CSD200 enrollment reader by the model CSD200i, which has an updated driver file. This updated driver file causes Velocity to generate a "No Biometric Reader found" error. The workaround is to make the new CSD200i enrollment reader use the old driver file (which was supplied with the model CSD200).
VEL-3421	Velocity cannot communicate with a controller using a 2-digit serial port number.	Velocity cannot communicate with a controller that is using a 2-digit serial port number; the port number must be a single digit. The workaround is to change the controller's serial port to an available port which has a single-digit number.

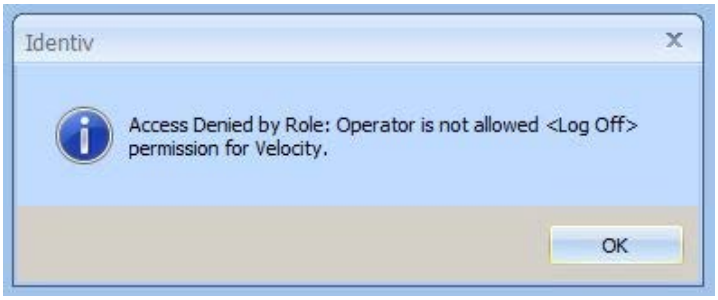
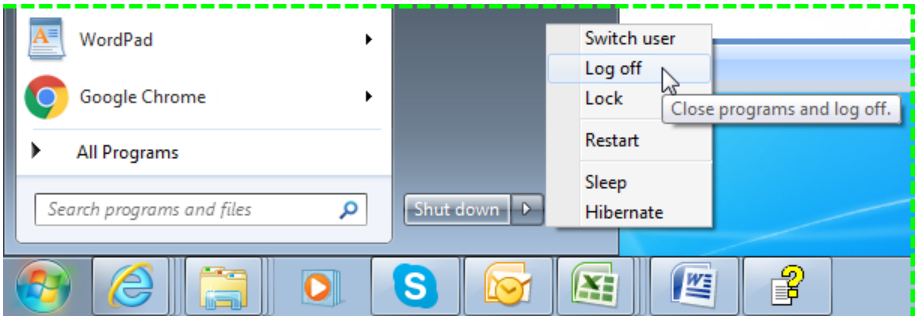
Reference ID	Summary	Description
VEL-3440	The Searching… dialog does not display complete information when there are many controllers with SNIB2 boards.	On a system where there are many controllers with SNIB2 boards, the Searching… dialog (which appears after you click the Search button on the Properties dialog of a port with the Network Type of TCP/IP selected and the "XNET 2 protocol" option checked) sometimes does not display complete information. There is no workaround for this issue.
VEL-3441	Clicking on the Search for SNIB2 button generates an error when there are too many devices to be listed	The SNIB2 Configuration Tool has a **Search for SNIB2** button:  But if there are too many Devices to be listed, the following error message is displayed:  There is no workaround for this issue. However, starting with the Velocity 3.6 release, the SNIB2 Configuration Tool has been superceded by a new SNIB Configuration Tool that also supports IPv6 addressing (which is a feature of the new SNIB3 board that is being developed).
VEL-3473	The Customization Manager does not allow you to type the characters { or } in an event message.	In the Customization Manager, you cannot type the following special characters in the New Value field of an Event: • **{** (left curly bracket) • **}** (right curly bracket) The workaround is to type those characters in some other application, copy those characters (to the Windows clipboard), and then paste them into the New Value field.
VEL-3484	The Report Manager's Event Customization report does not include any events for the new Edge EVO system.	The Report Manager's Event Customization report was not updated to include any events for the new Edge EVO system. There is no workaround for this issue.
VEL-3485	The Report Manager's Operator Log report does not include some events.	Some operator actions (such as performing an access function at a door) are shown in the Event Viewer, but are not included in the Report Manager's Operator Log report. These missing events do appear as Programming events in the All Events report.

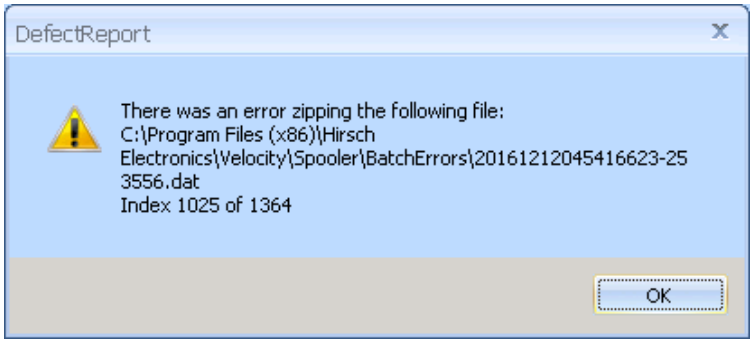
Reference ID	Summary	Description
VEL-3490	After switching from an operator whose role does not have permission to use the SNIB2 Import wizard, an Administrator is also denied access to that wizard.	After a Velocity client is switched from an operator whose role does not include the **Application Permissions ▸ Velocity ▸ SNIB2 Import Wizard – Use** permission to an Administrator (who has full permissions), the Administrator is also denied access to the SNIB2 Import wizard. The workaround is to restart the Velocity client and log in using an account that has the necessary role permission (instead of just switching operators).
VEL-3494	The Alarm Viewer does not apply the "Use 24 Hour Time Format" preference to previous alarms.	After you enable the **Use 24 Hour Time Format** option (on the General tab of the Velocity Preferences dialog), when you open the Alarm Viewer new alarms are displayed using the 24-hour time format, but the previous alarms continue to be displayed using the local time format specified in Windows. There is no workaround for this issue.
VEL-3495	When the Alarm Viewer's Force Fixed Column Sorting option is off, alarms in the Acknowledged pane sometimes are not sorted properly.	When the **Force Fixed Column Sorting** option (on the Sorting tab of the Alarm Viewer Properties dialog) is unchecked, the alarms in the Alarm Viewer's Acknowledged pane sometimes are not sorted in the expected order. The workaround is to manually refresh the Alarm Viewer.
VEL-3496	The "Restrict alarms and events using Velocity Roles" option can cause unexpected results when an operator has multiple roles.	The **Restrict alarms and events using Velocity Roles** option (on the Advanced page of the Velocity Settings dialog) works by excluding everything not assigned to an operator role, rather than by including only those things assigned to an operator role. This approach works for a single operator role, but can have unexpected results when an operator has multiple roles. For example, when this option is enabled on a system with two controllers, you could create an operator role responsible for the first controller and another operator role responsible for the second controller. If an operator is then assigned both of these roles, you probably would expect that the operator will see the events and alarms from both controllers, but instead the operator will not see any events or alarms from either controller. There is no workaround for this issue.
VEL-3498	The status of a new credential with a delayed activation date/time might be prematurely shown as Active (if it was created on a Client in an earlier time zone than the Velocity Server).	On a system where a Velocity Client is in an earlier time zone than the Velocity Server, a new user credential with a delayed activation date/time which is created on that Client might have its status prematurely shown as Active. The credential is not actually activated until the Velocity Server's time reaches the specified activation time. There is no workaround for this issue.
VEL-3504 and VEL-3506	VelocityServices must use the "US" date/time format	When VelocityServices is using a non-US date/time format where the month and the day of the month are in a different order, the software event 1297 is displayed after the 12th day of the month: Database is offline. VelocitySQLWriter is storing commands offline for later execution. After this, transaction events for the Edge EVO Controller integration were no longer displayed in the Event Viewer. To prevent this issue, VelocityServices must use the "US" date/time format.

Reference ID	Summary	Description
VEL-3526	An error occurs if the Status Viewer is open while applying the Velocity 3.5 SP2 update	If the Status Viewer is open while applying the Velocity 3.5 SP2 update, the following error message is displayed:  The workaround is to close the Status Viewer before performing the update.
VEL-3527	Photo Callup feature is limited to 10 concurrent windows	Velocity provides a Photo Callup feature (which is configured on the General tab of a door's Properties dialog) that displays a credential's photo when access is attempted at a specific door. You specify what information is displayed by the Photo Callup feature by selecting a badge template, and you determine how long the information is displayed. Because this feature remembered the location of the window used for each enabled door, it was common practice for an operator to manually reposition the windows so they did not completely overlay each other. If too many doors are enabled with the Photo Callup feature, there can eventually be problems caused by a lack of system resources. (This is especially true when the information is displayed indefinitely, rather than for just a few seconds.) To reduce the occurrence of these problems, the Photo Callup feature is now limited to 10 concurrent windows. For 10 or less enabled doors, the Photo Callup feature operates as before, with a window dedicated to each door and the system remembering the position of each window. For more than 10 enabled doors, the credential information for a door can appear in any available window. When all 10 Photo Callup windows are in use, a window is reused if a different credential attempts access at one of those doors. If no window is available, the credential information will not be displayed, and a message listing the user ID that was not displayed will be written to the log file. There is no workaround for this issue.
VEL-3605	XMSG 14 is not being parsed correctly	The XMSG 14 message (about detecting a socket break) is not being parsed correctly by Velocity. There is no workaround for this issue.
VEL-3607	An unexpected exception occurs if you disable a port while credentials or configuration information is being downloaded	An unexpected exception (in code region PollingEngineInterface.TranslateMessage) occurs if you disable a port while credentials or configuration information is being downloaded to a controller on that port. There is no workaround for this issue.
VEL-3629	Windows local Administrator privilege is needed to run Velocity's Service Control Manager from a Velocity Client computer	To run Velocity's Service Control Manager from a Velocity Client, you must be logged into Velocity with a Windows user account that has local Administrator privilege on that computer. If you switch operators and log into Velocity with a non-Administrator account, you will no longer be able to use the Service Control Manager to start or stop Velocity's services (even if that account has the "Application Permissions ▸ Service Control Manager ▸ Service Control Manager – Use" role permission). This is a Known Issue that is working as designed.

Reference ID	Summary	Description
VEL-3631	Velocity cannot install from a long file path	If you copy the Velocity installation files to a directory structure that has a long file path, the installation will fail while trying to copy some .CAB files. The workaround is to use a different directory structure that has a shorter file path.
VEL-3667	Enabling the Issue Control option for a credential but clearing the Max field causes problems	The Options tab of the Credential Properties dialog includes an Issue Control feature. But if you deliberately clear the value in the **Max** field so it is blank and then click OK, it will cause problems.  The credential will be locked, and you won't be able to select it in the Enrollment Manager until after you restart Velocity. 

Reference ID	Summary	Description
VEL-3776	The Cogent CSD200 device driver does not work on Windows 8.	The device driver for Cogent's CSD200 fingerprint reader does not work on newer versions of the Windows operating system (such as Windows 8, 8.1, or 10). This causes the following error in Velocity when you try to use the Biometrics tab of the Credential Properties dialog:  There is no workaround for this issue with a 3rd-party device driver.
VEL-3906	When a credential's activation date is set to a future date, its status is sometimes not being updated correctly.	A credential's status does not update correctly when its activation date is set to a future date and its record (within the UserCredentials table) includes the obsolete DTIIHostActivationComplete field which is set to 1 (True). The workaround is to run a database script, which can be obtained from Identiv Technical Support.
VEL-3923	Exporting a complex report to Excel sometimes results in incorrect column headings	When a complex report is exported to Excel, the column headings are sometimes in the wrong order. The workaround is to export the report as a comma-separated values text file, edit the headings as needed, import the file into Excel, and then save the file as an Excel workbook.
VEL-3928	Incorrect version numbers sometimes shown after updating CCM firmware on a downstream controller	After updating the CCM firmware on a downstream controller, sometimes the previous version numbers or all zeros are shown in the **Firmware Revision** section on the General page of the Controller Properties dialog. The workaround is to issue Diagnostic Command 2 – System Information from the Velocity Diagnostic Window.

Reference ID	Summary	Description
VEL-3941	Velocity's Operator > Log Off Windows command generates an error (and is unnecessary)	Clicking on the Velocity menu button and selecting the **Operator ▸ Log Off Windows** command generates the following error:  This functionality is not really necessary, because you can just log off Windows normally by clicking on the Windows **Start** button (in the lower left corner) and selecting the **Log off** command from the Shut down menu: 
VEL-4019	Status Viewer might display inaccurate status for controllers after the DTServer is shut down abnormally	When DTServer did not shut down correctly, the SuperStatus table was not updated properly (by SDServer), so the Status Viewer might display inaccurate status information for controllers. There is no workaround for this issue, except to restart the DTServer.
VEL-4021 and VEL-4125	SDServer Dispatch errors in log file	Sometimes when a Velocity client disconnects, the connection is not properly cleaned up, which causes exceptions in the Security Domain Service's log for each event processed. There is no workaround for this issue.
VEL-4039	Keypad programming is not truly disabled on an Mx controller until you download a configuration to it	Velocity's user interface implies that keypad programming is disabled by default for Mx controllers. But this is not really true until you have manually downloaded a configuration to the controller. There is no workaround for this issue.
VEL-4067	The Download Monitor does not have a Description for the download of a FICAM Degraded Mode configuration	On a Velocity system running Identiv's FICAM Solution, a controller enters Degraded Mode when the certificates for its stored credentials have not been checked within a specified time limit. The behavior of the attached RS-485 readers when a controller is running in Degraded Mode is specified separately for each reader, and typically a controller's configuration will be different for Degraded Mode and need to be downloaded. But the Download Monitor does not have a Description for this type of download. There is no workaround for this issue.
VEL-4119	Dialup controller does not connect with host when an alarm occurs	A dialup controller is unable to establish a connection with the host when an alarm occurs. There is no workaround for this issue.

Reference ID	Summary	Description
VEL-4124	Velocity System Report fails if there are more than 1024 files in the Spooler\BatchErrors folder	If there are more than 1024 files in the **Spooler\BatchErrors** folder, the Velocity System Report fails and the following error message is displayed:  There is no workaround for this issue.
VEL-4152	The Security Domain Service appears to hang at startup if it cannot connect to the SQL Server	Velocity's Security Domain Service appears to hang at startup if it cannot connect to the SQL Server for the Velocity database. This happens when either: • the SQL server is paused or stopped, or • an incorrect DBserver instance name is specified in the **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hirsch Electronics\ Velocity\Client** registry entry. If you examine the contents of the **Velocity Security Domain Service-Technical Support File.txt** file a few minutes after the Security Domain Service has been started and see that nothing else is being logged, you should assume that the SQL Server is not reachable, and take corrective action.
VEL-4343	Velocity does not warn you when importing an older incompatible version of a TS reader firmware file	To support the new feature of downloading firmware updates to a TS reader, the format of those TRN files was changed in the Velocity 3.6 SP2.1 release. But Velocity still allows you to import older incompatible formats without warning you that they will not work. Do not select a TS reader firmware version which shows a value of only " ()" in the drop-down list: