Velocity 3.6 SP2.1

Product Release Bulletin

August 2017

IDENTIV

Product Release Bulletin for Velocity 3.6 SP2.1

1. uTrust TS Government ScramblePad Readers
The Hirsch ScramblePad has been infused with the power of TS. Also, available now is the ability to update reader configurations via firmware downloads from Velocity. The core functionality of features are now available in FICAM configurations, over OSDP, with RREB and SNIB3.

The familiar ScramblePad functions include:

- Extended Access
- Code Tamper Disables User
- Function Groups Extensions
- and many more

(Please consult the DIGI*TRAC Design and Installation Guide and ask SE/TS/PM for more details).

The ScramblePad features appear on the **Options** page of the Properties dialog for a door or a reader:

The firmware download process is the same as CCM, SNIB2, and SNIB3. Once you import the correct file(s) into Velocity, the update becomes globally available to any reader. Firmware changes are made one reader at a time. Since the ScramblePad has always depended on two-way communication to implement the advanced features, it made perfect sense to bring them forward to our new hardware, beginning with FICAM. SNIB3 controls all the features with onboard logic, harmonized with CCM, for situational awareness and action. RREB provides the eight individual OSDP communication paths to up to sixteen readers.

Look for ScramblePad Display, If/Then Annunciation, If/Then LED control, onboard OSDP, and full support for commercial applications on Mx-1 and corresponding Velocity future releases. TS ScramblePad buzzer control as well as LED and Numeric display control are not included in Velocity 3.6 SP2.1.

2. FICAM PIV Implementation Support
To support full implementation of FICAM in EPACS, our initial high-speed CAK-enabled TS card readers are now complemented by Veridt's Stealth series readers: Stealth Dual, and Stealth Bio.

While we've always supported most Wiegand output readers, we're now supporting third-party OSDP-based two-way communicating readers. Juxtaposed to the facility of supporting many card data differences sent across Wiegand, we'll build out the additional reader support as project and market problems give us the opportunities to do so.

With uTrust TS Government readers and the addition of Veridt's Stealth OSDP readers to the Hirsch FICAM solution, customers have the following options when setting the authentication mechanism required for Controlled, Limited, and Exclusion areas (as needed to support their PIV implementation strategy):

Controlled:

- CAK
- PIV Auth

Limited:

- CAK + PACS PIN
- PIV Auth

Exclusion:

- PIV Auth + Bio

We're helping customers transition to PIV by enabling the use of non-FICAM credentials based on maturity stage or for un-PIVable individuals. The traditional CCOTZ setting is used as an assurance level setting in OSDP, where during a CCOTZ Time Zone, specific readers can be set to accept non-FICAM credentials (in addition to PIV-based FICAM-compatible credentials).

For a uTrust TS Government reader:

- Default – CAK only
- Lower Assurance Level – CAK or HF or LF

For a uTrust TS Keypad Government reader:

- Default – CAK (PACS PIN based on IDF)
- Lower Assurance Level – CAK or HF or LF or PACS PIN or CAK/HF/LF + PACS PIN

For a uTrust TS ScramblePad Government reader:

- Default – CAK (PACS PIN based on IDF)
- Lower Assurance Level – CAK or HF or LF or PACS PIN or CAK/HF/LF + PACS PIN

For a Veridt Stealth Dual reader:

- Default – PIV Auth (PACS PIN based on IDF)
- Lower Assurance Level 1 – PIV Auth or CAK (PACS PIN based on IDF)
- Lower Assurance Level 2 – PIV Auth or CAK or HF or LF (PACS PIN based on IDF)

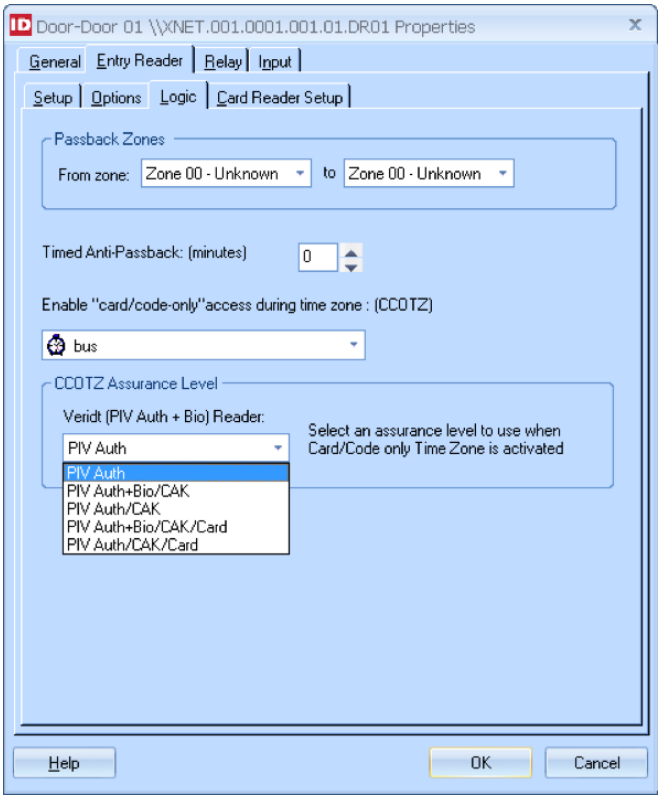
For a Veridt Stealth Bio reader:

- Default – PIV Auth + Bio (PACS PIN based on IDF)
- Lower Assurance Level 1 – PIV Auth (PACS PIN based on IDF)
- Lower Assurance Level 2 – PIV Auth + Bio or CAK or HF or LF (PACS PIN based on IDF)

- Lower Assurance Level 3 – PIV Auth + Bio or CAK (PACS PIN based on IDF)
- Lower Assurance Level 4 – PIV Auth or CAK (PACS PIN based on IDF)
- Lower Assurance Level 3 – PIV Auth + Bio or CAK or HF or LF (PACS PIN based on IDF)
- Lower Assurance Level 3 – PIV Auth or CAK or HF or LF (PACS PIN based on IDF)

For information about PIV Areas, Assurance Levels, CCOTZ, and IDF formats, consult existing Hirsch documentation or ask SE/TS/PM.

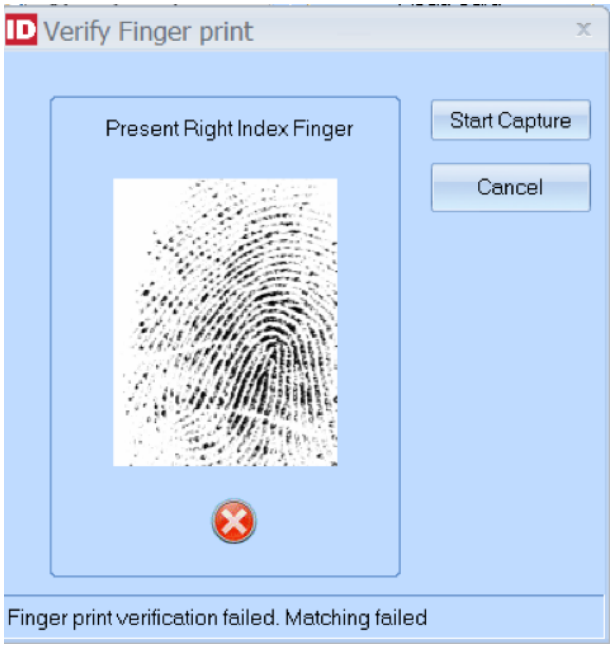
The option for setting a lower CCOTZ Assurance Level appears on the Logic page of the Properties dialog for a door or a reader:



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

Bio verification upon enrollment is now also included to support use of PIV Auth + Bio authentication at door locations into PIV Exclusion areas.

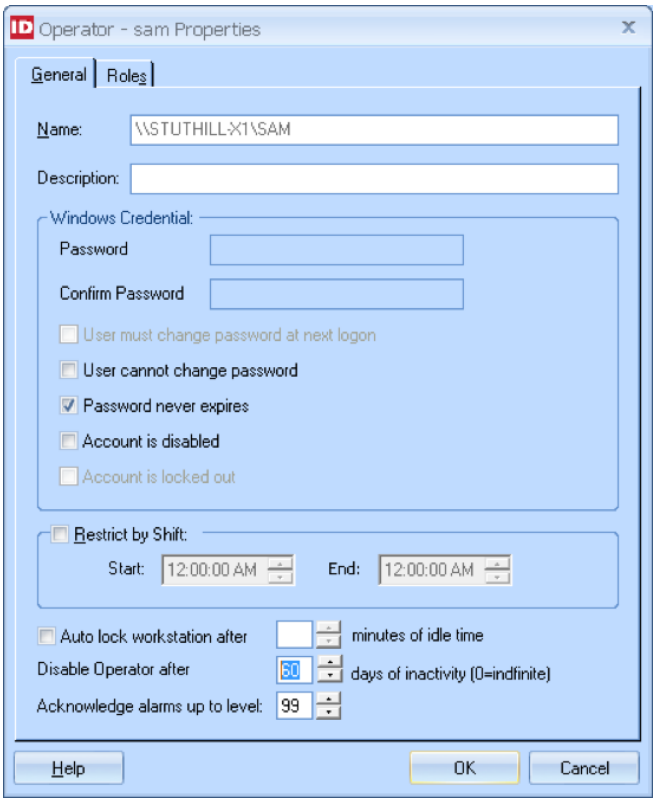
For example:



3. Velocity Operator Absentee Rule
NIST SP800-53 requires software application access to get revoked after a user-configurable period of inactivity, such as 30 or 60 days. It's up to the agency's CSO and can differ slightly based on the unique circumstances at each site. We have support for disabling Velocity Operators after 1-365 days without having used Velocity. The settings are the same as the Absentee Rule for cardholders.

Rest assured, Velocity Operators are still tied to Active Directory User objects. SSO continues to be supported, as well as smart card logon, password complexity, and all other Group Policy and network security settings. Of course an account disabled due to Windows inactivity or consecutive invalid logon attempts also cannot use Velocity.

The operator absentee setting (**Disable Operator after N days of inactivity**) appears near the bottom of the **General** page of the **Operator Properties** dialog:

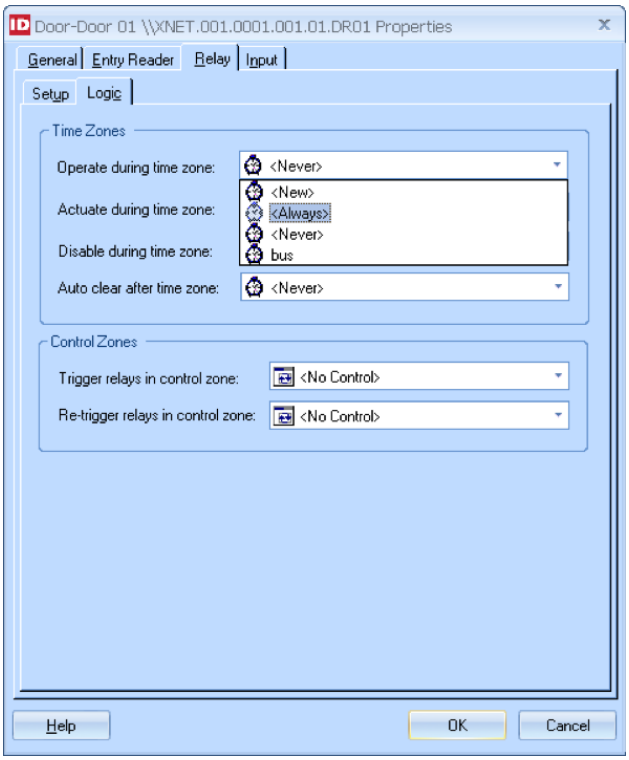


4. Relay Operate and Suppress

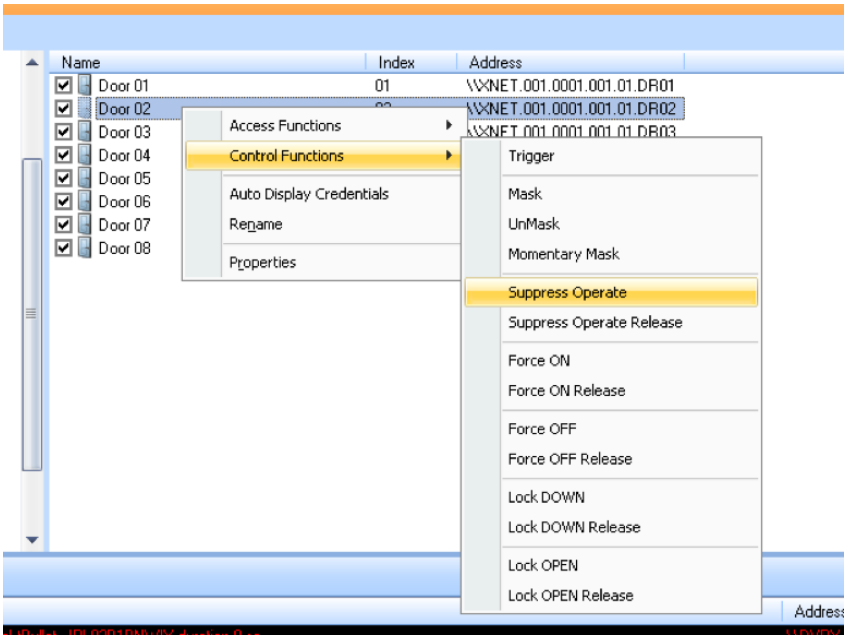
There are two new states for Doors and other Relays: **Suppress Operate** and **Suppress Operate Release**, which fall low on the Relay Command hierarchy, in contrast to the existing Actuate setting.

Relays are set to Operate or Suppress using either a Time Zone setting, right-click menu command, Master Control Zone, Command Set (single-click function in Graphics), or API instruction. **Suppress Operate** and **Suppress Operate Release** are also available as Credential Functions.

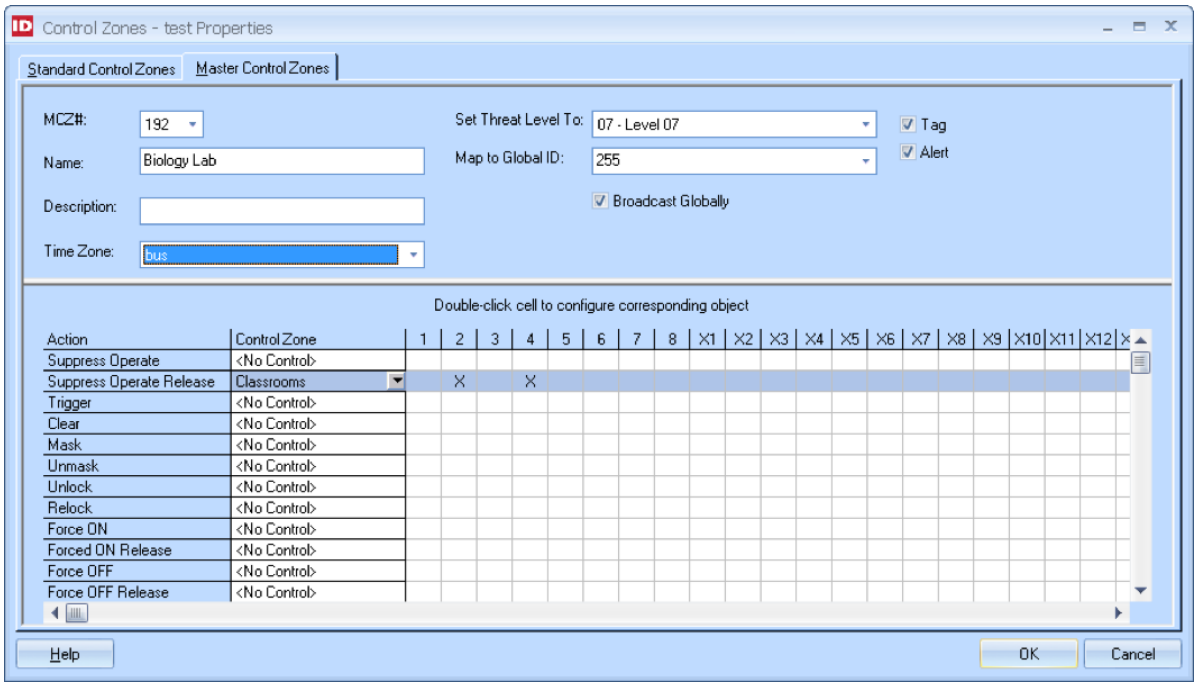
This is important because it's now much easier to set up lockdown applications based on Threat Level or other situations where controlled flow of access is critical (such as an active shooter). The programming of a relay by Time Zones or Control Zones is done on the **Logic** page of the Properties dialog for a door or a relay:



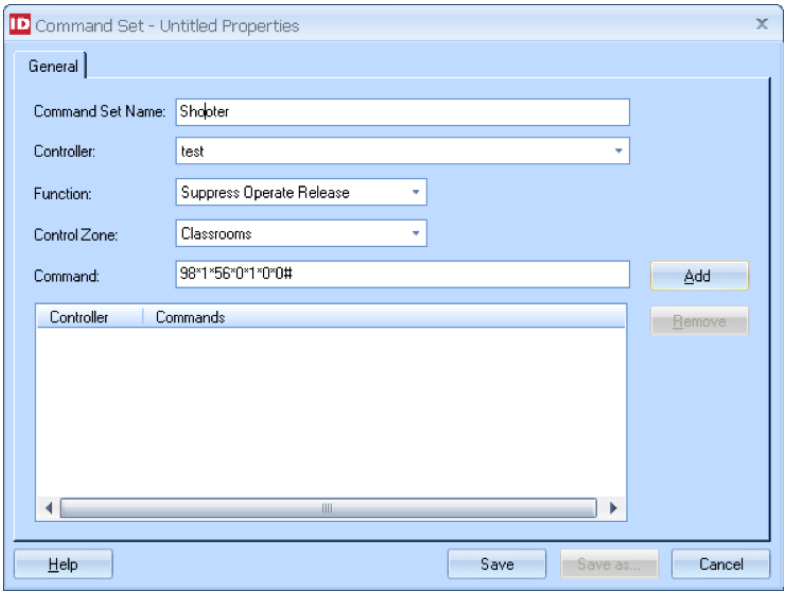
The manual setting of a door's relay is done using right-click menu commands:



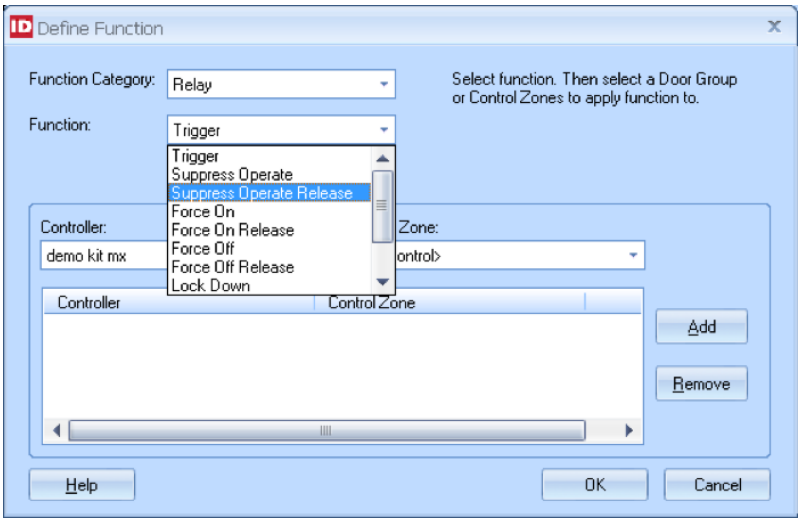
A relay can also be programmed by Master Control Zones:



A relay can also be programmed by Command Set:



A Credential Function can be defined to suppress the operation of a relay or release that suppression:



The Relay function hierarchy is as follows:

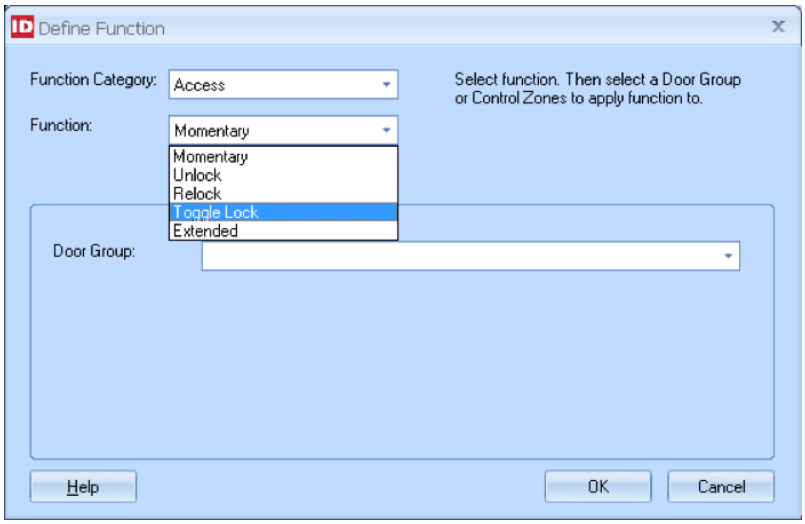
Lock Open / Lock Open Release [1] -- *Highest priority*
Lock Down / Lock Down Release [1]
CZ Disabled by Input [2]
CZ Actuated by Input [2]
Disable by Time Zone [3]
Actuate by Time Zone [3]
Clear Relays [3, 9]
Force Off / Force Off Release [1, 5]
Force On / Force On Release [1, 5]
Control Trigger [1, 2, 5, 6, 7]
Unlock / Relock / Toggle Lock [1, 4, 5, 8]
Extended Access [4, 5]
Access Trigger [4, 5] -- *Old Lowest priority*
Suppress Operate / Suppress Operate Release [10]
Operate by Time Zone [10] – *New Lowest Priority*

Footnotes:
[1] Control functions that can be triggered by a MCZ.
[2] Relay functions controlled by an input's setup screen.
[3] Relay functions controlled by a relay's "control by time zone" setup.
[4] Access functions. Typically the result of an access/whatever grant at a reader.
[5] Cleared by "Clear Relays" function
[6] Various things Trigger or Retrigger control zones, such as an input's "trigger CZ/retrigger SCZ" functions.
[7] If Control Mode time = 0, a trigger will alternately turn on or off the "Control Trigger" priority level.
[8] If Door Mode time = 0, an Access Grant will alternately Unlock or Relock the relay.
[9] "Clear Relays" is available as a function such as a credential or MCZ, or through "Clear Relay at end of Time Zone" on relay setups.
[10] "Operate by Time Zone" and "Suppress Operate/Suppress Operate Release" are the new “basement” sub-priority levels.

5. Toggle Lock Credentials

There is a new function that enables a single card/code/extension digit or other credential format to make any relay-controlled device (such as a lobby door, HVAC, or machine) "toggle" between off and on. Previously, the Relay itself could be set to toggle between off/on and we've added the flexibility to use that setting for dedicated locations plus the credential function for Relays which must provide timed operation of a device or Toggle.

The **Toggle Lock** function is available for a Credential Function:



6. Mx-2/4 Wiegand Exit Readers

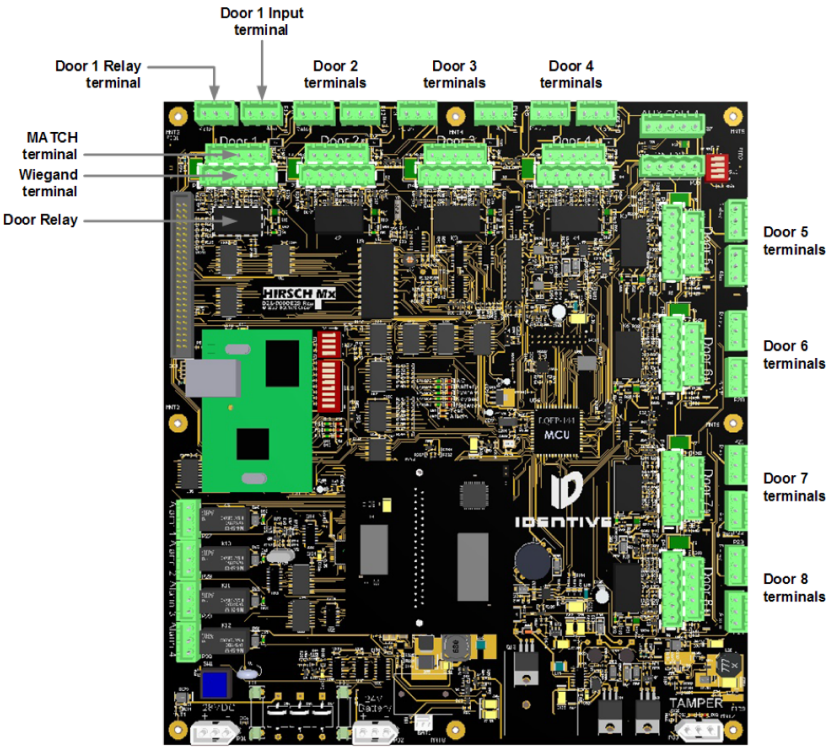
Repurposing the unused onboard Wiegand terminals on an Mx-2 or Mx-4 controller for exit readers is new in the Velocity 3.6 SP2.1 release. MATCH boards are no longer required for exit readers, except in the case of an Mx-8 where all of the onboard Wiegand terminals are assigned to entry readers.

Now, on Mx-2/4 we've enabled onboard Wiegand terminals 5 through 8 as dedicated exit reader terminals. Wiegand terminal 5 is the Exit for Entry terminal 1, 6 exits 2, 7 exits 3, and 8 exits 4. There are no setting changes required to be made in Velocity to enable this feature. It just works when readers are added to the controller – same as MATCH always has functioned. It's fully implemented on the motherboard now.

(The upcoming single-door Mx-1 controller has two Wiegand terminals, one dedicated to the entry reader and the other dedicated to the optional exit reader. It also supports OSDP with an OSDP RS-485 terminal, and will support all the new features to be introduced in TS ScramblePad and other products.)

The following diagram shows the location of the 8 door terminal groups on the Mx controller's main board, and the table shows the mapping of the 8 Wiegand terminals for the Mx-8, Mx-4, and Mx-2 models.

Door terminals on the Mx controller's main board:



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)